EDSA-402
ISA Security Compliance Institute – Embedded Device Security Assurance –
Testing the robustness of implementations of the IETF ARP protocol over IPv4

Version 2.31

September 2010

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”)provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SPECIFICATION.

WITHOUT LIMITING THE FOREGOING, ASCI DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THIS SPECIFICATION ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE SPECIFICATION AVAILABLE, ASCI IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS ASCI UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE. ANYONE USING THIS SPECIFICATION SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ASCI OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL,PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OFPRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SPECIFICATION, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SPECIFICATION OR OTHERWISE ARISING OUT OF THE USE OF THE SPECIFICATION, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS SPECIFICATION, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF ASCI OR ANY SUPPLIER, AND EVEN IF ASCI OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Revision history

Version	Date	Changes
2.1	2010.06.15	Initial version published to http://www.ISASecure.org
2.31	2010.09.28	Create distinct test criteria at high but supported rate and full auto-negotiated link rate; removed protocol conformance aspects of tests (removing 2 tests) since covered by other industry efforts; removed discovery phase since not required to perform uniform testing over all devices; removed mixing of valid and invalid messages in load testing since valid messages create more load on device

Contents

Foreword

NOTE This is one of a series of robustness test specifications for embedded devices. The full current list of documents related to embedded device security assurance can be found on the web site of the ISA Security Compliance Institute, http://www.ISASecure.org.

1 Scope

This document is intended to provide requirements for testing the robustness of embedded device implementations of the IETF ARP protocol, as a measure of the extent to which such implementations defend themselves against

- correctly formed messages and sequences of such messages;
- single erroneous messages; and
- inappropriate sequences of messages;

where failure of the device to continue to provide concurrent automation system control and reporting functions demonstrates potential security vulnerabilities within the device. This document is not intended to serve as a guide for testing the correctness of implementations or conformance to mandatory provisions of the controlling standard(s), which cannot be determined solely by observing a device's response to external stimuli.

NOTE 1 The ARP protocol is stateless, while the ARP translation table+cache contains state information resulting from temporal and transaction processing.

NOTE 2 Although conformance is explicitly NOT a goal of this testing, prior versions of this document included some aspects of conformance testing which have now intentionally been removed.

2 Normative references

This associated specification contains requirements common to this and similar robustness tests for other protocols for embedded devices, including requirements on test configurations.

[EDSA-310] *ISA Security Compliance Institute – Embedded device security assurance – Common requirements for communication robustness testing of IP-based protocol implementations*[1], as specified at http://www.ISASecure.org

NOTE 1 Within this document, references to specific subclauses of this normative reference are made through symbolic tags of the form [CRT.Symbolic_tag]; the resolution of those tags is made in [EDSA-310], Table 1.

These publications of the Internet Engineering Task Force (IETF) are the controlling specifications for the protocol whose robustness testing is the subject of this document:

NOTE 2 For each RFC*nnn*, the controlling version can be found at http://tools.ietf.org/html/rfc*nnn*.

RFC791, *Internet protocol [version 4]*

RFC826, *An Ethernet address resolution protocol*

RFC894, *A standard for the transmission of IP datagrams over Ethernet networks*

RFC1042, *A standard for the transmission of IP datagrams over IEEE 802 networks*

RFC1122, *Requirements for Internet hosts – Communication layers*

NOTE 3 Only 2.3.2 is referenced.

RFC5494, *IANA allocation guidelines for the address resolution protocol (ARP)*

NOTE 4 Other IETF specifications related to the above can be found in the Bibliography.

[1] to be published concurrently with this document

3 Definitions and abbreviations

3.1 Definitions

3.1.1
cache
ARP translation table+cache, consisting of statically managed table entries and dynamically entered, updated and deleted cache entries

NOTE See RFC 1122, 2.3.1.

3.1.2
device under test
device that is being stimulated and observed during testing to demonstrate the characteristics and behavior of the device when presented with the selected sequence of test stimuli

3.1.3
erroneous (message or PDU or option)
PDU that violates either syntactic rules on PDU structure or semantic rules on PDU content or both, or PDU option that violates either syntactic rules on PDU option structure or semantic rules on PDU option content or both

NOTE 1 Semantic and syntactic rule violations can interact, as when the value of one field determines the size of another field.

NOTE 2 The term erroneous includes syntactic malformation, semantically invalid values, and contextually invalid values and sequences

NOTE 3 This is addressed further in [CRT.Terminology_of_Erroneous].

3.1.4
“Ethernet”
either the IETF Ethernet II protocol or IEEE 802 SNAP over IEEE 802.2 Type 1 LLC over IEEE 802.3

3.1.5
inferior (protocol)
protocol at a lower layer or sublayer than the referenced protocol

3.1.6
lower tester
tester that controls and observes a protocol layer implementation in a DUT through stimulus and observation via lower protocol layers and a physical interconnection to the TD

NOTE This is the only type of testing used in the ISCI EDSA robustness tests.

3.1.7
malformed (message or PDU)
PDU that violates syntactic rules on PDU structure

NOTE This is addressed further in [CRT.Terminology_of_Erroneous].

3.1.8
superior (protocol)
protocol at a higher layer or sublayer than the referenced protocol

3.1.9
testing device
conceptual single network-connected device, possibly consisting of multiple physical network-connected devices, used to test the robustness of the device under test

NOTE This could be any programmable network-connected device capable of processing PDUs at the rate required for testing.

3.1.10
translation table+cache
database of entries consisting of (protocol type, sender protocol address, sender hardware address, statically-managed-flag) used by ARP to resolve a given network layer protocol address to a hardware MAC address

NOTE See RFC 826, “Packet Reception”.

3.1.11
upper tester
tester that controls and observes a protocol layer implementation in a DUT through stimulus and observation via a DUT-internal service interface between test software and the protocol layer under test

3.1.12
vulnerability
flaw or weakness in a system's design, implementation, operation, or management that could be exploited to violate the system’s integrity or security policy

3.2 Abbreviations

The following abbreviations are used in this document:

ARP	address resolution protocol
CRT	communication robustness testing
DL	data-link layer
DPDU	data-link-layer protocol data unit
DUT	device under test
IANA	Internet assigned numbers authority
ICMP	Internet control message protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet engineering task force
IP	Internet (network layer) protocol
IPv4	IP version 4 (uses 32-bit network layer addresses)
LRU	least recently used
MAC	medium access control / media access control (when multiple media are involved)
MAC frame	MAC-sublayer protocol data unit
(*N*)PDU	(*N*-layer) protocol data unit, where *N* = MAC (medium access control), D (data-link), N (network), T (transport), A (application), etc
NPDU	network-layer protocol data unit
SNAP	sub-network access protocol
SHA	source hardware address
SPA	source protocol address
TD	testing device
THA	target hardware address
TPA	target protocol address

4 Elements of the protocol under test

4.1 General

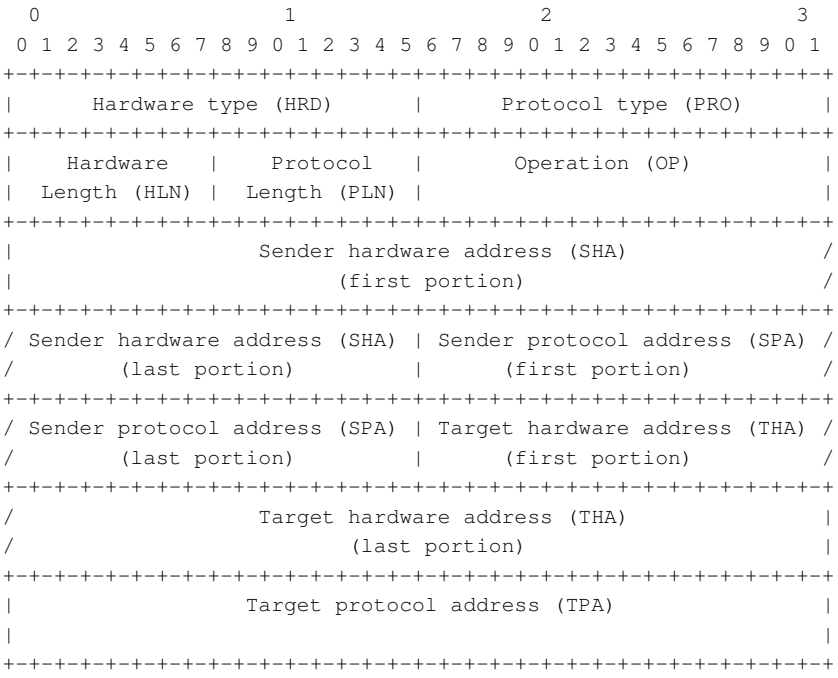
This document specifies robustness testing for the IETF ARP protocol, which is a stateless data-link layer protocol providing a method for discovering a host's link layer address, given an IPv4 network address.

NOTE IPv6 uses a different, related protocol called Neighbor Discovery (RFC2461) for address discovery and resolution.

4.2 ARP DPDUs

4.2.1 ARP DPDU structure

An ARP DPDU is structured as shown in Figure 1 with IPv4 as the Network Layer and IEEE 802 hardware addresses, using a big-endian octet order.



NOTE The above address length fields are parameterized for alternate protocols

Figure 1 – Generic ARP DPDU structure, shown for 6 B IEEE 802 and 4 B IPv4 addressing

4.2.2 Mandatory fields

The following fields are mandatory components of each ARP DPDU (where field sizes are specified in octets (B) or bits (b)):

a) Hardware type (HRD) (2 B): type of hardware for which the "Ethernet" MAC address is to be mapped; default value=0x0001 for "Ethernet". See IANA ARP parameters (Hardware Type) as specified at http://www.iana.org/assignments/arp-parameters/.

b) Protocol type (PRO) (2 B): type of network layer protocol address provided in Sender protocol address (spa), typical=0x0800 for IPv4. See IANA Ethernet numbers, as specified at http://www.iana.org/assignments/ethernet-numbers.

c) Hardware length (HLN) (1 B): hardware MAC address length in octets, for "Ethernet", HLN = 6.

d) Protocol length (PLN) (1B): protocol address length in octets. For IPv4, PLN = 4.

e) Operation (OP) (2B): type of operation being performed, either request (0x0001) or reply (0x0002). See IANA ARP parameters (Operation Code), as specified at http://www.iana.org/assignments/arp-parameters/.

f) Sender hardware address (SHA) (HLN B): hardware link layer address of the host sending the ARP request or reply DPDU. This is the same as the source “Ethernet” MAC address in the Ethernet header.

g) Sender protocol address (SPA) (PLN B): the network layer address for the indicated protocol type of the host sending the ARP request or reply DPDU. For IP, this is the IP address of the sending host.

h) Target hardware address (THA) (HLN B): hardware link layer address of the host receiving the ARP request or reply DPDU. This is the same as the destination “Ethernet” MAC address in the Ethernet header.

i) Target protocol address (TPA) (PLN B): the network layer address for the indicated protocol type of the host receiving the ARP Request or reply. In an ARP Request DPDU this field is ignored. For IP, this is the IP address of the receiving host.

4.2.3 Mandatory protocol aspects

4.2.3.1 Conveying MAC frame

ARP fixes the value for one field of any conveying “Ethernet” or Ethernet SNAP MAC frame.

- For IPv4, the ARP protocol SHALL be specified in the Ethertype field:
  - Ethertype type (2 B): 0x0806 (ARP)

4.2.4 Optional MAC components and elements of procedure

An ARP DPDU may be sent with the “Ethernet” MAC header destination address field set to the appropriate form of the broadcast address, as determined by the sending host routing table. Such behavior is typical when a host sends an initial ARP request DPDU, since the sending host ARP translation table+cache has no entry to map the specified target protocol address.

NOTE Follow-up unicast ARP request DPDUs may be sent to the last-known MAC address of an IP address in the ARP cache, as a means of validating that the cached {MAC address, IP address} association remains valid.

For an ARP reply DPDU, the “Ethernet” MAC header destination address is typically a unicast address. A receiving host SHOULD ignore an ARP reply DPDU with a broadcast address in the destination address field of its “Ethernet” MAC frame.

4.3 Mandatory and optional protocol features

The mandatory features of the ARP protocol are:

M1) The DL is required to perform address resolution when a PDU is passed from the Network Layer on a sending host, in order to convert the given Network Layer target protocol address to the target host MAC address required in the DPDU header. If the target protocol address is unable to be resolved, then the sending host SHALL create an ARP Request DPDU which it then transmits after setting the “Ethernet” DPDU’s Ethertype field to designate the ARP protocol, and setting the DPDU destination address to the broadcast address value, per RFC826, “Packet generation”.

M2) A received ARP DPDU SHALL be discarded without notification whenever the received

a) hardware type does not match the receiving host’s hardware type, or

b) target protocol address does not match any protocol address of the receiving host, or

c) the protocol specified in the ARP DPDU is not supported by the receiving host,

per RFC826, “Packet reception”.

M3) Received ARP DPDUs that are not discarded and contain a (protocol type, protocol address) pair already in the ARP translation cache SHALL cause the matching ARP translation cache entry to be updated with the sender hardware address field in the ARP DPDU, per RFC826, “Packet reception”.

M4) Received ARP DPDUs that are not discarded and contain a (protocol type, protocol address) pair not already in the ARP translation table+cache SHALL cause the ARP translation cache to be updated by adding the (protocol type, protocol address, sender MAC address) triplet, per RFC826, “Packet reception”.

M5) Received ARP DPDUs that have caused the ARP translation cache to be updated and have an ARP DPDU opcode=request SHALL cause an ARP reply DPDU to be created and unicast to the ARP request DPDU’s sender MAC address, after setting the ARP DPDU opcode=reply, obtaining the target MAC address value from the ARP translation table+cache and exchanging the sender and target (MAC, protocol) address pairs, per RFC826, “Packet reception”.

M6) Received ARP DPDUs that have caused the ARP translation cache to be updated and have an ARP DPDU opcode=reply SHALL be discarded without notification, per RFC826, “Packet reception”.

M7) A host SHALL provide a mechanism to prevent ARP flooding (repeatedly sending an ARP request DPDU for the same target protocol address more frequently than one request per target-protocol-address per second), per RFC1122, 2.3.2.1.

M8) A host shall provide a mechanism to flush long-unused entries from the ARP translation cache (also referred to as the “ARP cache”), per RFC1122, 2.3.2.1.

The optional (i.e., conditionally present) features of the ARP protocol are

C1) Any host MAY periodically create and send a unicast ARP request DPDU to a target protocol address currently in the ARP translation cache, for the purpose of validating the target hardware address in the ARP translation cache entry of the sending host, per RFC826, “Related Issue”.

C2) If the host mechanism for flushing out-of-date entries from the ARP translation cache involves a timeout, it SHOULD be possible to configure the timeout value, per RFC1122, 2.3.2.1.

C3) If the target protocol address is unable to be resolved, then the sending host SHOULD save at least one NPDU (from the set of NPDU’s with the same unresolved target protocol address), to be retransmitted after the target protocol address has been resolved, per RFC1122, 2.3.2.2.

5 Elements of other protocols required for the testing

The ARP is a stateless protocol, which manages and uses a translation table+cache, the contents of which may exhibit both temporal and transactional variation. A DUT implementing ARP may behave as a generator, receiver, and responder of ARP DPDUs. Robust evaluation of a DUT requires tests to stimulate each of these three behaviors, including both properly formed and erroneous ARP DPDUs and their conveying “Ethernet” MAC frames.

5.1 Protocol(s) from inferior layers used by this layer

ARP is a data-link layer protocol, where each ARP DPDU is conveyed via an “Ethernet” MAC frame. To achieve robust testing of the DUT’s implementation of ARP, the TD MUST be able to manipulate fields in the “Ethernet” MAC frame. If such manipulation is unavailable then only a subset of the ARP robustness testing may be conducted, limited to only those tests utilizing properly formed conveying “Ethernet” MAC frames.

5.2 Protocol(s) from superior layers used to test this layer

Testing of ARP robustness requires only transmission of ARP test PDUs to the DUT. Thus there is no requirement for a superior layer protocol during ARP robustness testing.

6 Robustness testing

6.1 Goals that drive testing requirements

The goal of the tests described in this document is to assess:

a) the robustness of an embedded control device with an implemented set of protocols, and

b) the device's resistance to attack, including the impact on the device's reporting and control functions while sustaining such an attack.

It is not a goal to determine the correctness of the implementation of those protocols, which would be a measure of their conformance to the requirements of the various protocol specifications.

This atypical testing goal interacts with vendor decisions to provide only partial implementations of protocols that are used within a proprietary or constrained context, such that those implementations are completely functional within the usage limits imposed by that context but are not conformant to the mandatory requirements of the controlling protocol standard.

As described by specific requirements in [EDSA-310], the consequent requirement is for this testing to

1) ascertain whether the DUT and other parts of the test configuration meet normal operational expectations before testing commences;
2) determine whether the DUT can survive receipt of invalid frames while continuing to function as expected in an automation environment; and
3) determine whether the DUT can sustain intervals of high and excessive communications load.

6.2 Testing overview

The DUT must be preconditioned to support testing by meeting the requirements of [EDSA-310] for demonstrating continued correct operation during testing;

Robustness testing occurs in three conceptual phases that may overlap, plus a test environment preconditioning phase.

a) The first conceptual phase, Baseline operation, attempts to demonstrate that the selected DUT protocol suite used for testing appears to operate properly for simple test cases under low load, before any protocol fuzzing or stress testing is attempted.

   NOTE 1 This initial demonstration of apparently correct behavior establishes the presumption that failure during additional testing is due to vulnerabilities of the specific protocol under test, rather than other protocols in the test suite.

b) The second conceptual phase, Basic robustness testing, probes the implementation for its ability to not evidence harm due to receipt of arbitrary erroneous frames, either singly or in combination.

   NOTE 2 This conceptual phase focuses on simple protocol robustness/fuzzing tests.

c) The third conceptual phase, Load stress testing, probes the implementation's response to high traffic rates incorporating valid PDUs.

   NOTE 3 This conceptual phase focuses on load/performance tests, first under high but supposedly sustainable receiver load, then under massive overload.

Although the robustness testing of this specification is conceptualized as occurring in distinct logical phases that progress from simple single-factor testing to more complex load testing incorporating PDUs with varying characteristics, there is no requirement that an actual robustness test process work in this ordered, sequential manner; any order of testing is permitted provided that the selected order does not lead to incorrect conclusions about robustness.

Requirement ARP.R1 – Criteria for robustness test failure

Pass or fail of basic robustness and load stress testing SHALL be determined by:

- whether or not essential services are adequately maintained under network traffic conditions created under these tests, as defined in [CRT.Essential_services];
- any particular conditions resulting in pass/fail mandated by the testing specified in this document.

The ARP protocol that is the subject of this specification is a stateless support protocol with an asymmetric query/response mechanism, which manages a translation table+cache. ARP is invoked as a byproduct of higher-layer protocols attempting to send messages to IP addresses, which drives the need to determine the MAC-level address of the device with the specified IP address.

Certain ARP options are host-configurable, including; maximum number of entries in the translation table+cache, timeout value used to flush table entries, and enable/disable of both ARP and ARP proxy support. Indirect baseline operation testing with implicit detection may be able to estimate the size of the translation cache and timeout values, while DUT support for ARP proxy may be undetectable remotely.

NOTE 4 Such indirect testing is not required for these robustness tests.

6.3 Protocol stack used for testing

6.3.1 Protocol(s) from inferior layers used by this layer

ARP is a higher-sublayer data-link layer protocol, with only the “Ethernet” MAC as an inferior sublayer. Though [EDSA-310] refers to a hardware type of “Ethernet”, this specification is equally applicable to other data-link media.

6.3.2 Protocol(s) from superior layers used to test this layer

Robustness testing of ARP robustness requires only transmission of ARP test PDUs to the DUT. However, baseline testing may require use of the IPv4 network layer protocol.

6.4 Phase 0: DUT preconditioning

Requirement ARP.R2 – Preconditioning of DUT and TD

The DUT, the TD(s) and possibly other devices in the test system SHALL be configured to allow observation of the performance of *essential services* of the embedded device under the test conditions, per the requirements in [CRT.Essential_services].

Essential services as defined in [CRT.Essential_services] include control loops, commands to control device configuration such as setpoints, and process alarms. A key approach to obtain observability is to use, as part of the test configuration, other automation system elements that have been engineered to communicate with and monitor the DUT.

6.5 Phase 1: Baseline operation

6.5.1 General

Requirement ARP.R3 – Demonstration of baseline operation

Before the TD commences robustness testing, the DUT SHALL demonstrate its ability to operate as expected in the test environment, including that the ARP component of the DUT’s protocol stack is present and functioning, and that the DUT can maintain essential services.

Requirement ARP.R4 – Susceptibility to cache poisoning

The DUT’s ARP translation cache+table is subject to attacks that thrash the cache. While such an attack may not disrupt other functions of the DUT, it can slow DUT communication and load the attached network, thus making it a legitimate subject of robustness investigation. Therefore, the baseline operation test phase of ARP SHALL include an assessment of the DUT’s resistance to ARP cache poisoning attacks.

6.5.2 Presence of proprietary protocol extensions

It is common practice for vendors to extend a standard protocol in a proprietary manner to provide functionality not covered by the standard protocol, or to provide more efficient or more constrained data transport for specific device information (e.g., when multiple device parameters require atomic update or readout as a group to maintain their inter-parameter consistency). Such extensions may take the form of extra message types, extra fields in standard messages, or extra functionality for standard fields in standard messages.

NOTE Robustness testing is not required to include specialized testing of proprietary protocol extensions. Rather, vendor disclosure of such extensions is intended to provide a basis for explanation of otherwise anomalous test results.

Requirement ARP.R5 – Equipment vendor disclosure of proprietary protocol extensions

When a protocol offered for testing has been implemented with deliberate proprietary extensions, the vendor SHALL document the extensions in a manner similar to that of Clause 4, such that robustness testing can explore the intended and unintended consequences of those protocol extensions. It is acceptable that access to this proprietary information be covered by a non-disclosure agreement (NDA) between the equipment vendor and the organization that is providing the ISCI robustness testing service.

6.6 Phase 2: Basic robustness testing

6.6.1 General

Areas of specific robustness testing are identified by analysis of the controlling protocol standards. These include identification of all field value ranges and of the bounding values of the underlying message representation (e.g., a range of 10..100 in a one-byte field, whose underlying representational bounding values are 0..255). Basic robustness testing includes testing the acceptability of each of these bounding values, and of the acceptance or rejection of adjacent values to those bounding values when such adjacent values can be represented in the message encoding.

Conceptually, basic robustness testing consists of the following, where volume or rate of message traffic is not a factor:

a) tests of valid message traffic:
   1) in expected sequences, sent at a low rate;

      NOTE ARP traffic is stateless, other than the momentary state that exists between the request and reply(s) of an ARP query transaction. However, the ARP translation table+cache is stateful since it functions as a look-aside LRU cache, albeit with update and replacement of static entries prohibited.

   2) in unexpected but valid sequences sent at a low rate (i.e., where the messages would be considered valid for the protocol under some conditions, but are not expected for the particular protocol state, message sequence or relative time);

b) tests of low rate erroneous message traffic (e.g., the ability of the device to function after receiving erroneous messages), including:
   1) single erroneous messages, including messages with inconsistent field values;
   2) properly formed messages in erroneous sequences
   3) sequences of erroneous messages.

[EDSA-310] describes the criteria for adequate performance of device essential services under these network traffic conditions. These criteria depend upon the specific service as well as whether the service operates on the same network interface used for test traffic.

6.6.2 Specific basic robustness testing

The ARP protocol is sensitive to flooding of the ARP translation cache, where the flooding is driven by receipt of multiple unsolicited changes to ARP cache entries. Various mechanisms have been proposed to provide partial protection against such flooding. One specific test attempts to discover whether any such partial protection has been implemented.

NOTE Details of cache poisoning attacks and defense mechanisms can be found via Internet search.

DUT failure to protect against cache poisoning is not a robustness failure. Rather, it demonstrates a need for compensating controls in any network that includes the susceptible DUT.

6.6.3 Basis for ARP robustness testing

Correctly and incorrectly formed ARP DPDUs sent to the DUT form the basis for ARP robustness testing.

Requirement ARP.R6 – Testing of each message field for sensitivity to invalid content

For basic robustness testing requiring erroneous messages or message sequences, valid ARP DPDUs or ARP DPDU sequences from the TD to the DUT SHALL be altered so that one component of the ARP DPDU is erroneous; or so that the ARP DPDU is in violation of 4.3, M1 or M5; or that it is both erroneous and in violation.

Such alterations SHALL be applied to each field of the ARP DPDU where alteration might have an impact on the DUT.

NOTE This type of testing can be described as single-message protocol “fuzzing”.

It is suggested that basic robustness testing proceed in stages, from simple to complex, as enumerated in 6.6.1 and indicated by the following list. In general, such ordering simplifies the task of locating the source(s) of software or hardware problems should they be uncovered by the testing. However, such ordering is not a requirement.

Requirement ARP.R7 – Constituent elements in basic robustness tests

Basic ARP robustness testing SHALL include the following elements, at low traffic rates, either in distinct test phases or intermixed in a form of the test supplier’s choosing:

a) valid message traffic

b) erroneous messages

6.6.4 Testing of proprietary protocol extensions

6.7 Phase 3: Load stress testing

6.7.1 General

NOTE 1 This testing phase is used to ascertain resistance to busy plant conditions as well as deliberate attacks.

Conceptually, load stress testing consists of tests of valid message traffic sent in two distinct phases:

a) tests of valid message traffic:

Phase 1 – Valid message traffic is sent at a high rate less than the saturation rate threshold specified by the DUT vendor (e.g., simulating normal but busy plant conditions);

Phase 2 – Valid message traffic is sent at up to the full auto-negotiated link rate (e.g., simulating an attack or malfunction of some kind);

Attacks against a protocol implementation take the form of repeated probing by malformed messages, or by correctly formed messages whose arrival sequence and relative timing are controlled by the attacker, or (more usually) by combinations thereof, all with the intent of exploiting some oversight or error in the specific protocol implementation(s), or of activating some intertwining aspects of a multi-layer protocol stack that were unconsidered by the implementing organization.

NOTE 2 Self-induced accidental attacks are also possible, due to designer or operator oversight.

Common examples of exploited oversights and errors are deliberate buffer overflows where the implementer had neglected to detect excessive message or field size, or recursive activation of character escape encoding when the implementer had not considered recursion. Implementation interactions within a multi-layer protocol stack may occur when an initial resource allocation (e.g., memory buffering) made by one protocol layer implementation is driven into an adjustment phase that conflicts with a resource allocation already made by a paired protocol layer implementation.

6.7.2 Basis for load stress testing

Device defenses against high traffic rates impact load stress testing, and are documented by the device vendor per the following requirement.

Requirement ARP.R8 – Documentation of self-protective rate limiting behavior

Where the DUT vendor imposes rate limiting on one or more of the protocols in the test process (e.g., “Ethernet” or ARP), the DUT vendor SHALL document that rate limiting occurs for that identified protocol when message rates exceed a perhaps-unspecified rate, as required by [CRT.Rate_limiting].

NOTE 1 The “Ethernet” protocol is included in this list as an identifiable placeholder for any physical and data-link protocols used to convey ARP DPDUs.

Requirement ARP.R9 – Constituent elements in load stress tests

Load stress testing SHALL include the following elements, either in distinct test phases or intermixed in a form of the test supplier’s choosing:

a) high-rate valid message traffic;

b) over-saturation-rate version of a), at the maximum auto-negotiated link rate that the TD can support.

Requirement ARP.R10 – Testing of saturation rate-limiting mechanism(s)

Saturation rate testing SHOULD be for durations of at least tens of seconds, long enough for any saturation effects to manifest. Tests that inherently involve a large number of DPDUs may need to run for much longer durations so that they do not cause other untoward impact on the test environment, which inherently involves the DUT, the TD and any other devices used in ascertaining the continuing performance of the DUT’s other normal functionality (e.g., interactions with superior or peer automation system components).

Requirement ARP.R11 – Reproducibility of robustness testing

Basic robustness testing SHALL use either a deterministic selection process (e.g., an offline test case generator or a seeded pseudo-random selection process), that tests combinations of valid and erroneous messages. See Clause 7 for specific required test cases.

Load stress testing SHALL use either a deterministic selection process (e.g., an offline test case generator or a seeded pseudo-random selection process), that tests series of valid messages. See Clause 7 for specific required test cases.

NOTE 2 The above constraint to use of a deterministic selection process does not prohibit use of feedback from analysis of DUT responses (and non-responses) as a means of further varying and focusing testing. Nor does it prohibit use of tester-selectable options and modes to determine the aggressiveness of the test process. Rather, it is merely an attempt to facilitate reproducibility by requiring use of reproducible means to select the order, sequence and components of each test.

6.8 Reproducibility

Requirement ARP.R12 – Overall reproducibility

Baseline operation, basic robustness testing, and load stress testing SHALL be reproducible per the requirements of [CRT.Reproducibility].

Those requirements recognize that deterministic behavior of the DUT itself is not under the control of the tester and must be assumed. Further, it is acceptable to branch a test process based upon prior results. Thus a change to the DUT may impact repeatability of a test even if the change does not intentionally cause variance for that test.

7 Specific test cases

Requirement ARP.R13 – Specific test cases

The tested suite of protocols SHALL be documented in at least the detail specified by Table 1.

Table 1 – ARP: Protocols used in test process

Protocol layer tested	Permissible alternatives	Protocols tested	Maximum load at which deliberate limiting occurs
Physical layer	IEEE 802.3		
Data-link layer	"Ethernet", ARP		
Network layer	IPv4 + ICMPv4 error reporting		

Requirement ARP.R14 – Testing SHALL include at least that specified by Table 2 through Table 12

These tables are descriptive, not proscriptive – there is no requirement that conforming robustness testing actually employ test sequences that are ordered or grouped as described in these tables.

Table 2 – ARP.T00: Baseline operation

Test ID	ARP.T00
Test name	Baseline operation
Test description	The basic operational aspects of the protocol under test, and of any inferior or selected superior supporting protocols used in the testing, shall be demonstrated as a means of checking that gross configuration or other errors are not interfering with the testing process, that ARP is a functioning part of the DUT's protocol stack, and that the protocol under test performs approximately as expected when not under test
Reference requirements	Requirement ARP.R3
Test type	Baseline operation
Test status	Mandatory
Expected DUT behavior	The DUT SHALL demonstrate basic protocol operability in the test configuration
Test object	To validate the lack of major errors in the configuration of the DUT and test environment
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD establishes that DUT is reachable and functions normally in the test environment, before protocol-specific testing commences
Expected response	The DUT demonstrates expected behavior in its "automation" environment, including that the ARP component of the protocol stack is present and functioning and that the DUT can adequately maintain essential services
Results	Pass or fail
Remarks	Initial failure of this test indicates a probably problem with the configuration of the TD or the test environment

Table 3 – ARP.T01: DUT cache poisoning

Test ID	ARP.T01
Test name	DUT cache poisoning
Test description	Properly formed unicast ARP request DPDUs specifying IPv4 addresses for which the DUT has previously generated ARP request DPDUs, but which have varying associated MAC addresses for the local DL-network, are sent by the TD to the DUT in an attempt to cause the DUT to churn the entries in its ARP translation cache. The DUT's response to this churning is observed
Reference requirements	Requirement ARP.R4
Test type	Baseline operation
Test status	Mandatory (see Remark 2)
Expected DUT behavior	The DUT defends itself against attempts to poison its ARP cache
Test object	To evaluate the DUT's ability to detect and ignore unexpected ARP reply DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TDs sends properly formed unicast ARP request DPDUs to the DUT, specifying IPv4 addresses for which the DUT has previously generated ARP request DPDUs, but which have varying associated MAC addresses for the local DL-network. The TD MAY test whether the DUT repeatedly updated its cache, or not, by sending subsequent IPv4 NPDUs to the DUT, where those NPDUs specify forwarding to the IP address of the prior-sent unsolicited ARP reply DPDU. The TD MAY monitor for any response from the DUT. If the DUT forwards the received NPDU to the most recently sent MAC address, then the DUT does not protect itself against DUT cache poisoning
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Determination of the need for compensating controls when the DUT's ARP implementation appears to not defend against DUT cache poisoning, which in this case SHALL be documented by the device vendor
Remarks	1) The DUT is expected to forward the received DPDU to a prior cached MAC address, where the DUT's selection of which MAC address to use as its forwarding destination MAC address provides insight into the DUT's vulnerability to cache poisoning attacks 2) This test may be run manually or by means other than the TD

Table 4 – ARP.T02: Truncated DPDU

Test ID	ARP.T02
Test name	Truncated DPDU
Test description	An ARP DPDU is sent as an “Ethernet” MAC frame payload, where the payload is a malformed ARP DPDU less than (HLN+PLN)×2+8 octets in length, truncating at least the DPDU’s TPA field, but where the “Ethernet” MAC FCS is correct for the truncated DPDU
Reference requirements	Requirement ARP.R6, violating 4.3, M5 or M6
Test type	Basic robustness: PDU structural violations
Test status	Mandatory
Expected DUT behavior	The DUT checks the ARP DPDU’s specified length before checksum validation
Test object	To evaluate the DUT’s consistency checks and processing order for received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends an invalid ARP DPDU such that the ARP DPDU length is less than 28 octets but the conveying “Ethernet” MAC frame payload is otherwise a valid ARP DPDU, chosen so that DPDU acceptance will lead to incorrect ARP processing on DPDU receipt. The TD MAY monitor for any response from the DUT
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	If the DUT fails to validate the length of the ARP DPDU = 28 octets, then the “Ethernet” MAC FCS may be incorrectly interpreted as part of the ARP DPDU’s TPA field. If this corrupt target protocol address is inserted into the DUT ARP translation cache, it will become an unused entry and will subsequently be flushed by the DUT ARP out-of-date validation mechanism. However, the desired entry (of the correct target protocol address) will not be made, resulting in the TD generating a retry of the ARP request to elicit an ARP reply from the DUT

Table 5 – ARP.T03: Inconsistent DPDU length

Test ID	ARP.T03
Test name	Inconsistent DPDU length
Test description	An ARP DPDU is sent whose length is (HLN+PLN)×2+8 octets , but less than the length indicated by the conveying “Ethernet” MAC frame
Reference requirements	Requirement ARP.R6, violating 4.3, M5 or M6
Test type	Basic robustness: content semantic violations
Test status	Mandatory
Expected DUT behavior	The DUT uses the ARP DPDU’s specified length rather than the size of the conveying “Ethernet” MAC frame
Test object	To evaluate the DUT’s consistency checks for received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends a valid ARP DPDU, where the conveying “Ethernet” MAC frame length field value is chosen so that DPDU acceptance will lead toincorrect ARP DPDU length processing on DPDU receipt. The TD MAY monitor for any response from the DUT
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	This test MAY expose whether “Ethernet” MAC payload length or the ARP DPDU’s specified length is dominant during receipt processing of well-formed-DPDUs

Table 6 – ARP.T04: Excessive DPDU length

Test ID	ARP.T04
Test name	Excessive DPDU length
Test description	An ARP DPDU is sent whose length is greater than (HLN+PLN)×2+8 octets, but having the length indicated by the conveying “Ethernet” MAC frame
Reference requirements	Requirement ARP.R6, violating 4.3, M5 or M6
Test type	Basic robustness: content semantic violations
Test status	Mandatory
Expected DUT behavior	The DUT uses the ARP DPDU’s specified length rather than the size of the conveying “Ethernet” MAC frame
Test object	To evaluate the DUT’s consistency checks for received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends a valid ARP DPDU, where the conveying “Ethernet” MAC frame length field value is chosen so that DPDU acceptance will lead to incorrect ARP DPDU length processing on DPDU receipt. The TD MAY monitor for any response from the DUT
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	This test MAY expose whether “Ethernet” MAC payload length or the ARP DPDU’s specified length is dominant during receipt processing of malformed-DPDUs

Table 7 – ARP.T05: Invalid operation

Test ID	ARP.T05
Test name	Invalid operation
Test description	Correctly formed ARP DPDUs are sent with invalid operation values
Reference requirements	Requirement ARP.R6, violating 4.3, M2
Test type	Basic robustness: content semantic violations
Test status	Mandatory
Expected DUT behavior	The DUT validates the ARP DPDU operation field on receipt and perform per requirement M2, M5 and M6
Test object	To evaluate the DUT’s semantic processing of received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends a properly formed ARP DPDU to the DUT containing an invalid operation value (for example: 0x0000, 0x0011, 0x0101, 0x1001, 0xFFFF). The TD MAY monitor for any response from the DUT
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	1) This test MAY expose failures to ignore invalid operation values. 2) Per RFC826, the ARP translation cache update or insertion occurs prior to checking the operation. Provided the “Ethernet” MAC Ethertype=ARP and requirements M2 is satisfied, the translation cache will be updated

Table 8 – ARP.T06: Incorrect specified lengths for address fields

Test ID	ARP.T06
Test name	Incorrect address field lengths
Test description	Correctly formed ARP DPDUs are sent with values in the HLN and/or PLN fields of the DPDU other than those required for the hardware interface and protocol under test, which for IEEE 802 and IPv4 are the values 6 and 4, respectively
Reference requirements	Requirement ARP.R6, violating 4.2.2, c) and d)
Test type	Basic robustness: content semantic violations
Test status	Mandatory
Expected DUT behavior	The DUT validates on receipt the values of the HLN and PLN fields of the ARP DPDU for appropriateness for the protocols employed by the DUT at its interface at which reception occurs
Test object	To evaluate the DUT's consistency checks for received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends a properly formed ARP DPDU to the DUT containing a value for the HLN and/or PLN fields that differs from that required for the sending hardware type ("Ethernet") and the selected network layer protocol (IPv4). The TD MAY monitor for any response from the DUT
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	This test exposes failures to validate the appropriateness of the lengths of the address fields conveyed in the DPDU

Table 9 – ARP.T07: Protocol address spoofing

Test ID	ARP.T07
Test name	Protocol address spoofing
Test description	Properly formed ARP request DPDUs and ARP reply DPDUs are sent by the TD, containing an SPA that is invalid for the DUT's sub-network
Reference requirements	Requirement ARP.R7 b), and d)
Test type	Basic robustness
Test status	Mandatory
Expected DUT behavior	The DUT protects itself against protocol address spoofing
Test object	To evaluate the DUT's ability to detect and ignore ARP DPDUs with an invalid SPA.
Test configuration	A TD is connected to the DUT by an underlying switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends properly formed ARP request and ARP reply DPDUs to the DUT, containing an invalid SPA. The TD MAY monitor for any response from the DUT
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	1) The DUT is expected to detect the invalid SPA contained in the ARP reply DPDU and not update the ARP translation cache. 2) Proper behavior of the DUT is observable only for ARP Request DPDUs, as evidenced by the absence of an ARP reply DPDU from the DUT

Table 10 – ARP.T08: Hardware address spoofing

Test ID	ARP.T08
Test name	Hardware address spoofing
Test description	Properly formed ARP request and ARP reply DPDUs are sent by the TD, containing an SHA which is the same as the DUT's
Reference requirements	Requirement ARP.R7 b), and d)
Test type	Basic robustness
Test status	Mandatory
Expected DUT behavior	The DUT protects itself against hardware address spoofing
Test object	To evaluate the DUT's ability to detect and ignore ARP DPDUs with an SHA matching the DUT
Test configuration	A TD is connected to the DUT by an underlying switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends properly formed ARP request and ARP reply DPDUs to the DUT, containing an SHA matching the DUT's SHA. The TD MAY monitor for any response from the DUT
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	1) The DUT is expected to detect the matching SHA and ignore the DPDU. 2) A hardware address spoof results in a denial of service (DoS) characterized by no traffic from the DUT, since the DUT ARP translation cache may contain only entries referring to itself. A secondary effect of this attack may be an overload of DUT resources, since every transmitted DPDU may be looped-back to the DUT

Table 11 – ARP.T09: Translation cache size

Test ID	ARP.T09
Test name	Translation cache size
Test description	A large number of unique ARP DPDUs are sent to attempt to exceed the size of the ARP translation cache
Reference requirements	Requirement ARP.R9
Test type	Load stress
Test status	Mandatory
Expected DUT behavior	The DUT protects itself against a large number of DPDUs
Test object	To evaluate the DUT's ability to receive and withstand a large number of DPDUs addressed to it within the time period configured for detecting out-of-date ARP translation cache entries, per RFC 1122, 2.3.2.1
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends a large number valid ARP DPDUs addressed to the DUT with a Sender Protocol Address that is generally increasing (monotonic or otherwise). The actual number of valid DPDUs to be sent by the TD may be selected based on the desired overall test duration or a priori knowledge of the number of entries in the ARP translation cache as implemented by the DUT. If the latter source is used, the number of valid DPDUs SHOULD exceed the number of entries supposedly implemented by the DUT in the ARP translation cache. The TD MAY monitor the DUT for any evidence of DUT problems handling the expected overflow of its local ARP translation cache
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	1) Using the DUT default settings for the ARP timeout the test procedure should cause the ARP translation cache to be completely filled. The DUT handling of ARP translation cache overflow should be robust enough to prevent the DUT from evidencing any degradation of control and display response 2) The DUT is expected to respond to valid ARP DPDUs addressed to it and to ignore the invalid ones

Table 12 – ARP.T10: Maintenance of service under high load, including network saturation

Test ID	ARP.T10
Test name	Maintenance of service under high load, including network saturation
Test description	A flurry of ARP DPDUs is sent to attempt to overwhelm the DUT's receive processing and storage resources. This test proceeds in two phases: • Phase 1: as a high load test during which the DUT SHOULD respond normally to received messages • Phase 2: as a network saturation test during which the DUT MAY invoke protective behaviors such as blocking network reception but SHOULD otherwise function normally. See [CRT.Rate_limiting] for additional requirements
Reference requirements	Requirement ARP.R9
Test type	Load stress
Test status	Mandatory
Expected DUT behavior	The DUT protects itself against a flood of received ARP DPDUs • Phase 1: The DUT continues to function, adequately maintaining both essential services and network communications, in the presence of a sudden burst of received UDP TPDUs, provided that the load thus induced is less than that claimed as supportable by the DUT vendor. The DUT vendor SHALL state a rate limit below which protective measures are not expected to be invoked; • Phase 2: The DUT adequately maintains essential services, even if it must reduce or cease network communications during the period of network overload.
Test object	To evaluate the DUT's ability to receive and withstand a burst of ARP DPDUs addressed to it
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends valid ARP DPDUs that are either explicitly or implicitly addressed to the DUT • Phase 1: at a rate less than that at which the DUT's manufacturer claims DUT protective measures will be invoked; • Phase 2: at a rate up to the auto-negotiated maximum rate of the underlying network, maintains that high load rate for a few seconds, then gradually reduces its sending rate to zero. ARP DPDUs sent to the DUT MAY be conveyed by Ethernet frames using any of the types of explicit or implicit IP addressing (e.g., unicast, broadcast ,multicast), in any combination During phase 1, testing SHALL proceed in two or more steps, first using only ARP request DPDUs, then using only ARP reply DPDUs. An optional third test step MAY intermix ARP request and reply DPDUs
Expected DUT response	• Phase 1: The DUT is expected to continue network communication even under high load while adequately maintaining essential services. • Phase 2: The DUT is expected to activate protective measures at some (vendor unspecified) level of resource demand, and to recover some reasonable time interval after that demand for resources is reduced substantially below the level at which the protective measures were triggered. The DUT is expected to adequately maintain essential services throughout the test
Results	Pass or fail
Remarks	The DUT vendor is not required to be able to predict the nessaging rate at which such protective measures are invoked, but SHOULD be able to put an upper bound on time after the stimulus ceases before the recovery is complete

Bibliography

IANA protocol and number registries, http://www.iana.org/protocols/
registries of various assigned code points for standard Internet protocols

— — — — — —