EDSA-401
ISA Security Compliance Institute –
Embedded Device Security Assurance –

Testing the robustness of implementations of two common "Ethernet" protocols

Version 2.01

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 OF PRIVACY, 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
1.7	2010.06.18	Initial version published to http://www.ISASecure.org
2.01	2010.09.28	Added tests for broadcast and unicast destination address tolerance (had multicast); runt (short) frame testing mandatory only if TD can support, since test may not be supportable by modern hardware; create distinct test criteria at high but supported rate and full auto-negotiated link rate; removed protocol conformance aspects of 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 document 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 IEEE 802.3 "Ethernet" protocol, either as Ethernet II or as IEEE 802.3 Type 1 and IEEE 802 SNAP, as a measure of the extent to which such implementations defend themselves against

- correctly formed messages and sequences of such messages, whether addressed to the device or not;
- 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 basic data-link "Ethernet" protocol is stateless, without distinction between server and client roles. There is state associated with the auto-negotiation of data rate and two-way-alternate/two-way-simultaneous mode that is found in some of the IEEE 802.3 Physical layers, but that is a conformance issue that is considered to be outside the domain of robustness testing that is the subject of this specification.

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

The following associated specification contains requirements common to this and similar robustness tests for other protocols often found in 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.

This publication of the Institute of Electrical and Electronics Engineers (IEEE) is the controlling specification for testing the robustness of the "Ethernet" protocol variants – both Ethernet II and IEEE 802.3 with IEEE 802.2 Type 1 and IEEE 802 SNAP – that is the subject of this document:

IEEE 802.3:2005, *IEEE Standard for Information Technology – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

NOTE 2 The selected specification is the version that will have been used to design the hardware and software that implements Ethernet II in most currently fielded DUTs. It is not the latest version from IEEE, but is more current than the latest version published as ISO/IEC 8802-3.

These publications of the Internet Engineering Task Force (IETF) are the controlling specifications for the higher-(sub)layer protocols that are used for testing the robustness of the Ethernet II protocol that is the subject of this document.

NOTE 3 For each RFC*nnn*, the controlling version can be found at http://tools.ietf.org/html/rfc*nnn*.

IANA port numbers, as specified at http://www.iana.org/assignments/port-numbers

---

[1] to be published concurrently with this document

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 4 Only 2.3.2 of RFC1122 is referenced.

NOTE 5 Other IETF specifications related to the above can be found in the Bibliography.

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

NOTE 6 Other IETF specifications related to the above can be found in the Bibliography.

IEEE 802, *IEEE standard for local and metropolitan area networks: Overview and architecture*, available with supplements at http://standards.ieee.org/getieee802/802.html

IEEE 802.1Q, *IEEE standard for local and metropolitan area networks – Virtual bridged local area networks*, available at http://standards.ieee.org/getieee802/802.1.html

IEEE 802.2, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – -Local and metropolitan area networks – Specific requirements – Part 2: Logical link control*, available at http://standards.ieee.org/getieee802/802.2.html

IEEE 802.3, *IEEE standard for information technology – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CMSA/CD) access method and physical layer specifications*, available in five parts with supplements at http://standards.ieee.org/getieee802/802.3.html

3 Definitions and abbreviations

3.1 Definitions

3.1.1
broadcast MAC address
address field of 0xFFFF FFFF FFFF (all 1's)

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 II
IEEE 802.3 as harmonized with the original DEC/Intel/Xerox Ethernet

3.1.5
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.

3.1.6
malformed (message or PDU)
PDU that violates syntactic rules on PDU structure

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

3.1.7
priority-tagged frame
four-octet record within an IEEE 802 frame that specifies the frame contains a tag header that carries priority information but carries no VLAN identification information.

3.1.8
station
device providing a physical layer interface to a communications medium

3.1.9
testing device
conceptual single network-connected device, possibly consisting of multiple physical network-connected devices, used to assess the vulnerability of the device under test according to defined procedures

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

3.1.10
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

3.1.11
VLAN-tagged frame
four-octet record within an IEEE 802 frame that specifies the frame contains a tag header that carries both VLAN identification, which restricts the frame to the identified VLAN, and frame priority information

NOTE The same 4-octet record conveys both VLAN and priority tag information.

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

APDU	application protocol data unit
ARP	address resolution protocol
CRT	communication robustness testing
DLL	data-link layer
DoS	denial of service
DPDU	data-link-layer protocol data unit
DSAP	(LLC) destination service access point
DUT	device under test
EDSA	embedded device security assurance
FCS	IEEE 802.3 frame check sequence
frame	IEEE 802.3 MAC sub-layer PDU

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)
IPv6	IP version 6 (uses 128-bit network layer addresses)
LLC	IEEE 802.2 logical link control
lsb	least significant bit
MAC	media access control sub-layer (of the DLL)
(*N*)PDU	(*N*-layer) protocol data unit, where *N* = D (data-link), N (network), T (transport), A (application), etc
NPDU	network-layer protocol data unit
OUI	(IEEE-assigned) organizationally unique identifier
PHY	IEEE 802.3 physical layer
SNAP	IEEE 802 sub-network access protocol
SSAP	(LLC) source service access point
TD	testing device
VLAN	virtual local area network

4 Elements of the protocol under test

4.1 General

This document specifies robustness testing for the IEEE 802.3 “Ethernet” protocol, either as Ethernet II or as IEEE 802.3 Type 1 and IEEE 802 SNAP, each of which provides a stateless data link sub-layer protocol providing an unordered, unprioritizable, unreliable point-to-multipoint communications path. Ethernet II uses the basic frame defined by IEEE 802.3 but replaces IEEE 802.3’s two-octet Length/Type field with a two-octet EtherType field that never specifies a length, whereas the IEEE 802.3 Type 1 plus IEEE SNAP protocol variant adds eight octets to the basic IEEE 802.3 frame but can coexist with other uses of the IEEE 802.3 protocol.

With respect to the IP protocol suite whose implementations are tested by the EDSA robustness test suite, IP NPDUs and ARP DPDUs are transmitted over IEEE 802.3 networks using IEEE 802.3 with either

a) 2 B of Ethernet II EtherType headers as specified by RFC894; or

b) 8 B of IEEE 802.2 and IEEE 802 SNAP headers as specified by RFC 1042.

NOTE Although there is an IEEE 802 defined protocol type for IP, which could enable a third “Ethernet” variant using IEEE 802.2 Type 1 without the IEEE 802 SNAP header, IPv4 traffic cannot be encapsulated directly within IEEE 802.2 DPDUs without use of IEEE 802 SNAP because there is no protocol type for ARP. IPv6 does not use ARP, so can be transmitted directly over IEEE 802.2 without SNAP, but this option is seldom used in industrial systems.

4.2 Frames

4.2.1 Frame structure

The IEEE 802.3 frame with IEEE 802.2 and IEEE 802 SNAP is structured as shown in Figure 1, using a big-endian octet order. The location and structure of the optional IEEE 802.1Q VLAN/priority tag is included.

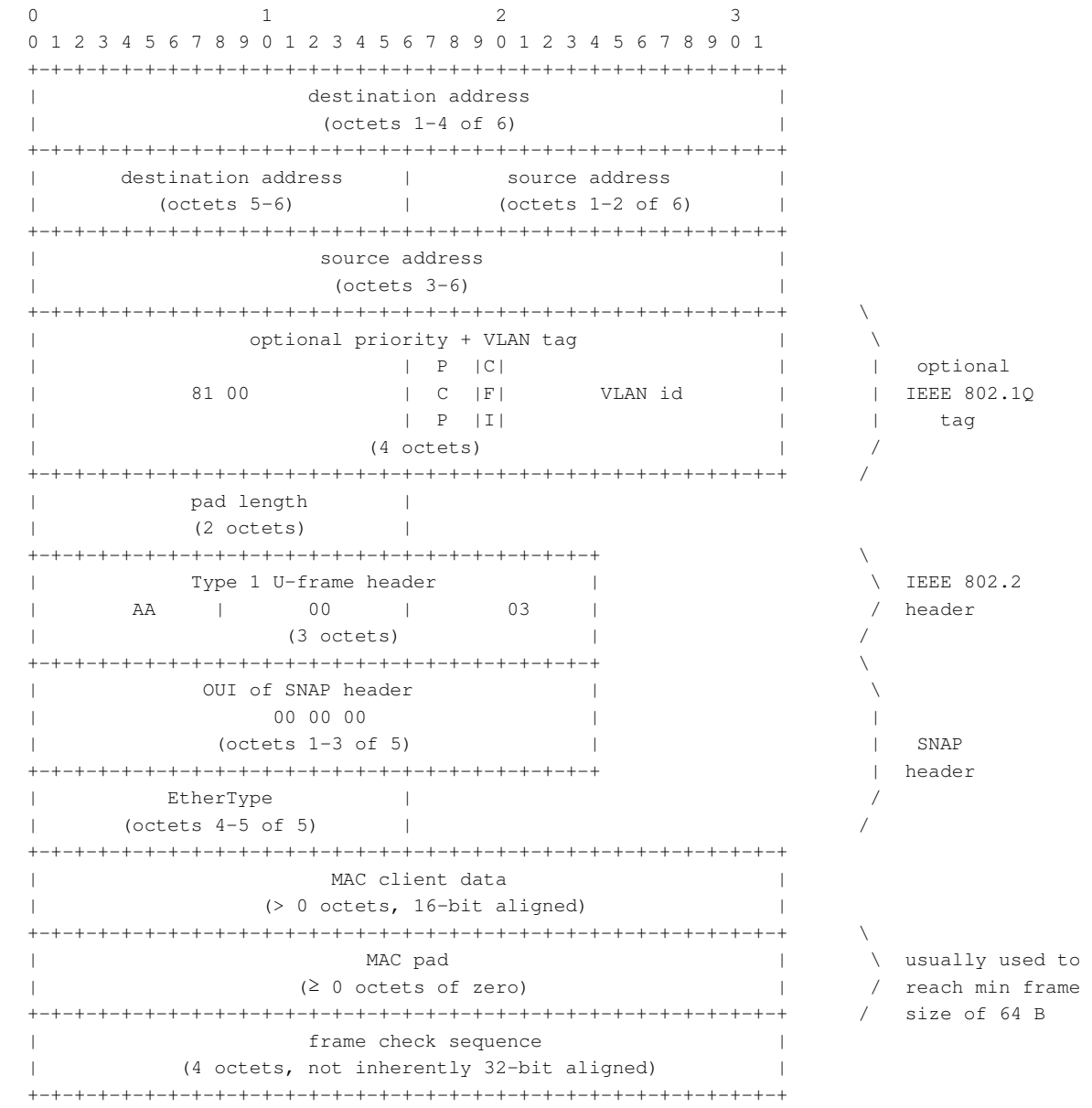

Figure 1 – IEEE 802.3 frame structure with IEEE 802.2 Type 1 and IEEE 802 SNAP

The Ethernet II frame is structured as shown in Figure 2, using a big-endian octet order. The location and structure of the optional IEEE 802.1Q VLAN/priority tag is included.

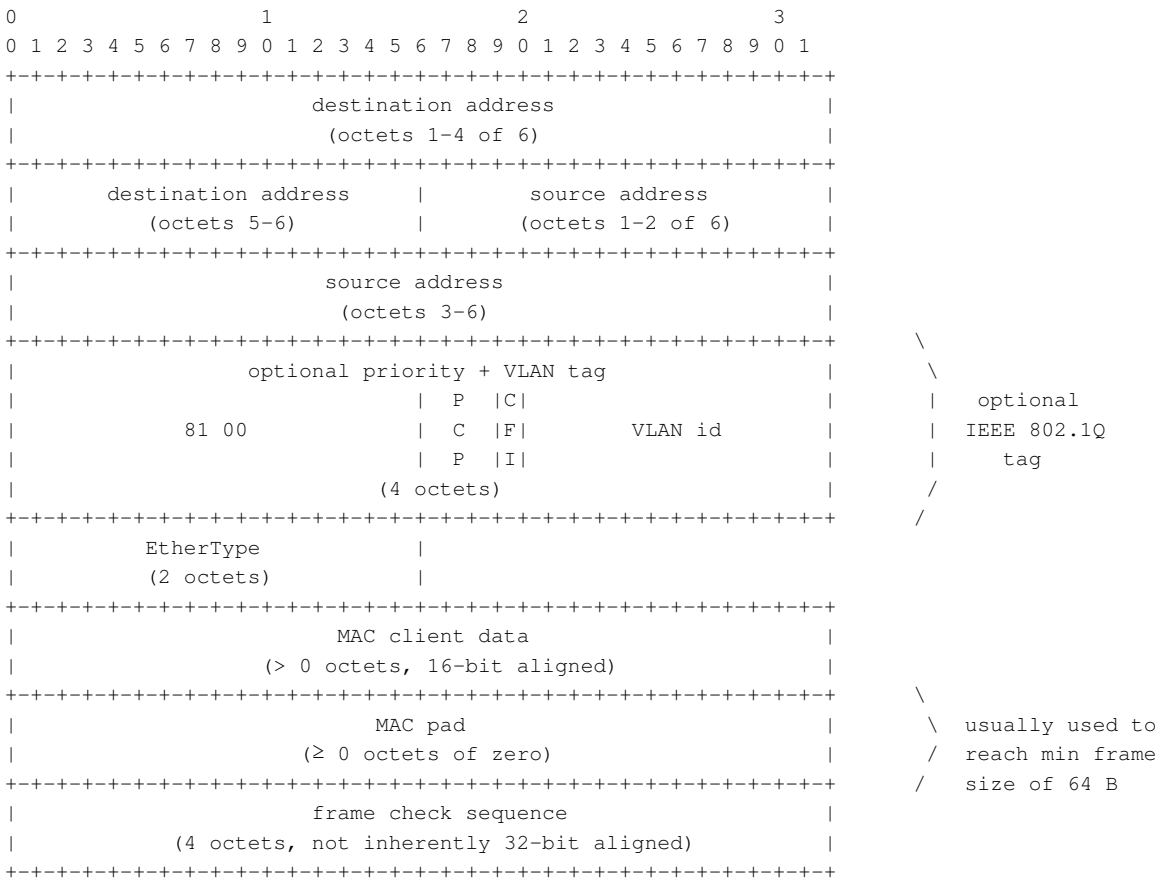

Figure 2 – Ethernet II frame structure

4.2.2 Mandatory and optional fields

The following fields are components of either Ethernet II frames or IEEE 802.3 Type 1 and IEEE 802 SNAP frames (where field sizes are specified in octets (B) or bits (b)):

a) Destination address (6 B): specifies the station(s) for which the frame is intended, as specified by IEEE 802.3, 3.2.3.1.

b) Source address (6 B): specifies the station from which the frame was initiated, as specified by IEEE 802.3, 3.2.3.1.

c) Optional Q-tags (0 B, 4 B, 8 B), as specified by IEEE 802.1Q, each of which consists of:

   1) Tag protocol identifier (TPID) (2 B), with the fixed value 0x8100: designates that the following two octets specify frame priority and VLAN restriction information;

   2) Priority code point (PCP) (3 b): specifies the IEEE 802.1p priority of the frame, from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of data-link traffic (e.g., voice, video, data, etc)

   3) Canonical format indicator (CFI) (1 b): indicates the presence of a (source) Routing information field (RFI) in the frame, which is expected to have the value 0 in Ethernet frames;

   4) VLAN identifier (VID) (12 b): specifies the VLAN to which the frame belongs, where a value of 0 means that the frame is not restricted to a single VLAN;

      NOTE 1 When the VID value is zero, the 802.1Q tag specifies only a priority, so is referred to as a priority tag. The hexadecimal VID value of 0xFFF is reserved. All other VID values may be used, supporting up to 4094 VLANs. On bridges, the VID value of one (1) is often reserved for management.

   NOTE 2 Use of double tagging, where a frame contains two consecutive 4 B Q-tag fields, is defined but normally restricted to use by Internet service providers. Use of double tagging in automation networks is not supported.

d) Type/Length field(s):

For frames that conform to Ethernet II, this is

1) EtherType (2 B): specifies a hardware vendor or a protocol type, per http://www.iana.org/assignments/ethernet-numbers. The IEEE Assigned Numbers Authority maintains the authoritative list of EtherTypes: http://standards.ieee.org/regauth/ethertype/eth.txt

For frames that conform to IEEE 802.2 Type 1 with an IEEE 802 SNAP field, this is a sequence of three subfields:

2) Length (2 B): specifies the number of data octets, field e), in the frame;

3) IEEE 802.2 Type 1 header (3 B): always 0xAA 00 03, designating the IEEE 802 SNAP subprotocol;

4) IEEE 802 SNAP header, with two subfields:

   i) Organizationally Unique Identifier (3 B): always zero (0x00 00 00) when designating the IP protocol suite;

   ii) EtherType (2 B): as specified in 1).

NOTE 3 In essence, the use of IEEE 802.3 Type 1 and IEEE 802 SNAP inserts 2 B of Length field and 6 B of fixed header (0xAA 00 03 00 00 00) before the EtherType field that is present in either protocol.

NOTE 4 Use of the shorter non-SNAP IEEE 802.2-only encapsulation of IP via the IEEE 802.2-defined code point for IP is explicitly forbidden by RFC1122, 2.3.3. Thus it is not tested here, even though implementations that choose to not conform to RFC1122 may exist.

e) Data (≥ 1 B): fully transparent data octets, nominally conveying information for a higher-(sub)layer protocol, as specified by IEEE 802.3, 3.2.7. For IEEE 802.3 with IEEE 802.2 and IEEE 802 SNAP headers, the maximum permitted size of the data field is such that the entire frame is 1536 B or less in size.

NOTE 5 For Ethernet II, a larger maximum size is permitted only when jumbo frames (4.2.4.2) are negotiated.

f) Pad (≤ 46 B): any extra padding octets that were added to make the “Ethernet” frame size be at least 64 B, as specified by IEEE 802.3, 3.2.7.

NOTE 6 For Ethernet II frames, all of these pad octets should be 0x00, as specified by RFC894.

NOTE 7 The requirement for padding short IEEE 802.3 frames arose from collision detection requirements that existed in early low-data-rate half-duplex interfaces to the IEEE 802.3 PHY medium. More recent IEEE 802.3 PHYs use full-duplex interfaces at a much higher data rate and do not require such padding.

g) Frame check sequence (4 B): a modified cyclic redundancy check (CRC) of the MAC octets excluding the FCS, as specified by IEEE 802.3, 3.2.8.

NOTE 8 Most of the above fields are also documented at http://www.iana.org/assignments/arp-parameters/.

4.2.3 Mandatory protocol aspects

IEEE 802.3 mandates a minimum frame size of 64 B and a maximum frame size of 1536 B. This is a legacy from early IEEE 802.3 half-duplex PHYs. When required, extra bytes needed to extend the frame to the required minimum 64 B frame size are added near the end of the frame via its optional Pad field. When used with IEEE 802.2 Type 1 and IEEE 802 SNAP, the size of the conveyed data field is carried in the frame’s Length field, as specified in 4.2.1 d)2); when used as Ethernet II it is not.

4.2.4 Optional MAC components and elements of procedure

4.2.4.1 VLAN tagging

IEEE 802.1Q adds a 4-octet infix “Q-tag” to the 802.3 frame, immediately after the MAC source address field, where the Q-tag includes 802.1Q VLAN information and 802.1P priority information. For more information see http://en.wikipedia.org/wiki/IEEE_802.1Q

Q-tagging is used to restrict frames to specific VLANs and/or to convey the data-link priority of the frame. Priority-tagged frames make sense for automation systems. Thus the DUT needs to accept Q-tagged frames whether or not it can interpret the Q-tag’s content.

4.2.4.2 Jumbo frames

IEEE 802.3 does not support “jumbo frames” – ones whose size exceeds that permitted by the IEEE 802.3 standard – because use of such frames would create interoperability problems. However, many procurement specifications require that purchased equipment support jumbo frames. When devices have that capability, it typically is a configuration option of the device, used with the Ethernet II version of the “Ethernet” frame format. For more information see http://en.wikipedia.org/wiki/Jumbo_frame.

Due to lack of interoperability, devices that are configured to support jumbo frames and those that are not (or cannot be) usually are not permitted on the same subnet. However, an attacker is not so constrained. Therefore, while the DUT need not process jumbo frames correctly, it is not permitted to malfunction when receiving jumbo frames.

4.3 Mandatory and optional protocol features

The mandatory features of the “Ethernet” protocol that are amenable to testing using standard “Ethernet” hardware are:

M1) Each “Ethernet” frame SHALL contain at least 64 octets; frames that otherwise would contain fewer than 64 octets SHALL include a Pad field, per IEEE 802.3, 3.1.1.

NOTE 1 The Ethernet hardware of some TDs may extend automatically the size of frames less than the minimum. When that is the case, DUT testing of robustness to receipt of overly short frames (known as “runt frames”) will not occur.

M2) As used by the TD to test the DUT with valid frames, the “Ethernet” frame SHALL comprise a maximum of 1518 octets when no Q-tag is present, or 1522 octets when one Q-tag is present, per IEEE 802.3, 3.1.1 and IEEE 802.1Q.

NOTE 2 This size can increase to over 15 kB when jumbo frames (4.2.4.2) are employed on Ethernet II networks. Embedded devices are not expected to use such large frames when communicating with automation control devices.

M3) As used by the TD to test the DUT with invalid frames, the “Ethernet” frame MAY exceed the maximum frame size specified in M1).

M4) The first (lsb) bit in the destination address field SHALL be used to designate the address type as either an Individual address (lsb = 0) or a Group address (lsb = 1), per IEEE 802.3, 3.2.3.b. However, the broadcast address (0xFF FF FF FF FF FF) is classified as a group address even though its first bit is zero.

M5) The “Ethernet” frame’s EtherType field SHALL contain a valid value as specified at http://www.iana.org/assignments/ethernet-numbers and http:/standards.ieee.org/regauth/ethertype/eth.txt

M6) The number of pad octets required in a frame data field SHALL be computed such that the total frame size is 64 B, and shall be zero when the total frame size without pad octets is 64 B or greater.

NOTE The TD may exceed this limit when testing the DUT’s ability to accept or reject very large frames.

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

C1) All Ethernet II frames received by a device with a destination address set to the IEEE 802 broadcast address SHALL be presented to the superior network layer.

5 Elements of other protocols required for the testing

5.1 General

At the data-link layer, typically after an initial data-link-layer-assisted physical-layer data rate and half-duplex/full-duplex mode negotiation, “Ethernet” functions as a stateless protocol for conveying client data in a transparent manner without that data being interpreted by the conveying “Ethernet” protocol. A DUT implementing “Ethernet” SHALL be both an initiator and a receiver of frames; however the only vulnerability as an initiator results from use by a higher layer protocol in the DUT. Such a vulnerability is probed by testing the higher layer protocol itself. Thus evaluation of the robustness of a DUT’s “Ethernet” implementation only requires testing the DUT’s receiver role when receiving both properly formed and

erroneous frames, where the latter includes IEEE 802.3 frames whose length exceeds the maximum length of 1536 octets expected for DUTs tested by the EDSA IEEE 802.3 robustness test.

NOTE Most switches will not forward too-short or overly-long frames, which is why the test configuration for Ethernet tests uses hubs or other non-limiting connections where possible.

The primary behavior of an “Ethernet” receiver is to pass the contained received PDU to a higher sublayer protocol upon receipt of a properly formed Ethernet frame, and to pass nothing to a higher layer protocol upon receipt of an improperly formed frame. In the case of a properly formed frame that the DUT correctly accepts, the DUT’s vulnerability is within the higher layer protocol, which is not the subject of this test. In the case of an improperly formed frame, the frame may be discarded, ignored, or communicated to local communications stack management. However, in no case should receipt of such an erroneous frame have any lasting affect on the DUT’s ability to receive other frames.

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

The “Ethernet” data-link protocol of the test configuration uses one of the many IEEE 802.3 physical layer (PHY) protocols.

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

As noted in 5.1, testing of Ethernet robustness requires only transmission of test frames to the DUT. Thus there is no requirement for a superior layer protocol during Ethernet 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.

A non-switched connection is typically used between the TD and the DUT for these tests. This is because most switches will drop malformed or oversize “Ethernet” frames which must be received by the DUT in order to execute the tests.

NOTE 1 In many test environments, point-to-point connections are not employed because the EDSA test methodology requires the DUT to demonstrate continued operation in a control environment typical of that in which it would be embedded for normal operation. This normally requires the DUT to be in communication with superior and/or peer control devices, often from the same

automation vendor, while it is under test. Test environments that use point-to-point connections between the DUT and the TD, where the TD itself forwards traffic between the TD and other devices in the automation environment, also are acceptable.

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 2 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 3 This conceptual phase focuses on 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 4 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 frames 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 "Ethernet".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 "Ethernet" protocol that is the subject of this specification is a stateless protocol without any query/ response mechanisms.

NOTE 4 Various IEEE 802.3 addenda add stateful sub-protocols to the basic IEEE 802.3 protocol. None of those sub-protocols except link rate and full-duplex/half-duplex negotiation are expected in an automation environment. Link rate and full-duplex/half-duplex negotiation is a property of some IEEE 802.3 PHYs, so is excluded from this data-link robustness test specification. None of the other various optional stateful sub-protocols specified in IEEE 802.3 addenda are addressed in this robustness test.

6.3 Protocol stack used for testing

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

"Ethernet" designates either of a specific pair of related data-link layer protocols based on IEEE 802.3, with the physical layer, also defined as a wide selection of alternatives within IEEE 802.3, remaining as the only inferior layer.

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

As noted in 5.1, testing of Ethernet robustness requires only transmission of test frames to the DUT. Thus there is no requirement for a superior layer protocol during Ethernet robustness testing.

6.4 Phase 0: DUT preconditioning

Requirement "Ethernet".R2 – Preconditioning of DUT, TD and any firewalls between the DUT and TD

The DUT SHALL be preconditioned for robustness testing, typically by

a) configuring the DUT, the TD(s) and possibly other devices in the test system to use an implementation of the “Ethernet” protocol;

b) configuring the DUT, the TD(s) and possibly other devices in the test system 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 “Ethernet”.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 maintaining essential services.

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 1 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.

NOTE 2 Proprietary extensions to the “Ethernet” protocol are not expected, due to the high commodity hardware content of most “Ethernet” implementations.

Requirement “Ethernet”.R4 – 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 EDSA 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 Although some of the IEEE 802.3 addenda are stateful, and the IEEE 802.3 PHY autonegotiation protocol is stateful, the subset of the "Ethernet" data-link protocol that is relevant to industrial automation systems is stateless.

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 Basis for "Ethernet" robustness testing

Correctly and incorrectly formed "Ethernet" frames sent to the DUT form the basis for "Ethernet" robustness testing.

Requirement "Ethernet".R5 – Testing of each message field for sensitivity to invalid content

For basic robustness testing requiring erroneous messages or message sequences, valid "Ethernet" frames SHALL be altered so that one component of the "Ethernet" frame is erroneous; or so that the "Ethernet" frame is in violation of at least one requirement in 4.3, M1 through M6; or that it is both erroneous and in violation.

Such alterations SHALL be applied to each field of the "Ethernet" frame where alteration might have an impact on the DUT.

NOTE 1 This type of testing can be described as single-message protocol "fuzzing".

NOTE 2 It is the Ethernet protocol itself that is being tested, not any conveyed higher-level protocol.

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 "Ethernet".R6 – Constituent elements in basic robustness tests

Basic "Ethernet" 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

6.6.3 Specific basic robustness testing

Basic robustness testing SHOULD include combinations of:

a) selection of basic frame format:

1) frames that use the Ethernet II encoding;

2) frames that use the IEEE 802.2 Type 1 and IEEE 802 SNAP encoding;

b) inclusion of Q-tag headers: zero, one, and two or more Q-tag headers;

NOTE 1 Use of two or more Q-tag headers is not proper on automation networks, but an attacker is not limited by such constraints.

c) selection of total frame size:

1) less than 64 B;
2) less than 64 B before considering padding, but padded to 64 B;
3) less than 64 B before considering padding, but padded to more than 64 B in violation of the specifications;
4) 64 B or greater, but not greater than 1518 B plus the size of any Q-tags, without padding;
5) 64 B or greater, but not greater than 1518 B plus the size of any Q-tags, before considering padding, with padding in violation of the specifications, such that the total frame size is 1518 B plus the size of any Q-tags, or less;
6) 1519 B plus the size of any Q-tags, or greater, without padding;
7) 1519 B plus the size of any Q-tags, or greater, before considering padding, with padding in violation of the specifications.

Basic robustness testing also SHOULD include frames that specify use of IEEE 802.2, but do not contain the correct value for the next six octets; the Type 1 header and the IP OUI of the SNAP header. This testing also should include frames that specify use of IEEE 802.2 Type 1 and IEEE 802 SNAP, but where the "EtherType" field that immediately follows the SNAP OUI is a Q-tag preceding a correct EtherType.

Requirement "Ethernet".R7 – Specific focus of basic robustness testing

Specific focus SHOULD be put on testing both "Ethernet" protocol alternatives: Ethernet II and IEEE 802.2 Type 1 plus IEEE 802 SNAP. All of the other alternatives and combinations of this subclause also SHOULD be tested.

NOTE 2 Some DUTs may be able to process both alternatives; others may function only with one. However, since an attacker can generate both forms, the DUT needs to survive attacks in either form. Likewise, while networks are configured to use or not use jumbo frames of more than 1536 B, an attacker could generate such frames even on networks where they are not permitted.

Basic robustness testing of the "Ethernet" protocol MAY be used to explore rate sensitivity and other aspects of the DUT's "Ethernet" protocol implementation.

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:

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. 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 "Ethernet".R8 – Documentation of self-protective rate limiting behavior

Where the DUT vendor imposes rate limiting on the protocols in the test process (i.e. "Ethernet" and related IEEE 802 protocols), 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].

Requirement "Ethernet".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 "Ethernet".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 frames 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 "Ethernet".R11 – Reproducibility of robustness testing

Basic robustness testing SHALL use 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 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 The above constraint to use 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.

6.7.3 Specific load stress testing

Due to its simplicity and statelessness, the only specific feature of the "Ethernet" protocol that requires special attention during load stress testing is the implementation's ability to receive frames in the three supported IEEE 802.3 addressing modes: unicast, broadcast and multicast, and to filter frames addressed to a multicast destination address, because such filtering usually involves a secondary software filtering step.

Load stress testing of the "Ethernet" protocol itself, with or without concurrent testing of other protocols, MAY be used to explore rate sensitivity and other aspects of the DUT's "Ethernet" protocol implementation.

6.8 Reproducibility

Requirement "Ethernet".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 "Ethernet".R13 – Specific test cases

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

Table 1 –"Ethernet": 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"	IEEE 802.3 as Ethernet II and IEEE 802.3 with IEEE 802.2 Type 1 and IEEE 802 SNAP	

Requirement "Ethernet".R14 – Testing SHALL include at least that specified by Table 2 through Table 10

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 – "Ethernet".T00: Baseline operation

Test ID	"Ethernet".T00
Test name	Baseline operation
Test description	The basic operational aspects of the protocol under test shall be demonstrated as a means of checking that gross configuration or other errors are not interfering with the testing process, and that the protocol implementation under test performs approximately as expected when not under test
Reference requirements	Requirement "Ethernet".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 "Ethernet" 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 probable problem with the configuration of the TD or the test environment

Table 3 – "Ethernet".T01: Runt frame tolerance

Test ID	"Ethernet".T01
Test name	Runt frame tolerance
Test description	"Ethernet" frames which are less than 64 octets are sent to the DUT to evaluate the DUT's ability to withstand receipt of such frames
Reference requirements	4.3 M1, 6.6.3, Requirement "Ethernet".R5, Requirement "Ethernet".R6
Test type	Basic robustness
Test status	Mandatory except when the TD hardware is incapable of generating overly short frames
Expected DUT behavior	The DUT SHALL survive receipt of "Ethernet" frames less than 64 B in size
Test object	To probe the robustness of the DUT's ability to withstand receipt of overly-short "Ethernet" frames
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 otherwise-valid "Ethernet" frames addressed to the DUT
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	

Table 4 – “Ethernet”.T02: IEEE 802.2 Type 1 with IEEE 802 SNAP misplaced Q-tag tolerance

Test ID	“Ethernet”.T02
Test name	IEEE 802.2 Type 1 with IEEE 802 SNAP misplaced Q-tag tolerance
Test description	“Ethernet” frames using IEEE 802.2 Type 1 and IEEE 802 SNAP, which contain a Q-tag followed by an EtherType immediately after the frame’s SNAP header’s OUI field, are sent to the DUT to evaluate the DUT’s ability to withstand receipt of such frames
Reference requirements	6.6.3 , Requirement “Ethernet”.R5, Requirement “Ethernet”.R6, IEEE 802 SNAP, IEEE 802.1Q
Test type	Basic robustness
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against receipt of an IEEE 802 SNAP header that contains a Q-tag
Test object	To probe the robustness of the DUT’s ability to withstand receipt of an IEEE 802 SNAP header that contains a Q-tag
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 otherwise-valid IEEE 802.3 frames using IEEE 802.2 Type 1 and IEEE 802 SNAP, addressed to the DUT, where the frame contains a Q-tag as the “EtherType” of the SNAP subheader
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	

Table 5 – “Ethernet”.T03: Q-tag tolerance

Test ID	“Ethernet”.T03
Test name	Q-tag tolerance
Test description	“Ethernet” frames which contain two or more consecutive Q-tags are sent to the DUT to evaluate the DUT’s ability to withstand receipt of such frames
Reference requirements	6.6.3, Requirement “Ethernet”.R5, Requirement “Ethernet”.R6, IEEE 802.1Q
Test type	Basic robustness
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against receipt of “Ethernet” frames with multiple Q-tags
Test object	To probe the robustness of the DUT’s ability to withstand receipt of “Ethernet” frames with multiple Q-tags
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 otherwise-valid “Ethernet” frames addressed to the DUT, but which contains two or more Q-tags
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	

Table 6 – "Ethernet".T04: Jumbo frame tolerance

Test ID	"Ethernet".T04
Test name	Jumbo frame tolerance
Test description	"Ethernet" frames whose total size exceeds 1536 B are sent to the DUT to evaluate the DUT's ability to withstand receipt of oversize frames, which could overflow DUT receive buffers
Reference requirements	6.6.3, Requirement "Ethernet".R5, Requirement "Ethernet".R6, IEEE 802.3, 3.2.8
Test type	Basic robustness
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against receipt of oversize "Ethernet" frames
Test object	To probe the robustness of the DUT's ability to receive and withstand oversize "Ethernet" frames
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 otherwise-valid "Ethernet" frames addressed to the DUT, whose total size exceeds 1536 B
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	

Table 7 – "Ethernet".T05: IEEE 802 unicast destination address tolerance

Test ID	"Ethernet".T05
Test name	IEEE 802 multicast destination address tolerance
Test description	A flurry of "Ethernet" frames is sent to attempt to overwhelm the DUT's receive processing and storage resources. The destination address in the frame is the correct MAC address of the DUT
Reference requirements	6.7.3, Requirement "Ethernet".R10, IEEE 802.3, 3.2.8
Test type	Load stress
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against a flood of received "Ethernet" frames
Test object	To probe the robustness of the DUT's ability to receive and withstand a burst of "Ethernet" frames that explicitly address the DUT
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 "Ethernet" frames with the destination address field containing the DUT's MAC address
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	

Table 8 – “Ethernet”.T06: IEEE 802 broadcast destination address tolerance

Test ID	“Ethernet”.T06
Test name	IEEE 802 multicast destination address tolerance
Test description	A flurry of “Ethernet” frames is sent to attempt to overwhelm the DUT’s receive processing and storage resources. The destination address in the frame is the IEEE 802 Broadcast address
Reference requirements	6.7.3, Requirement “Ethernet”.R10, IEEE 802.3, 3.2.8
Test type	Load stress
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against a flood of received “Ethernet” frames
Test object	To probe the robustness of the DUT’s ability to receive and withstand a burst of “Ethernet” frames with the broadcast destination addresses that implicitly addresses the DUT and all other devices
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 “Ethernet” frames with the destination address field containing the IEEE 802 Broadcast address
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	

Table 9 – “Ethernet”.T07: IEEE 802 multicast destination address tolerance

Test ID	“Ethernet”.T07
Test name	IEEE 802 multicast destination address tolerance
Test description	A flurry of “Ethernet” frames is sent to attempt to overwhelm the DUT’s receive processing and storage resources. The destination address in the frame is randomly selected from within the range of valid multicast address ranges, per: http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml
Reference requirements	6.7.3, Requirement “Ethernet”.R10, IEEE 802.3, 3.2.8
Test type	Load stress
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against a flood of received “Ethernet” frames
Test object	To probe the robustness of the DUT’s ability to receive and withstand a burst of “Ethernet” frames with multicast destination addresses, most of which do not implicitly address the DUT
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 “Ethernet” frames with the destination address field containing randomly selected entries from the multicast address spaces. The TD monitors for any response from the DUT
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	

Table 10 – "Ethernet".T08: Maintenance of service under high load, including network saturation: Raw DPDU flood

Test ID	"Ethernet".T08
Test name	Maintenance of service under high load, including network saturation: Raw NPDU flood
Test description	A flurry of "Ethernet" frames is sent to the DUT 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 "Ethernet".R10
Test type	Load stress
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against a flood of received "Ethernet" frames • Phase 1: The DUT SHALL continue to function, adequately maintaining both essential services and network communications, in the presence of a sudden burst of received "Ethernet" frames, 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 SHALL adequately maintain 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 "Ethernet" frames 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]. The DUT vendor SHALL state a rate limit below which protective measures are not expected to be invoked
Test procedure	The TD sends valid "Ethernet" frames 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.
Expected 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 or rate limiting 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 control throughout the test
Results	Pass or fail
Remarks	The DUT vendor is not required to be able to predict the ging rate at which such protective measures are invoked or such limiting occurs, 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

IANA ARP parameter assignments, http://www.iana.org/assignments/arp-parameters/

— — — — — —