NAME

proberoute − Prints the route that IP packets take to a network host with multiple protocols and detection methods.

SYNOPSIS

proberoute [OPTION] DEST

proberoute [OPTION] DEST PORT

DESCRIPTION

> **Attention:** The proberoute command is only intended for use in network testing, measurement, and management. It should be used primarily for manual fault isolation. Because of the load it imposes on the network and causes some security implications, the proberoute command requires super-user privileges, and should not be used during normal operations or from automated scripts. See the **SECURITY** section.

Proberoute is a program that behaves in much the same way that **traceroute(8)** does, but has more options. The proberoute command attempts to trace the route an IP packet follows to a target host by launching UDP/TCP/ICMP probe packets with a small maximum time−to−live (Max_ttl variable), then listening for an ICMP **TIME_EXCEEDED** response from gateways along the way. Probes are started with an Max_ttl value of one hop, which is increased one hop at a time until an ICMP **PORT_UNREACHABLE, ICMP_ECHOREPLY, ICMP_TSTAMPREPLY** or TCP **RST, SYN, ACK** messages is returned. These messages indicates that the host has been located.

Unlike the traceroute program, the proberoute default sends three TCP probes at each Max_ttl setting to record the following:

* Max_ttl value
* Address of the gateway
* Round-trip time of each successful probe

The number of probes sent can be increased by using the **−q** flag. If the probe answers come from different gateways, the command prints the address of each responding system. If there is no response from a probe within a 3-second time−out interval, an ***** (asterisk) is printed for that probe.

The proberoute command prints an **!** (exclamation mark) with an abbreviation before the round-trip time indicates that received the ICMP notification message:

Item	Description
!	Port unreachable (the ttl is <= 1)
!PORT	Port unreachable
!H	Host unreachable
!N	Network unreachable
!P	Protocol unreachable
!F	Need fragment
!S	Source route failed
!U	Unknown network
!W	Unknown host
!I	Source route isolated
!A	Admin prohibited network
!Z	Admin prohibited host
!Q	Bad tos for network
!T	Bad tos for host

!X	Admin prohibited filter
!V	Host precedence violation
!C	Precedence cutoff
!TTL	Time exceeded

Increase the verbosity by **-v** flag will show the detail message. When received the ICMP Need Fragment error message (!F flag), the proberoute program will change the next hop Maximum Transmission Unit (MTU) with the same Max_ttl value and trying again. If the ICMP error message is not expected, the proberoute command will exit.

The TCP/UDP probe packets are set to an unlikely value so as to prevent processing by the destination host. You can change the destination port with **-p** option.

OPTIONS

Item Destination

−v, −−verbose
Verbose output, multiple -v options increase the verbosity.

−h, −−help
Show the brief help message.

−P *protocol*
Send packets of specified IP protocol. *protocol* should be "TCP", "UDP" or "ICMP". Alternately, you can specify the **−−tcp, −−udp,** or **−−icmp** flags. Note that these options can be specified at the same time.

−−tcp Send the TCP SYN probe packets, this technique is often referred to as half−open scanning, because you don't open a full TCP connection. The default destination port is 33434, which can be changed with **−p** flags. Refer to the RFC 793 and Nmap **−sS** option, A SYN/ACK indicates the port is listening (open), while a RST (reset) is indicative of a non-listener. If no response is received after several retransmissions, the probe is marked as an ***** (asterisk). The hop IP can also be fetched if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received. The port is also considered open if a SYN packet (without the ACK flag) is received in response.

−−udp Send the UDP probe packets. The default destination port is 33434. For some common ports such as 53 (DNS), 161 (SNMP), 67/68 (DHCP), etc., which can be specified with **−p** or **-g** flags, a port−specific probe is sent to increase response rate. If an ICMP Port Unreachable error (type 3, code 3) is returned, the host is reachable (the port is closed). Other ICMP Unreachable errors (type 3, codes 0, 1, 2, 9, 10, or 13) will be captured and get the source address IP from them. Occasionally, because of the UDP port is open, a service will respond a UDP packet instead of a ICMP error message, so the probe will be timed−out and marked as an *****, because the proberoute program will increase the destination port by 1 every hop, the host IP will display at the next hop.

−−icmp
Send the ICMP Echo probe packets, wait for the ICMP Time Exceeded error or ICMP Echo Reply message.

−A, −−all Same as '--tcp --udp --icmp'.

−p, −−port *portnum*
Set the base destination port number for TCP or UDP, the default is 33434. The proberoute command will increment the UDP port number every Max_ttl, but keep the TCP port number unchanged. Note that when UDP and TCP probe packets are used at the same time, this option is valid only for TCP probes, while UDP base port number is fixed to 33434.

−g, −−source−port *portnum*
For UDP, TCP, set the source port number used in probes. The default is random port.

−S, −−source−ip *IPaddr*
Set the source address for probes, must use **-i** option to specify the interface you wish to send.

−i *interface*
Specify a network interface to send probes and obtain the source IP address for outgoing probe packets.

−q *nqueries*
Specifies the number of probe packets the traceroute command sends at each Max_ttl setting. The default is three probes. Note that some routers and hosts can use ICMP rate throttling. In such a situation specifying too large number can lead to loss of some responses.

−w *waittime*
Sets the time (in seconds) to wait for a response to a probe. The default is 3 seconds.

−f *first_ttl* Set the initial time−to−live used in outgoing probe packets. The default is 1, i.e., start with the first hop.

−m *max_ttl*
Set the max time−to−live (max number of hops) used in outgoing probe packets.

−F, −−frag−size *frag_size*
Specify the IP fragment size (must be a multiple of eight). Because some firewalls don't check the fragmented packets for performance reasons, fragments are possible to reach the host.

−s, −−mtu *MTUsize*
Using the specified MTU as the probe packets size. Default is auto detection. Note that when UDP and other protocols are used at the same time, this option is only valid for other protocols while the UDP packet length is fixed to 52-byte. This option is ignored when send the TCP syn package because the TCP syn package cannot have any payload.

−−conn (TCP connect probe)
TCP connect probe is usable for detecting the path MTU when the firewall only opening for the specific TCP port. When the connection established, the proberoute program will send the out−of−sequence probe packet with specific length and TCP flags (usually with **−−ack** flag), for preventing processing by the destination host.

Because of using **connect(2)** call will make the tcp session full opening, not recommended for normal use, because a destination application is always affected (and can be confused). For the same reason, if the destination is in the same subnet (ttl = 1), Proberoute never call **connect(2)**.

−−syn/ack/push/null/fin/xmas
Use TCP SYN, ACK, PUSH, Null, FIN and Xmas probes with **−−tcp** option. This feature comes from the **nmap(1)** program. **−−null** option doesn't set any bits (TCP flag header is 0), **−−xmas** sets the FIN, PSH, and URG flags. When the firewall is open, refer to the RFC 793 (Page 65)

- If the target host state is CLOSED, an incoming segment not containing a RST causes a RST to be sent in response.
- If the target host state is LISTEN, any acknowledgment segment causes a RST to be sent in response.
- If the target host state is LISTEN, the SYN packet causes a SYN + ACK to be sent in response.
- If the target host state is ESTABLISHED, the out−of−sequence packet causes an ACK should be sent in response.

−−badsum
Send the probe packets with a bogus checksum. Since virtually all host IP stacks properly drop these packets, any responses received are likely coming from a firewall or IDS that didn't bother to verify the checksum.

−−badlen Send the probe packets with a bad IP option length (by IP timestamp option). An ICMP Parameter Problem error message will be sent when a router (MUST generate this message) or a host (SHOULD generate this message) finds a problem with the IP header parameters. This option is not very helpful for tracing route.

−e, −−echo
−−echo−reply
Send ICMP echo/echo−reply probes. when the firewall is open:

- The **ICMP_ECHO** probe causes the target host MUST response the **ICMP_ECHOREPLY** message.
- The **ICMP_ECHOREPLY** probe causes the target host MAY response the **ICMP_UNREACH_PORT** message.

−t, −−tstamp
−−tstamp−reply
Send ICMP timestamp/timestamp−reply probes. when the firewall is open:

- The **ICMP_TSTAMP** probe causes the target host MAY response the **ICMP_TSTAMPREPLY** message.
- The **ICMP_TSTAMPREPLY** probe causes the target host MAY response the **ICMP_UNREACH_PORT** message.

−j, −−source-route *gateway*
Sets IP Loose Source Route option. Tell the network to route the packet through the specified gateway (Unfortunately, most routers have disabled source routing for security reasons).

−l, −−list Print the list of the network interface avaiable on the system, but Proberoute can't sniff loopback packets on Windows system.

−−simulate
When the connection is established, to detect the route by sending a order bye packet, which must be used with **−−conn** option.

−−reverse
Set the TTL of the probe packet decreased from large to small. Used to evade the Cisco ASA firewall **ttl−evasion−protection** policy.

−−retransmit
Retransmit the specified packet in interactive mode, should be used with **−−conn** and **−−interact** option. Note: retransmit the last packet received by the other side will be considered as the TCP keepalive probe.

−−interact
When the connection is established, control the frequency of sending bytes through this option. Each time a line read from stdin, sends a "\x00" byte by **write()** . This option can be used with *tcpdump* and Unix *discard* service. For example, asymmetric routing will cause network rejection due to non-synchronization of TCP sessions, this option can be used to send probe packets when retransmission occurs.

PARAMETERS

Item Description

HOST Specifies the destination host, either by host name or IP number. This parameter is required.

PORT Specifies the destination port or service for TCP or UDP protocol. The default port is 33434.

EXAMPLE

A sample use and output might be:

```
$ sudo ./proberoute -A www.ccb.com http
proberoute to www.ccb.com (114.251.28.14) from 192.168.0.100 (en0)
with TCP UDP ICMP protocol
destination: 0.0.0.0, gateway: 192.168.0.1, mask: 0.0.0.0
1 hops min, 30 hops max
outgoing MTU = 1500
  1  192.168.0.1  125.682 ms  0.178 ms  0.063 ms
  2  192.168.0.1  !F  10.378 ms * *
  3  182.93.63.226  10.342 ms
     182.93.63.222  0.104 ms
     182.93.63.226  0.057 ms
  4  182.93.63.225  10.405 ms
     182.93.63.221  0.090 ms  0.110 ms
  5  202.175.54.69  10.163 ms
     202.175.54.77  0.120 ms  0.089 ms
  6  219.158.35.37  20.366 ms  0.102 ms  0.084 ms
  7  219.158.97.30  20.372 ms  0.090 ms  0.109 ms
  8  219.158.97.1  21.376 ms  0.099 ms *
  9  219.158.7.17  52.008 ms
     219.158.15.37  0.209 ms
     219.158.7.17  52.589 ms
 10  61.49.214.6  40.893 ms  0.118 ms
     202.96.12.2  10.415 ms
 11  124.65.61.174  40.759 ms  10.622 ms  31.370 ms
 12  61.148.157.10  52.019 ms  0.136 ms  10.123 ms
 13  61.148.14.34  41.982 ms  0.071 ms  10.966 ms
 14  202.106.80.123  41.084 ms  0.109 ms  41.323 ms
 15  114.251.28.14  !TTL  51.908 ms  !TTL  0.133 ms  !TTL  51.926 ms
 16  202.106.80.123  41.755 ms  10.226 ms  31.636 ms
 17  * * *
 18  114.251.28.14  52.930 ms  0.107 ms  52.539 ms
Port 80 open
```

Note that:

- The line 2 hop received the ICMP Destination Unreachable messages containing Code 4 (Fragmentation needed and DF set), so the proberoute program change the next–hop MTU and try again, with **–v** flag will see the changed MTU.
- The line 15 hop arrived the target host, but received the ICMP Time Exceeded messages, since only the router will send this message, so the proberoute program will continue to trace route, and arrived the real target host at the line 18 hop.
- Because of the **–A** flag, each probe sends TCP, UDP, and ICMP packets respectively, but the line 17 hops don't send ICMP Time Exceeded messages (it is also unlikely that ttl is too small to reach us), perhaps due to the firewall rules. You can try proberoute's advanced options for firewall evasion or spoofing under the permission from the network administrator.

FILES

Proberoute relies on **libpcap** library, which provide common methods to access the datalink layer by wrapping the BSD Packet Filter (BPF), the Linux PF_PACKET interface, or other methods. **Npcap** and **WinPcap** are Windows versions of the **libpcap** library, by making use of the NPF/NDIS API.

Item
: Description

/usr/lib/libpcap.a
: Libpcap library file

/dev/bpf?
: BPF device

/proc/net/dev
: Network interfaces information

C:\Windows\system32\[Npcap?]\Packet.dll
: WinPcap/Npcap low-level dynamic link library.

C:\Windows\system32\[Npcap?]\wpcap.dll
: WinPcap/Npcap high-level and system-independent library.

SEE ALSO

traceroute(8), nmap(1), ping(1)

SECURITY

This command requires privileged users due to using **libpcap/WinPcap** and raw socket.

When used properly, Proberoute helps to detect the routing problems and location errors. But when used improperly, Proberoute could (in rare cases) cause damage to the network or host, even get you sued, fired, or banned by your ISP.

Refer to the advice from Lyon (author of Nmap), the best way to avoid controversy when using Proberoute is to always secure written authorization from the target network representatives before initialing any probing.

WARNING

Since the **--frag-size** can split the packet into eight bytes, so a 20-byte TCP header would be split into three packets, but this feature is not supported or even dangerous on some systems.

Especially the fragment size of eight bytes MAY causes the AIX system crash immediately. In addition, the TCP packet can't be fragmented less than the size of header on AIX system.

COPYRIGHT

AVAILABILITY

The source code of proberoute command is available from https://github.com/GongCun/proberoute, it's very much welcome to participate in the development and help to improve Proberoute.

BUGS

The round-trip times between the router or the target host depends on the time the packet is captured, rather than the actual round-trip time, such as the delay of 500 ms on the Windows system due to the delay of **WinPcap**.

The following is a list of those features not yet implemented:

* IPv6 supporting.
* Reverse DNS lookups (PTR).
* Autonomous System (AS) path lookups.
* Sending several probes concurrently.
* Can not use **--conn** option on some Windows system.

Since the old version of **WinPcap** does not support PPP/VPN connection on Windows Vista or above, the

new version of **Npcap** must be installed so that the Proberoute can detect routing on the PPP/VPN connection.

In addition to the pcap filter, Proberoute supports receiving data from raw sockets (by *recvfrom* on Unix/Linux, *WSARecvFrom* on Windows), user can specify Proberoute receiving data through raw sockets via the environment variable **PROBE_RECV**, Use **–vvv** flags can watch which capture catch the packet:

```
$ sudo PROBE_RECV=1 ./proberoute –vvv –icmp google.com
```

Because of IPsec with Authentication Header (AH) or Encapsulating Security Payload (ESP) can not be captured by **libpcap**, in this case, should detect the route by raw sockets. Due to the limitations of most operating systems, TCP data is not allowed to be received directly by raw socket, so when using the TCP protocol to detect routing, the '*' (asterisk) may still be displayed after reaching the destination. On Windows, the TCP protocol cannot be used to detect routing on the PPP/VPN connection, and normal connection may not be able to detect routing on overly noisy ports.

On Windows system, when Proberoute received ICMP Fragmentation Needed error message, if use the same size of message to traceroute again, will trigger "message too long" error, must reduce the message size to the path MTU.

Since I have no environment to test these link types such as IEEE 802.11 wireless LAN, PPPoE, SLIP, or Cisco PPP with HDLC framing, etc., so there may be BUGs hidden in them. If you found any bug, please report it to Cun Gong <gong_cun@bocmacau.com>, thank you very much.