TCP Test Suite

Testing the Transmission Control Protocol with Maxwell Pro

Design and quality assurance engineer use the Maxwell Pro TCP Test Suite to find and fix bugs in their TCP stack or engine. The tests help ensure a sufficiently robust TCP stack or engine, not vulnerable to the wide range of attacks in today's Internet. The tests make use of the Maxwell Pro network emulation environment, so that each test sequence can intelligently impair all aspects of the TCP protocol.

The TCP Test Suite contains unique test cases that take on parameters for greater coverage. The tests ensure TCP compliance through vulnerability and robustness testing, with tests for both IPv4 and IPv6.

The Maxwell Pro TCP Test Suite can provide you with the customization and flexibility you need to accurately test your implementation and meet your schedules.

What's Inside...

- TCP Options Processing: pg. 2
- TCP Connection: TCP state ESTABLISHED pg. 2
- TCP Connection Close: TCP states FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, LAST-ACK, TIME-WAIT pg. 3
- TCP Client and Server Side Test Coverage pg. 3
- Sample Test Documentation pg. 3
- Possible Behaviors or Outcomes: pg. 4
- Other Areas of Test Coverage pg. 4
- Establishing a source of authority pg. 4

Kings Village Center #66190
Scotts Valley, CA 95067
iwl.com
+1.831.460.7010
info@iwl.com

The tests are grouped into categories as follows:

TCP Connection Setup:

- TCP states CLOSED, LISTEN, SYN-RECEIVED, SYN-SENT.
- Test the ability to handle malformed or illegal sequence and acknowledgment numbers during the remainder of the connection.

TCP Options Processing:

Insertion and modification of options during the TCP connection set up sequences.

- Unknown options with and without length fields
- Illegal options (e.g. bad option number or valid option with invalid size)
- Non zero padding between end of option and end of TCP header
- Zero length options
- Known options with wrong lengths (e.g. max segment size option with length of five)
- Options with very long lengths that fit in the TCP header
- Options with very long lengths that do not fit in the TCP header
- No end-of-option option
- Valid options with illegal and unusual values
- Valid options with values that exercise bit boundary conditions
- Options at various times during the connection
- Valid options on unnatural boundaries
- Break the usual single SYN/ACK into two distinct packets
- Options missing from TCP MSS calculation

TCP Connection: TCP state ESTABLISHED

- Send RST and URG into zero offered window
- Remove push bits
- Split segment into N small segments
- Split segment into N small segments and add a PUSH bit on each small segment
- URG bit plus urgent pointer of zero, 1, maximum-1 and maximum value
- Urgent pointer with non-zero value but URG bit not set
- Sequence of segments/packets with URG with the urgent pointer in each successive packet pointing to a lower sequence number
- Premature use of socket pair and initial sequence number
- Exercise slow start at connection startup
- Trigger congestive Testing TCP Congestion Avoidance backoff by delaying (or dropping) packets or ACK flags
- After triggering congestive backoff, discard or delay first/second/third segments
- Insert ECN bit into IP underneath TCP connection
- Put connection startup options into TCP packets during connection (and shutdown phases)

- Vary the offered window sizes to check for boundary conditions
- Vary the offered window size to be odd numbers
- Offset the sequence number space to exercise wrap arithmetic
- Memorize and replay segments/packets beyond normally expected times.
- Rapidly change the offered window (including zero window and maximum window)

TCP Connection Close: TCP states FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, LAST-ACK, TIME-WAIT

- Add options to the shutdown packets
- Throw a SYN or SYN/ACK where the FIN/ACK is expected
- Break FIN/ACK into two distinct packets, one with ACK and the other with FIN
- Send data into a half closed connection
- Test the time wait connection duration

TCP Client and Server Side Test Coverage

Maxwell Pro supports BOTH server side and client side TCP testing.

- Server side testing is often possible straight "out of the box" with no programming needed. Client side testing is almost as simple, only requiring that one compile a dual client-server program to run on the target test machine. IWL provides the source code for this program in ANSI C which uses the POSIX.1-2001 socket API to virtually eliminate or minimize porting issues.
- After the initial connection handshake, the TCP state transition possibilities become identical for the client and server side. Thus, only a small fraction of any tests from any supplier are relevant to those state changes. The Maxwell Pro TCP tests provide 100% state diagram coverage, and over 80% of it can often be tested with no extra porting or programming effort.

Sample Test Documentation

Purpose of the Test: Impairment to handle no end-of-option option

Impairment Algorithm:

1. Maxwell Pro will detect the start of a TCP connection between Device A and Device B.

2. Maxwell Pro will intercept a TCP packet flowing from Device A to Device B that contains an option. (Several variations include: modifying only packets during the initial three way handshake, during the data transfer phase, and during the connection termination handshake.)

3. Maxwell will change the contents of the packet so that option zero (meaning end of option list is removed) and replaced with an illegal value.

Possible Behaviors or Outcomes:

The TCP stack in Device B may hang while waiting for the (non-existent) end of option value. Device B may time-out. Device B may accept the options.The TCP Test Suite is used by design engineers, quality assurance engineers and testers to find and fix bugs in their TCP stack or engine. The tests help ensure that the TCP stack is sufficiently robust so that it is not vulnerable to the wide range of attacks in today's Internet. The tests make use of the Maxwell Pro network emulation environment, so that each test sequence can intelligently impair all aspects of the TCP protocol.

Other Areas of Test Coverage

- The user may control several aspects of IPv4 fragmentation, such as the MTU (fragment size), fragment overlap, and fragment order. This permits most of the tests to be expanded for more test coverage.
- Reaction to changes in network characteristics (e.g. congestion)
- Sequence Number Arithmetic
- Changing of IP addresses, MAC addresses, and routes underneath the TCP connection

Establishing a source of authority

The Maxwell Pro TCP Test Suite references the RFCs that correlate to each test area. These official IETF documents detail the Internet standards and best current practices that can point the user toward a better understanding of the problem.

RFCs Referenced

- RFC 2018 TCP Selective Acknowledgement Options
- RFC 2001 TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms
- RFC 793 Transmission Control Protocol (TCP)
- RFC 1122 Requirements for Internet Hosts -- Communication Layers
- RFC 1323 TCP Extensions for High Performance
- RFC 5681 TCP Congestion Control

Want to learn more?

IWL
Kings Village Center #66190
Scotts Valley, CA 95067
iwl.com
+1.831.460.7010
info@iwl.com