Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. (Source: RFC 2131)

Maxwell Pro DHCP Test Suite

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

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

The tests are grouped into categories as follows:

IPv4 DHCP Client (packets from DHCP client to DHCP server)

- Change fields (such as hardware type) to values that have not been assigned by IANA.
- Set field lengths (such as hardware address length) to invalid values.
- Set time values to the maximum.
- Force "must be zero" fields and flags to be non-zero.
- Change various IP address fields to contain invalid values such as broadcast (255.255.255.255) and localhost (127.0.0.1).
- Change hardware address fields to invalid values.
- Change host name and boot file name to invalid, non-null-terminated values.
- Set the magic cookie bytes to an incorrect value.
- 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.

IPv4 DHCP Server (packets from DHCP server to DHCP client)

- Change fields (such as hardware type) to values that have not been assigned by IANA.
- Set field lengths (such as hardware address length) to invalid values.
- Set time values to the maximum.
- Force "must be zero" fields and flags to be non-zero.
- Change various IP address fields to contain invalid values such as broadcast (255.255.255.255) and localhost (127.0.0.1).
- Change hardware address fields to invalid values.
- Change host name and boot file name to invalid, non-null-terminated values.
- Set the magic cookie bytes to an incorrect value.
- 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.

IPv6 DHCP Client (packets from DHCP client to DHCP server)

- 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.

IPv6 DHCP Server (packets from DHCP server to DHCP client)

- 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.

Establishing a source of authority

The Maxwell Pro TCP/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.

RFCs Referenced

- RFC 2131 Dynamic Host Configuration Protocol
- RFC 2132 DHCP Options and BOOTP Vendor Extensions

Sample Test Documentation

Test documentation follows the format below:

- Purpose of the Test:
- Impairment Algorithm:
- Possible Behaviors or Outcomes:

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