sanfoundry.com

"traceroute" Command Usage Examples in Linux

by linuxcmd2

9-11 minutes

This tutorial explains Linux “traceroute” command, options and its usage with examples.

traceroute – Print the route packets take to network host.

DESCRIPTION

traceroute is a network troubleshooting utility which shows number of hops taken to reach destination also determine packets traveling path. Below we are tracing route to global DNS server IP Address and able to reach destination also shows path of that packet is traveling.

SYNOPSIS

traceroute [-d] [-F] [-l] [-n] [-v] [-x] [-f first_ttl] [-g gateway [-g gateway] | -r] [-i iface] [-m max_ttl] [-p port] [-q nqueries] [-s src_addr] [-t tos] [-w waittime] host [packetlen]

OPTIONS :

-d

Set the SO_DEBUG socket option.

-F

Set the “don’t fragment” bit.

-I

Use ICMP ECHO instead of UDP datagrams.

-n

Print hop addresses numerically rather than symbolically and numerically. This saves a nameserver address-to-name lookup for each gateway found on the path.

-v

Verbose output. For each hop, the size and the destination of the response packets is displayed. Also ICMP packets received other than TIME_EXCEEDED and UNREACHABLE are listed as well.

-x

Prevent traceroute from calculating checksums. Note that checksums are usually required for the last hop when using ICMP ECHO probes. See the -I option.

-f first_ttl

Set the starting ttl value to first_ttl, to override the default value 1. traceroute skips processing for those intermediate gateways which are less than first_ttl hops away.

-g gateway

Specify a loose source route gateway. The user can specify more than one gateway by using -g for each gateway. The maximum that can be set is 8.

-r

Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to send probes to a local host through an interface that has been dropped by the router daemon.

-i iface

Specify a network interface to obtain the source IP address for

outgoing probe packets. This is normally only useful on a multi-homed host. The -s option is also another way to do this. Note that this option does not provide a way to specify the interface on which the probe packets are sent.

-m max_ttl

Set the maximum ttl used in outgoing probe packets. The default is 30 hops, which is the same default used for TCP connections.

-p port

Set the base UDP port number used in probes. The default is 33434. traceroute hopes that nothing is listening on UDP ports (base+(nhops- 1)*nqueries) to (base+(nhops*nqueries)-1)at the destination host, so that an ICMP PORT_UNREACHABLE message will be returned to terminate the route tracing. If something is listening on a port in the default range, this option can be used to select an unused port range.nhops is defined as the number of hops between the source and the destination.

-q nqueries

Set the desired number of probe queries. The default is 3.

-s src_addr

Use the following address, which usually is given as an IP address, not a hostname, as the source address in outgoing probe packets. On multi-homed hosts, those with more than one IP address, this option can be used to force the source address to be something other than the IP address traceroute picks by default. If the IP address is not one of this machine’s interface addresses, an error is returned and nothing is sent. When used together with the -i option, the given IP address should be configured on the specified interface. Otherwise, an error will be returned.

-t tos

Set the tos(Type-of-service) in probe packets to the specified value.

The default is zero. The value must be an integer in the range from 0 to 255. Gateways along the path may route the probe packet differently depending upon the tos value set in the probe packet.

-w waittime

Set the time, in seconds, to wait for a response to a probe. The default is five (5) seconds.

host The network host.

EXAMPLES

1. Ping the host to see if its alive

```
# traceroute 4.2.2.2

traceroute to 4.2.2.2 (4.2.2.2), 30 hops max, 60
byte packets
 1  192.168.50.1 (192.168.50.1)  0.217 ms  0.624
ms  0.133 ms
 2  227.18.106.27.mysipl.com (27.106.18.227)
2.343 ms  1.910 ms  1.799 ms
 3  221-231-119-111.mysipl.com (111.119.231.221)
4.334 ms  4.001 ms  5.619 ms
 4  10.0.0.5 (10.0.0.5)  5.386 ms  6.490 ms  6.224
ms
 5  gi0-0-0.dgw1.bom2.pacific.net.in
(203.123.129.25)  7.798 ms  7.614 ms  7.378 ms
 6  115.113.165.49.static-mumbai.vsnl.net.in
(115.113.165.49)  10.852 ms  5.389 ms  4.322 ms
 7  ix-0-100.tcore1.MLV-Mumbai.as6453.net
(180.87.38.5)  5.836 ms  5.590 ms  5.503 ms
 8  if-9-5.tcore1.WYN-Marseille.as6453.net
(80.231.217.17)  216.909 ms  198.864 ms  201.737
```

```
ms
 9  if-2-2.tcore2.WYN-Marseille.as6453.net
(80.231.217.2)  203.305 ms  203.141 ms  202.888 ms
10  if-5-2.tcore1.WV6-Madrid.as6453.net
(80.231.200.6)  200.552 ms  202.463 ms  202.222 ms
11  if-8-2.tcore2.SV8-Highbridge.as6453.net
(80.231.91.26)  205.446 ms  215.885 ms  202.867 ms
12  if-2-2.tcore1.SV8-Highbridge.as6453.net
(80.231.139.2)  202.675 ms  201.540 ms  203.972 ms
13  if-6-2.tcore1.NJY-Newark.as6453.net
(80.231.138.18)  203.732 ms  203.496 ms  202.951
ms
14  if-2-2.tcore2.NJY-Newark.as6453.net
(66.198.70.2)  203.858 ms  203.373 ms  203.208 ms
15  66.198.111.26 (66.198.111.26)  201.093 ms
63.243.128.25 (63.243.128.25)  206.597 ms
66.198.111.26 (66.198.111.26)  204.178 ms
16  ae9.edge1.NewYork.Level3.net (4.68.62.185)
205.960 ms  205.740 ms  205.487 ms
17  vlan51.ebr1.NewYork2.Level3.net (4.69.138.222)
203.867 ms vlan52.ebr2.NewYork2.Level3.net
(4.69.138.254)  202.850 ms
vlan51.ebr1.NewYork2.Level3.net (4.69.138.222)
202.351 ms
18  ae-6-6.ebr2.NewYork1.Level3.net (4.69.141.21)
201.771 ms  201.185 ms  201.120 ms
19  ae-81-81.csw3.NewYork1.Level3.net
(4.69.134.74)  202.407 ms  201.479 ms
ae-92-92.csw4.NewYork1.Level3.net (4.69.148.46)
208.145 ms
```

```
20  ae-2-70.edge2.NewYork1.Level3.net
(4.69.155.80)  200.572 ms
ae-4-90.edge2.NewYork1.Level3.net (4.69.155.208)
200.402 ms ae-1-60.edge2.NewYork1.Level3.net
(4.69.155.16)  203.573 ms
21  b.resolvers.Level3.net (4.2.2.2)  199.725 ms
199.190 ms  202.488 ms
```

2. Disable IP address and host name mapping

```
$ traceroute google.com -n
traceroute to google.com (173.194.36.7), 30 hops
max, 60 byte packets
1  220.224.141.129  109.352 ms  109.280 ms
109.248 ms
2  115.255.239.65  131.633 ms  131.598 ms  131.573
ms
3  124.124.251.245  131.554 ms  131.529 ms
131.502 ms
4  115.255.239.45  131.478 ms  131.464 ms  199.741
ms
5  72.14.212.118  199.674 ms  199.637 ms  199.603
ms
6  209.85.241.52  199.578 ms  199.549 ms  209.838
ms
7  209.85.241.187  199.488 ms  177.264 ms  177.196
ms
8  173.194.36.7  177.159 ms  187.463 ms  187.434
ms
```

3. Configure Response Wait Time

The -w option expects a value which the utility will take as the response time to wait for. In this example, the wait time is 0.1 seconds and the traceroute utility was unable to wait for any response and it printed all the *'s.

```
$ traceroute google.com -w 0.1
traceroute to google.com (74.125.236.101), 30 hops
max, 60 byte packets
1  * * *
2  * * *
3  * * *
..
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

4. Configure Number of Queries per Hop

The traceroute utility sends 3 packets per hop to provide 3 round trip times. This default value of 3 is configurable using the option '-q'. This option expects an integer which it sets as new value of number of probes per hop.

```
$ traceroute google.com -q 5
traceroute to google.com (173.194.36.46), 30 hops
max, 60 byte packets
1  220.224.141.129 (220.224.141.129)  91.579 ms
91.497 ms  91.458 ms  91.422 ms  91.385 ms
2  115.255.239.65 (115.255.239.65)  91.356 ms
91.325 ms  98.868 ms  98.848 ms  98.829 ms
```

```
3  124.124.251.245 (124.124.251.245)  94.581 ms
107.083 ms  107.044 ms  107.017 ms  106.981 ms
4  115.255.239.45 (115.255.239.45)  106.948 ms
106.918 ms  144.432 ms  144.412 ms  144.392 ms
5  72.14.212.118 (72.14.212.118)  115.565 ms
115.485 ms  115.446 ms  115.408 ms  115.381 ms
6  72.14.232.202 (72.14.232.202)  115.351 ms
87.232 ms  117.157 ms  117.123 ms  117.049 ms
7  209.85.241.189 (209.85.241.189)  126.998 ms
126.973 ms  126.950 ms  126.929 ms  126.912 ms
8  bom04s02-in-f14.1e100.net (173.194.36.46)
126.889 ms  95.526 ms  95.450 ms  95.418 ms
105.392 ms
```

5. Configure the TTL value to start with

By default its value is 1 which means it starts off with the first router in the path but using the '-f' option (which expects the new value of TTL) a new value of the TTL field can be set

```
$ traceroute google.com
traceroute to google.com (74.125.236.132), 30 hops
max, 60 byte packets
1  220.224.141.129 (220.224.141.129)  89.181 ms
101.540 ms  101.503 ms
2  115.255.239.65 (115.255.239.65)  101.468 ms
101.431 ms  101.324 ms
3  124.124.251.245 (124.124.251.245)  121.373 ms
121.350 ms  158.694 ms
4  115.255.239.45 (115.255.239.45)  101.223 ms
141.135 ms  123.932 ms
5  72.14.212.118 (72.14.212.118)  123.867 ms
```

```
123.832 ms  123.802 ms
6  72.14.232.202 (72.14.232.202)  123.773 ms
123.742 ms  587.812 ms
7  216.239.48.179 (216.239.48.179)  587.723 ms
587.681 ms  587.642 ms
8  bom03s02-in-f4.1e100.net (74.125.236.132)
577.548 ms  577.524 ms  587.512 ms

$ traceroute google.com -f 8
traceroute to google.com (74.125.236.129), 30 hops
max, 60 byte packets
8  bom03s02-in-f1.1e100.net (74.125.236.129)
96.961 ms  96.886 ms  96.849 ms
```

Sanfoundry Global Education & Learning Series – 1000 Linux Tutorials.