Troubleshooting Tools

An overview of the main tools for verifying network operation from a host

Fulvio Risso
Mario Baldi
Politecnico di Torino
(Technical University of Turin)

Notes

- The commands/programs described in this presentation are commonly available both on UNIX and Windows workstations.
- Nevertheless:
  - Options and parameters might be different
  - Output might be different
  - Hence...
    - Content of this presentation should not be taken literally
    - It should be used as a starting point
    - Command syntax and output should be double-checked
  - Moreover only options and parameters considered relevant to our purposes are listed here.
  - For some commands an equivalent program with graphic interface might exist.

ping

- Checks network reachability of a host
- Syntax:
  ping [options] target

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t</td>
<td>ICMP Echo Request messages sent continually until Ctrl+C is pressed (in UNIX this is default behaviour).</td>
</tr>
<tr>
<td>-c count</td>
<td>Sends count ICMP Echo Request messages (in Windows default count is 4).</td>
</tr>
<tr>
<td>-I TTL</td>
<td>ICMP Echo Request messages are sent into IP packet with Time To Live field containing TTL (only Windows).</td>
</tr>
<tr>
<td>-w timeout</td>
<td>A reply is waited for at most timeout milliseconds; if a later reply is ignored.</td>
</tr>
<tr>
<td>-R</td>
<td>(Possibly) records path taken by packets by activating Record Route option in the ICMP Echo Request message.</td>
</tr>
</tbody>
</table>
ping Output Example

PING www.xenia.it (209.238.252.133): 56 data bytes
64 bytes from 209.238.252.133: icmp_seq=0 ttl=113 time=1318 ms
64 bytes from 209.238.252.133: icmp_seq=1 ttl=113 time=1738 ms
64 bytes from 209.238.252.133: icmp_seq=2 ttl=113 time=1756 ms
64 bytes from 209.238.252.133: icmp_seq=3 ttl=113 time=1808 ms
64 bytes from 209.238.252.133: icmp_seq=4 ttl=113 time=1804 ms
64 bytes from 209.238.252.133: icmp_seq=5 ttl=113 time=1751 ms
64 bytes from 209.238.252.133: icmp_seq=6 ttl=113 time=1617 ms
64 bytes from 209.238.252.133: icmp_seq=7 ttl=113 time=1526 ms
64 bytes from 209.238.252.133: icmp_seq=8 ttl=113 time=902 ms
64 bytes from 209.238.252.133: icmp_seq=9 ttl=113 time=1409 ms

--- www.xenia.it Ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms) min/avg/max = 902/1562/1808 ms

Round-trip time (RTT): time elapsed from the transmission of an ICMP Echo Request to the reception of the corresponding ICMP Echo Reply; it is a measure of the “distance” between local and target host.

ping Working Principle

- Testing host sends an ICMP Echo Request message to target host
- Target host replies with ICMP Echo Reply message

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interpreting ping Outcome

- If replies are received, connectivity to target host exists
- When replies are not received
  - A routing problem might exist on the path from local host to target
  - A routing problem might exist on path from target to local host
  - The two paths might not be the same
  - Routers might be configured not to forward IP packets containing ICMP messages
  - A firewall on the path might filter out ICMP messages
  - A Personal Firewall on the local host or target host might filter out ICMP messages
Traceroute

- Shows the (likely) path (or route) to the target host
  - Shows routers traversed by packets traveling from local host to target host
  - IP address or domain name of one interface of each router is shown
    - Not necessary the interface having received or forwarded the packet

Syntax

- traceroute [options] target (UNIX)
- tracert [options] target (Windows)

Traceroute Output Example

```
traceroute to library.airnews.net (206.66.12.202), 30 hops max, 40 byte packets
1  rbrt3 (208.225.64.50)  4.867 ms  4.893 ms  3.449 ms
2  519.Hssi2-0-0.GW1.EWR1.ALTER.NET (157.130.0.17)  6.918 ms  8.721 ms  16.476 ms
3  113.ATM3-0.XR2.EWR1.ALTER.NET (146.188.176.38)  6.323 ms  6.123 ms  7.011 ms
4  192.ATM2-0.TR2.EWR1.ALTER.NET (146.188.176.82)  6.955 ms  15.400 ms  6.684 ms
5  105.ATM6-0.TR2.DFW4.ALTER.NET (146.188.136.245)  49.105 ms  49.921 ms  47.371 ms
6  298.ATM7-0.XR2.DFW4.ALTER.NET (146.188.240.77)  48.162 ms  48.052 ms  47.565 ms
7  194.ATM9-0-0.GW1.DFW1.ALTER.NET (146.188.240.45)  47.886 ms  47.380 ms  50.690 ms
8  iadfw3-gw.customer.ALTER.NET (137.39.138.74)  69.827 ms  68.112 ms  66.859 ms
9  library.airnews.net (206.66.12.202)  174.853 ms  163.945 ms  147.501 ms
```

Round-trip time (RTT): time elapsed from the transmission of an ICMP Echo Request to the reception of the corresponding ICMP Time Exceeded message; it provides a very loose measure of the travel time between local host and each router. Sometimes travel time changes significantly in the course of a few seconds due to temporary congestion of routers.

Traceroute Working Principle

1. Local host sends an ICMP Echo Request message in IP packet with TTL = 1
2. First router (default gateway) decrements TTL and discards IP packet and reacts sending ICMP TTL Exceeded in Transit
3. Local host receives ICMP TTL Exceeded in Transit and from source address of encapsulating IP packet learns one IP address of first router
   - Specific interface depends on router implementation
   - Might be interface through which IP packet was sent
4. Local host sends another ICMP Echo Request message in IP packet with incremented TTL (TTL = 2)
5. Default gateway forwards IP packet decrementing TTL (=1)
6. Second router on the path decrements TTL and discards IP packet and reacts sending ICMP TTL Exceeded in Transit

Some Unix implementations send a UDP message rather than an ICMP Echo Request message
### Traceroute Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f TTL</td>
<td>TTL used as initial value for Time To Live field in first IP packet rather than the default 1.</td>
</tr>
<tr>
<td>-l</td>
<td>Uses ICMP Echo Request messages rather than UDP messages (UNIX only).</td>
</tr>
<tr>
<td>-p port</td>
<td>Generates UDP messages to port destination port rather than default 35434 (UNIX only).</td>
</tr>
<tr>
<td>-m count</td>
<td>Uses count as the maximum value for the Time To Live field rather than the default 30.</td>
</tr>
<tr>
<td>-w timeout</td>
<td>A reply is waited for at most timeout milliseconds; if a later reply is ignored.</td>
</tr>
<tr>
<td>-q count</td>
<td>count test messages are generated for each value of the Time To Live field (default is three).</td>
</tr>
</tbody>
</table>

### arp

- Shows and modifies ARP cache content

**Syntax**

```
arp [options] [IPAddr] [EthAddr]
```

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Shows the current ARP cache content highlighting static and dynamic entries.</td>
</tr>
<tr>
<td>-d IPAddr</td>
<td>Eliminates from ARP cache MAC address mapping corresponding to host IPAddr.</td>
</tr>
<tr>
<td>-s IPAddr EthAddr</td>
<td>Adds static mapping between network address IPAddr and data-link address EthAddr.</td>
</tr>
</tbody>
</table>

### arp Sample Output

```
C:\>arp -a

Interface: 130.192.16.81 --- 0x30004

Internet Address Physical Address Type
130.192.16.17 00-e0-63-13-7e-01 dynamic
130.192.16.36 00-10-4b-35-f2-fa dynamic
```
netstat

- Shows main network parameters

**Syntax:**

```
netstat [options]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no param.]</td>
<td>Lists active layer 4 connections and sessions.</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>Lists active layer 4 connections and sessions, as well as TCP or UDP servers on the local host.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Shows per-protocol (layer 3 and 4) statistics.</td>
</tr>
<tr>
<td><code>+</code></td>
<td>Displays IP routing table.</td>
</tr>
</tbody>
</table>

### netstat Output Example

```
C:\>netstat -a
Active Connections
```

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>localhost:80</td>
<td>truciolo:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>truciolo:80</td>
<td>localhost:0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>truciolo:2747</td>
<td>localhost:2748</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>truciolo:2747</td>
<td>localhost:2748</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>UDP</td>
<td>microsoft-ds</td>
<td>truciolo:*</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>isakmp</td>
<td>truciolo:*</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>1030</td>
<td>localhost:*</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>3456</td>
<td>localhost:*</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>3456</td>
<td>localhost:*</td>
<td></td>
</tr>
</tbody>
</table>

### netstat Output Example

```
C:\>netstat -r
Route Table
```

```
Interface List
0x1 ....................
.00 10 4b 35 f2 fa.... 3Com EtherLink PCI
```

```
Active Routes:
```

<table>
<thead>
<tr>
<th>Network Destination</th>
<th>Network Mask</th>
<th>Gateway</th>
<th>Interface Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>100.192.3.0</td>
<td>255.255.255.0</td>
<td>130.192.28.4</td>
<td>130.192.28.4</td>
</tr>
<tr>
<td>100.192.28.4</td>
<td>255.255.255.255</td>
<td>130.192.28.4</td>
<td>130.192.28.4</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>130.192.28.4</td>
<td>130.192.28.4</td>
<td>130.192.28.4</td>
</tr>
</tbody>
</table>

```
Persistent Routes:
None
```
netstat Output Example

```
C:\>netstat -s
IPv4 Statistics

Packets Received = 177621
2191 received header errors
650093 received address errors
Datagrams forwarded = 0
Datagrams unreachables = 0
Datagrams redirects = 0
Datagrams fragments = 0
Unknown protocol packets received = 0
Received packets discarded = 0
Received packets delivered = 177619

Datagrams forwarded = 0
Routings discarded = 0
Output packets discarded = 0
Output packets delivered = 177619
Reassembly successful = 0
Reassembly required = 0
Reassembly fragmented = 0
Datagrams successfully fragmented = 0
Datagrams failed fragmentation = 0
Fragments created = 0

ICMPv4 Statistics

Received Sent
Messages 124 6
Errors 0 0
Protocol unreachable 171 476
Port unreachable 0 0
Time exceeded 0 0
Address unreachable 371 476
Source quench 0 0
Redirects 0 0
Echoes 555 49
Echo replies 168 5
Timestamps 0 0
Timestamp replies 0 0
Address masks 0 0
Address mask replies 0 0

TCP Statistics for IPv4

Active Open = 8743
Passive Open = 728
New Syn Retransmits = 403
Reteule Counters = 1520
Estab. Counters = 1520
Unk. Counters = 1520

UDP Statistics for IPv4

Active Open = 8743
Passive Open = 728
New Syn Retransmits = 403
Reteule Counters = 1520
Estab. Counters = 1520
Unk. Counters = 1520
```

route

```
route
Displays and modifies IP routing table
Syntax:
route [options] [command] [parameters]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>print</td>
<td>Displays routing table, equivalent to <code>netstat -r</code>.</td>
</tr>
<tr>
<td>add NetAddr mask Gateway</td>
<td>Adds route for network NetAddr/NetMask (e.g., 10.0.0.0/255.255.255.0) through next hop Gateway.</td>
</tr>
<tr>
<td>delete NetAddr mask Gateway</td>
<td>Removes route for network NetAddr/NetMask (e.g., 10.0.0.0/255.255.255.0) through next hop Gateway.</td>
</tr>
</tbody>
</table>
```
ipconfig
 Displays and modifies some of the IP stack parameters.
 Syntax:
 ipconfig [options]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no param.]</td>
<td>Displays main TCP/IP configuration data (addresses, netmask, default gateway, DNS server).</td>
</tr>
<tr>
<td>/all</td>
<td>Displays all TCP/IP configuration data (addresses, netmask, default gateway, DNS server, lease time for DHCP assigned addresses).</td>
</tr>
<tr>
<td>/displaydns</td>
<td>Displays local host DNS cache.</td>
</tr>
<tr>
<td>/flushdns</td>
<td>Flushes local host DNS cache.</td>
</tr>
</tbody>
</table>

ipconfig Output Example

```plaintext
C:>ipconfig
Windows IP Configuration

Ethereal adapter Local Area Connection:

Connection-specific DNS Suffix .
IP Address . . . . . . . . . . . . : 130.192.16.81
Subnet Mask . . . . . . . . . . . : 255.255.255.0
IP Address . . . . . . . . . . . . : fe80::20b:dbff:fe14:50bb%8
Default Gateway . . . . . . . . : 130.192.16.17

fe80::207:ebff:fe7e:c60%8

DNS Servers . . . . . . . . . . .: 130.192.3.21
  130.192.3.26
  fe80::0:0:111
  fe80::0:0:212
  fe80::0:0:313
```

ipconfig Output Example

```plaintext
C:>ipconfig /all
Windows IP Configuration

Host Name . . . . . . . . . . . . : truciolo
Primary DNS Suffix . . . . . . . :
Node Type . . . . . . . . . . . . : Hybrid
IP Routing Enabled . . . . . . : No
WINS Proxy Enabled . . . . . . : No

Ethereal adapter Local Area Connection:

Connection-specific DNS Suffix .
IP Address . . . . . . . . . . . . : 130.192.16.81
Subnet Mask . . . . . . . . . . . : 255.255.255.0
IP Address . . . . . . . . . . . . : fe80::20b:dbff:fe14:50bb%8
Default Gateway . . . . . . . . : 130.192.16.17

fe80::207:ebff:fe7e:c60%8

DNS Servers . . . . . . . . . . .: 130.192.3.21
  130.192.3.26
  fe80::0:0:111
  fe80::0:0:212
  fe80::0:0:313
```
### ipconfig Output Example

```plaintext
C:\>ipconfig /displaydns
Windows IP Configuration

--------------------------------------------------
Record Name ........: www.polito.it
Record Type ........: 5
Time To Live ........: 86398
Data Length ..........: 4
Section .............: Answer
CNAME Record .......: web01.polito.it

--------------------------------------------------
Record Name ........: localhost
Record Type ........: 1
Time To Live ........: 0
Data Length ..........: 4
Section .............: Answer
A (Host) Record ....: 127.0.0.1

--------------------------------------------------
```