Mac TCP Watcher v2.0

1993-96 Peter N Lewis & Stairways Software Pty Ltd

This program is $10 shareware.

Features

Open Transport Native.
PowerPC Native.
Compatible with Classic MacTCP.
Provides internal TCP information.
DNS, UDP, TCP and Ping tests.
Traceroute function.
Balloon Help.

Contents

What Mac TCP Watcher Does

Mac TCP Watcher displays the internals of MacTCP or Open Transport, including a list of all the current TCP connections and information relating to these connections. Mac TCP Watcher reports as many errors as possible so it can be used to test your TCP setup.

Mac TCP Watcher can test by sending UDP and TCP echos, and ICMP Ping packets. The echo tests require a nice unix box to support the echo ports, so to get around this, Mac TCP Watcher has a UDP and TCP echo port server, so you can test it to yourself, as well as to other Macs running Mac TCP Watcher. There is a function to test your DNS. Finally Mac TCP Watcher has a Traceroute function which lets you determine the path your TCP packets are taking to a given destination.

Note: DNS means Domain Name System, it is the service that converts names (like www.stairways.com) and converts them into IP numbers (like 205.199.66.216), or vice versa (enter 205.199.66.216 and get www.share.com).

This documentation describes in some detail tests you can do on your TCP/IP stack. On the Macintosh the two most widely used TCP/IP stacks are MacTCP and Open Transport. Open Transport is the newer and more 'robust' of the two. Throughout this document both MacTCP and Open Transport TCP/IP code is referred to as your 'TCP stack' and your MacTCP control panel or TCP/IP control panel is referred to as your 'TCP control panel'.

Using Mac TCP Watcher

When you run Mac TCP Watcher, the first window which pops up is the TCP Info window. This contains TCP information and a series of buttons which are tests you can run. Most of the fields are self explanatory, but some additional detail is given in the section below 'The TCP Info window'.

All the statistics displayed in the TCP Info window are accumulated since the TCP stack was initialised, **not** from when Mac TCP Watcher was started. Thus if you quit and start Mac TCP Watcher again, none of the connection or transmission numbers should have decreased.

The tests (Ping, UDP, TCP, DNS and Trace) all require that you enter either the machine name or IP number of a machine. By default Mac TCP Watcher fills in the IP number of your Macintosh.

The TCP Info Window

Mac Name : This is the DNS name. If the Mac doesn't have a valid DNS name, Mac TCP Watcher will complain when it is launched. If you have to deal with a lot of Macs with this problem, you may want to disable this feature. You can do this by changing the STR# 900 string from "Report" to anything else.
Mac IP : The IP number of your Macintosh. This number is read from your TCP control panel.

Connections : The number of active TCP connections.
Attempts , **Opened** : The number of connections which were attempted, and successfully opened.
Accepted : The number of accepted incoming connections.
Closed : The number of connections successfully closed.
Aborted : The number of connections successfully aborted.

Received , **Duplicates** , **Sent** , **Retransmitted** : Are the number of bytes (or, in brackets, the number of packets) which were Received and Sent, plus how many packets had to be Retransmitted and how many packets were Duplicates of packets already received.

RTO Min , **RTO Max** : The minimum and maximum time between retransmitted packets.

Ping, UDP and TCP

Ping and UDP tests do similar things: they send out packets which are echoed back to your machine by the machine which you specify when you start the test. The round trip time is calculated by how long it takes for packets to return. The Ping and UDP displays also show Minimum, Maximum and Average times. All times are in seconds.

Clicking on the 'Continuous' check box makes the Ping or UDP test run until you cancel it. If you hold the Control key down when you activate the Ping or UDP test (whether by clicking on the button in the TCP Info window, using a command key combination or double clicking on an entry in a Traceroute window) then the 'Continuous' checkbox will be activated.

Note that times for the Ping and UDP are not terribly accurate. Times will vary according to the load on your machine and processor speed as well as network activity and network distance. But it *will* tell you if the machines are alive and connected. (Times for Ping on machines running MacTCP should be more accurate. On OT machines Ping, like UDP depends on Mac TCP Watcher polling for the return of the Ping or UDP packet.)

The TCP test makes a TCP connection to a machine, sends a line of text and looks for the response. It depends on there being a TCP echo port on the target machine. Most Unix machines will have one and there is a TCP echo function built into Mac TCP Watcher, so you can test against your own machine or other Macintoshes running Mac TCP Watcher. This is a simple success/failure test.

Note: MacTCP appears to have a bug (surprise!) that makes the Pings fail to return from your own machine. This happens on some machines and not others. I've tested it the Apple's own MPing program, and the same thing happens. If all the Ping packets time out, try using the UDP test instead.

DNS

DNS stands for Domain Name Server. If you have things properly configured and your Internet Service Provider (ISP) is properly configured you should be able to enter DNS names (like www.stairways.com) and convert them into IP numbers (like 205.199.66.216), or vice versa (enter 205.199.66.216 and get www.share.com).

If this does not work, or it only works part of the time, you probably do not have your Mac's DNS set up correctly. For more information you should read Eric Behr's Mac TCP Info document. (Included in the Mac TCP Watcher distribution, also available at: <http://www.math.niu.edu/~behr/Comp/mactcp.html>)

Traceroute

Traceroute is a very useful function for analysing network behaviour. It determines the path that your TCP packets take to a given destination (you enter the destination at the start of the test as either an IP number or a DNS name). Note that Traceroute is an OT only function. You cannot use it under MacTCP. (The button greys out under MacTCP.)

The results are fairly straightforward. Here is a completed Traceroute from crazy.peter.com.au to swing.iinet.net.au:

```
Hop  Result  Min    Avg    Max    IP            Name
1    3/3     0.003  0.003  0.003  203.8.112.1   guppy.peter.com.au
2    3/3     0.184  0.192  0.207  139.130.177.2 iinet.gw.au
3    3/3     0.180  0.182  0.185  203.14.168.3  swing.iinet.net.au
```

Note that the originating machine is not displayed.

Hop : Just gives the order in which the TCP packets progress from machine to machine.
Result : Received/Sent packets, or other information (see below).
Min , **Avg** , **Max** : The Minimum, Average and Maximum round trip time in seconds that the packets took to go to and return from that machine.
IP , **Name** : The IP number and name of the remote machine which is conveying your TCP packets.

There are other possible annotations which can appear in the Result column:

!Host , **!Network** , **!Protocol** , **!Port** : A Host, Network, Protocol or Port is unreachable, respectively.
!Frag : Source route failed or fragmentation needed. OT always sets the "don't fragment" bit, so you may get this with some routers that cannot handle the bit being set even if the packet is small enough that it does not need to be fragmented.
!Route : Source Route Failed

?Network , **?Host** : Destination Network or Host unknown. This is a router error.

Isolated : Source host isolated.

XNetwork : Communication with destination network administratively prohibited.

XHost : Communication with destination host administratively prohibited.

TOS Net : Network unreachable for type of service.

TOS Host : Host unreachable for type of service.

!TTL : TTL was very small on the return packet (<=1) so it may indicate that the TTL was incorrectly set on the returning packet. (For a discussion of TTLs, see the section below 'How Traceroute works: TTLs'.)

If you double click on an entry in a Traceroute window, Mac TCP Watcher will run a ping test on that site.

How Traceroute works: TTLs

TTL stands for Time To Live. When a TCP packet is sent a TTL is set, which is the number of routers it can pass through before the packet is killed. As the packet passes through a router the TTL is decremented until, when the TTL reaches zero, the packet is destroyed and a return message is initiated. (This is an ICMP "time exceeded" message.) The return message should have the TTL reset by terminating router.

Traceroute works by setting the TTL for a packet to 1, sending it out, listening for the reply and when it gets it, examining the packet to determine where the packet came from. This machine is one hop away from your machine. Then it sets the TTL to 2 and so on...

Unfortunately not all TCP stacks behave correctly. Some TCP stacks set the TTL for the ICMP "time exceeded" message to that of the message it has just killed. So if the TTL is 0, the packet will be killed by the next machine to which it is passed.

This can have two effects on a traceroute. If the computer is an intermediate machine in the traceroute, the entry will remain blank. No information is returned to the machine conducting the traceroute because the "time exceeded" message never makes it back.

But if the machine you are doing a traceroute to has a misbehaving TCP stack, the return packets won't arrive until the TTL is high enough that it can make both the trip there and back. So Traceroute will show a number of failed connections equal to n (the number of hops the destination machine is away from the machine doing the traceroute) minus 1. For example:

```
1   3/3   0.003  0.004  0.007  203.8.112.1    guppy.peter.com.au
2   3/3   0.184  0.193  0.198  139.130.177.2  iinet.gw.au
3   2/3   0.195  0.237  0.279  203.14.168.3   swing.iinet.net.au
4   3/3   0.183  0.297  0.370  130.95.97.1    muchacho.connections.uwa.edu.au
5   3/3   0.179  0.274  0.322  130.95.128.16  hacienda.uwa.edu.au
6   0/3
7   0/3
8   0/3
9   0/3
10  0/3
11  !TTL  0.194  0.218  0.261  130.95.1.150   redback.cs.uwa.oz.au
```

Entries 6-10 are blank because redback has set the TTL incorrectly. Redback is actually 6 hops away, but it shows n-1 too many entries in Traceroute.

Machines running MacTCP display this bug. (Redback.cs.uwa.oz.au, listed above, runs MacTCP.) Open Transport handles TTL correctly. The original distributions of 4.3 BSD had this error, so some varieties of Unix machine will display the problem.

The times in traceroute are total round trip times in seconds. The Min/Avg/Max should increase from machine n to machine n+1, but they may not, for a variety of reasons.

To start with the times are based on the number of tests listed in the results column (typically 3 for a completed traceroute). The times for these tests can vary depending on network usage. So if the network is under heavy load when you are testing a machine 4 hops away and slackens when you start testing a machine 5 hops away, the time for machine 5 may be lower than the time for machine 4, despite the fact that it has taken a longer physical path.

Second, returning a "time exceeded" message requires more computational time than routing a packet onwards. So if machine 4 is under heavy load when it is being probed by traceroute, while machine 5 is not, the times for machine 4 may be higher than the times for machine 5. This is probably the case in the above example: machine 4 (muchacho.connections.uwa.edu.au) is heavily loaded, while machines 5 and "11" (hacienda.uwa.edu.au and redback.cs.uwa.oz.au) are less loaded, so they return the "time exceeded" message faster.

Finally, packet paths may not be the same coming and going. If the return path from machine 5 does not trace back through machine 4 the time for machine 5 is partially independent of the time for machine 4.

Testing With Mac TCP Watcher

To test your TCP/IP setup on your Mac, try following the procedure outlined below. Networks build upon basic functions: the sequence outlined below tries to test the most basic functions first and then tests succesive layers of your network. If your Mac passes all the tests you can be pretty confident you have your TCP stack configured correctly.

A) IP number Configuration.

1. Launch Mac TCP Watcher.
2. Note the IP number at the top left (Mac IP).
3. Test the ICMP by clicking the Ping button, and typing in the IP number of your Macintosh. Your Mac will Ping itself. If you are using MacTCP and the Ping test fails, try the UDP test. It may just be the bug in MacTCP described above (in 'How Traceroute works: TTLs').

If any of these fail, your TCP is most probably badly configured:

Check the configuration in the MacTCP or TCP/IP Control Panel (your TCP control panel). If it looks ok and you are running MacTCP, then reinstall MacTCP by deleting MacTCP, MacTCP Prep, and MacTCP DNR from all folders in the System Folder (ie, the System Folder, Preferences, Control Panels, and Extensions). Reinstall the control panel from the original disks, and reset the configuration. Reboot. Try again.
If it still fails, you have a problem, try reading Eric Behr's [MacTCP Info document](), included in this package (Thanks Eric!).
If it still fails, you're probably going to have to talk to a local expert (like your ISP's help desk). If you *are* the local expert, you really have a problem.

Try a UDP and TCP test to your Mac's IP. They should work.

B) Network Test

Now, find another machine on the network, as near (network-wise) as you can manage (a Mac running Mac TCP Watcher that passes the above tests will do, a unix machine will also do). Using its IP number, try the Ping test. If that works, try the UDP and TCP tests as well.

Note : Some unix machines do not support the UDP or TCP echo tests. You can see if they support the TCP test by telneting to port 7 on the machine in question: if it connects and echos what you type, it works, and should pass the test. You can telnet to a particular port using NCSA Telnet by entering:

machine.name port_number

eg amug.org 7

...in the Host/Session name of the Open Connection dialog box.

Repeat the above for various machines further away. You can also try the Traceroute test to a far away machine like 204.62.193.2 (amug.org) to see where there are network failures. (Hopefully there won't be any!) Remember that if you enter a Domain Name (like www.stairways.com) you will be, implicitly, testing your DNS.

C) DNS Configuration

Ok, now test your Name Server. Try the DNS Test with a name of a near by machine, it should tell you the IP. Now try again with the IP, it should tell you the name. Repeat for your Mac, and for other names and addresses.

If none of these work, then your Mac's DNS is badly set up. Read Eric's MacTCP Info document.

If the name lookup works (ie, finds the IP address), but the reverse doesn't find the name, this generally indicates a problem with the Domain Name Server itself, ask the administrator of the machine why it fails.

If your Mac passes all these tests then your TCP setup should be fine!

How It Works

Mac TCP Watcher simply calls the MacTCP or Open Transport software, asks it for the information and displays it.

The Ping Test sends ICMP Ping packets, and counts (and matches) the replies. The UDP Test sends UDP echo packets to port 7 and counts (and matches) the replies. The TCP Test connects to the TCP echo port (port 7 again) and sends a line and checks for the response. The DNS Test looks up the IP for the name, or the name for the IP.

Traceroute is described above in 'A Technical Note on TTLs', but if you are interested in more information there is excellent source code for traceroute at:

<http://dev.info.apple.com/ >

Note that Traceroute exploits some features of Open Transport to provide accurate timings. Unfortunately this also means Traceroute functions only on machines running Open Transport.

All tests will accept either names or IP numbers, but obviously if you use a name, you are implicitly testing the DNS.

A server for each of the TCP and UDP echo ports is built in to Mac TCP Watcher, and echos anything sent to them. MacTCP automatically echos the ICMP Ping packets.

Limitations

Mac TCP Watcher requires MacTCP 1.1 or later or Open Transport 1.1 or later, and System 7.0 or later.

Registering

This program is Shareware, which means if you use it, you should send us US$10.

You can register one of two ways: on-line registration using a web browser, or off-line registrating using the Register program.

Our online registration can be found at:

<http://order.kagi.com/?PL >

Or, using the Register program, you need to:

1. Get hold of a copy of the Register program.

2. Run the Register program and fill out the form.

3. Send it to Kagi Shareware.

About 1: Register is distributed with Anarchie 1.6.0 and there is an Anarchie bookmark for Register in the NetPresenz distribution. You can also get Register from the following sites:

<ftp://mirrors.aol.com/pub/peterlewis/ >

<ftp://ftp.share.com/peterlewis/ >

<ftp://ftp.amug.org/pub/peterlewis/ >

<ftp://ftp.HappySize.co.jp//pub/peterlewis/ >

<ftp://redback.cs.uwa.edu.au/Others/PeterLewis/ >

<ftp://sunsite.cnlab-switch.ch/mirror/peterlewis/ >

..or there are download links on the following Web page:

<http://www.stairways.com/register/topay.html >

About 2: You need to enter your name, email, postal address, and the shareware you wish to pay for. The form accepts many different payment methods such as: US Check, Money Order, Cash (in many different currencies), Visa, Mastercard, American Express, First Virtual, and Invoice (to be given to your accounts payable department).

About 3: Then either email the data generated by the registration program or print it and send it via postal mail or fax. Credit card information is encrypted by the Register program.

The address to send the completed form is output by Register when you Print or Copy the completed form. The addresses are:

Email: shareware@kagi.com

FAX: +1 510 652 6589

Snail-mail:

Kagi Shareware

1442-A Walnut Street #392-PL

Berkeley, California, 94709-1405

USA

Site Licensing:

World-Wide Source Code License: US$5000

World-wide license: US$2000

Universities or companies site license: US$500

Curtin University and the University of Western Australia are exempt.

Single-user license: US$10.

Warranty

There is absolutely NO warranty, guarantee, hint, suggestion or anything else that would lead anyone to think that Mac TCP Watcher does anything stated in this documentation. It usually does not destroy data (systems, hardware, etc), and has sometimes worked on our Macs running System 7.5.3. It will probably not work with the 64k ROM. It might work with the other models, but we don't have them all, so we don't know.

If it doesn't work please check out our Website and read the Mac TCP Watcher FAQ:

<http://www.stairways.com/mtcpw/index.html >

..and then mail our support address:

<support@stairways.com.au>

We answer all our E-Mail, so if you don't get a response within a week or so, please mail us again.

Fine Print

Peter Lewis and Stairways Software Pty Ltd hereby disclaims all warranties relating to this software, whether express or implied, including without limitation any implied warranties of merchantability or fitness for a particular purpose. Peter Lewis and Stairways Software Pty Ltd will not be liable for any special, incidental, consequential, indirect or similar damages due to loss of data or any other reason, even if Peter Lewis, Stairways Software Pty Ltd, or an agent of his has been advised of the possibility of such damages. In no event shall Peter Lewis or Stairways Software Pty Ltd be liable for any damages, regardless of the form of the claim. The person using the software bears all risk as to the quality and performance of the software.

US Government :

Government End Users: If you are acquiring the Software and fonts

on behalf of any unit or agency of the United States Government, the

following provisions apply. The Government agrees:

(i) if the Software and fonts are supplied to the Department of

Defense (DoD), the Software and fonts are classified as "Commercial

Computer Software" and the Government is acquiring only "restricted rights"

in the Software, its documentation and fonts as that term is defined in

Clause 252.227-7013(c)(1) of the DFARS; and

(ii) if the Software and fonts are supplied to any unit or agency

of the United States Government other than DoD, the Government's rights in

the Software, its documentation and fonts will be as defined in Clause

52.227-19(c)(2) of the FAR or, in the case of NASA, in Clause

18-52.227-86(d) of the NASA Supplement to the FAR.

Acknowledgements

Thanks to Quinn for his Developer Technical Support for Mac TCP Watcher and thanks to everyone on the net for being a lot of fun!