Test your IPv4 and IPv6 Stack

The Maxwell Pro IP Test Suite is used by design engineers, quality assurance engineers and testers to find and fix bugs in their IP stack or engine. The tests help ensure that the IP 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 IP protocol.

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

What's Inside:

The Maxwell Pro IP Test Suite provides the customization and flexibility required to accurately test your implementation and meet your schedules.For IPv4 and IPv6 testing, Maxwell Pro provides many customization and optimization features for very thorough testing. This includes:

- User control of 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

IPv4 Datagram tests:

Here is a summary of some of the areas covered in the IPv4 datagram tests:

- Set protocol field to a value not yet assigned by IANA.
- Set total length field to zero.
- Set total length field to maximum size.
- Set IHL and total length fields so that header goes past end of datagram.
- Destination address is set to the loopback '127.0.0.1' address.
- Destination address is set to '0.0.0.0' broadcast address.
- Destination address is set to '255.255.255.255' broadcast address.
- Source address is set to the '0.0.0.0' broadcast address.
- Source address is set to the loopback '127.0.0.1' address.
- Protocol field is 200 (unassigned) and source address is a broadcast address.
- Protocol field is 200 (unassigned) and source address is a loopback address.
- TTL field is zero and source address is a broadcast address.
- Datagram is truncated so protocol field indicates another protocol follows, but none does.
- IPv4 version field set to value other than 4.
- Adjust header so checksum is -0 and set checksum field to -0.
- Adjust header so checksum is -0 and set checksum field to +0.
- Adjust header so checksum is +1 and set checksum field to +0.
- Verify processing of TTL field.
- Change ICMPv4 destination address to '224.0.0.1' multicast address.
- Check for continuous dead gateway detection pinging.
- Check for dead gateway detection pinging while traffic being sent.
- Verify link layer broadcasts with specific addresses are discarded.
- Verify that ICMPv4 host and net redirects are treated the same.

IPv6 Datagram tests:

Here is a summary of some of the areas covered in the IPv6 datagram tests:

- Duplicate datagram header.
- Datagram's next header field set to a value not yet assigned by IANA.
- Datagram payload length is zero.
- Datagram payload length is set to different values, up to maximum size.
- Destination address is not the DUT's, such as the unspecified '::' address, loopback '::1', multicast 'FF00::', and so on.
- Source address is not the test machine's address, such as the unspecified address, loopback, multicast, and so on.
- The "next header" is 200 (unassigned) and source address is unspecified, loopback, a multicast, and so on.
- Hop count is zero and source address is unspecified, loopback, multicast, and so on.

IPv4 and IPv6 Fragmentation tests:

- Change fields (such as the option code of the Client Identifier option) to values that have not been assigned by IANA.
- Change field lengths to invalid or unusual values.
- Remove Client Identifier option.
- Remove Server Identifier option.
- Truncate DUID of Client Identifier option to hardware type field.
- Change transaction ID field to 0xffffff.
- Changes the T1 and T2 fields of the IA_NA option to one second in the future.
- Change message type.
- Allow the user to overwrite an 8, 16, or 32-bit value in the packet.
- Allow the user to overwrite an 8, 16, or 32-bit value in a specified DHCP option.

IP Options Processing tests

- Unknown options
- Illegal options
- Zero length options
- Known options with wrong lengths
- Malformed options

IP Framing Tests

- Change frame size to larger than IP datagram
- Substitute jumbo frames for normal frames

Establishing a source of authority

The Maxwell Pro IP 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.

IP RFCs Covered

- RFC 791, Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks
- RFC 1108 U.S. Department of Defense Security Options for the Internet Protocol
- RFC 1122 Requirements for Internet Hosts -- Communication Layers
- RFC 2113 IP Router Alert Option
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2675 IPv6 Jumbograms
- RFC 2711 IPv6 Router Alert Option
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4302 IP Authentication Header
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Sample Test Documentation

Purpose of the Test:

Set Auth Extension Length Past Original Length by 8

What the Test Does:

This test sets the auth extension length field to appear as if it extends at least 8 bytes past the original length. It does not actually add any bytes to the header.

Expected Outcome:

The receiving node should either notice the bad length or fail on the computation of the Integrity Check Value (ICV). If the length is determined to be bad, the receiving node should respond with an ICMP parameter problem message. If the ICV is invalid, the receiving node must silently discard the packet and may make an audit log entry.

Notes:

ICMP rate limiting may prevent a response for every stimulus packet.

References:

- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4302 IP Authentication Header
- RFC 4443 Internet Control Message Protocol (ICMPv6)for the Internet Protocol version 6 (IPv6)