IMEA OneNet® Beta Test DRAFT Standard Test Announcement Application Documentation Package

IMEA OneNet® Beta Test DRAFT Standard
Test Announcement
and Application

On September 21, 2016 at the NMEA International Conference and Expo at Naples Grande Beach Resort in Naples Florida, during the NMEA Luncheon Meeting, NMEA's Director of Standards and the IMEA OneNet Standards Committee announced a call for BETA Testers from any potential equipment manufacturer of a product utilizing the BETA Test Draft of the IMEA OneNet Standard.

Beta testing is a critical and comprehensive validation of the OneNet Standard. Products be developed and tested to work properly and meet the OneNet requirements. In addition, there will be Plugfests to test products for interoperability and interconnectivity. The OneNet standard contains of a number of interrelated and complex modules. For a basic description see the BETA Base Module and the BETA Device Architecture Module which are attached (See Appendix B). Feedback and input to the standard is the number one goal for the acceptance and successful launch of the OneNet Standard for all stakeholders. The IMEA OneNet Standard is the property of NMEA.

A maximum of ten (10) BETA tests slots are available for manufacturers desiring to participate as a BETA Tester. If all ten (10) slots are not filled by October 30, 2016 then we will close the call and proceed with those manufacturers that have signed on.

Objectives:

1. Functional Tests
    - Verifies that the standard meets its functional/feature requirements
2. Configuration Tests
    - Assures all functions work under the combinations within the standards

3. Fix and/or change the requirements of the standard as discovered
4. Fix and/or change the language for enhanced interpretation and clarity
    - Minimize ambiguity within the standard

Scope:

- All requirements and functionality in the OneNet Beta Test Standard in all modules (except Gateways) are expected to be implemented within the respective product(s)
- Gateways will need to fulfill all the functionalities of the Gateway module and all relevant modules
- Manufacturers are expected to maintain a table of issues/questions and possible solutions during the product development phase of the Beta Test. This document will be called Beta Issue Table (BIT).
- Manufacturers are expected to share this table with other Beta Test manufacturers and with NMEA.
- Manufacturers may create scenarios which can help clarify the solution of an issue/question.
- The BIT might result in an applications document.
- Final evaluation for the "public" release of the OneNet Standard

To qualify, a company must:

- Sign the NMEA Confidentiality Agreement (if not already on record)
- Sign the NMEA Copyright Assignment Agreement (if not already on record)
- Agree to design and develop a product utilizing the IMEA OneNet Standard
- Have design engineers attend at least 2 working group meetings to be held in USA during calendar year 2017
    - These will essentially be for discussion to share issues found
    - First meeting will be held November 29, 30, 2016 at the USCG R&D Center in New London,CT.
- Participate in regular Go to Meetings as determined
- Attend at least 2 OneNet Beta Test Plugfests for interconnectivity and interoperability
- Participate in the bulletin board, Trello
    - This encourages collaboration on a regular basis with all members of the Beta Test
- Participate in the collaboration email application, Slack
- Openly share test results with NMEA, Beta Test Members, and the NMEA OneNet Standards Committee
- Not talk to the press during the Beta Test Program

- May not share the Beta Test Standard with other manufacturers. If needed for product development purposes, manufacturers should contact NMEA and receive permission in writing.
- Complete a short exit survey

Included in this Package

- Appendix A: Beta Tester Contract
- Appendix B: IMEA Base Module and IMEA Device Architecture Module
- Appendix C: General IMEA Onenet Product Certification Categories
- Appendix D: Plan and Timeline
- Appendix E: Beta Issues Table

Time:

Applications open from October 1 to October 31, 2016.
The BETA Test period will run from December 1, 2016 thru May 5, 2017.
See the Plan and Timeline which is attached (See Appendix D). Actual times may be adjusted based on actual testing results and feedback.

Manufacturer Investment: To participate a manufacturer will provide an investment of $5,000 to NMEA. At the successful completion of the Beta Test, the manufacturer will be credited for this investment towards other NMEA standard's fees. Successful completion is defined as bringing an IMEA OneNet product to market. If the manufacturer does not complete the Beta Test, or fails to bring a OneNet product to market, the manufacturer will forfeit this investment.

In addition, upon completion of the Beta Test and publication of the OneNet Standard the manufacturer will also receive the **Manufacturer Incentives** as listed below.

To participate, the manufacturer must complete, sign and send the BETA Test Application which is attached. (See Appendix A)

Manufacturer Incentives: NMEA will provide the following incentives:

- The BETA DRAFT OneNet Standard FREE
- The "PUBLISHED' OneNet Standard FREE
- The NMEA Product Code FREE
- If the equipment manufacturer brings a product to market, the OneNet Product Certification will be FREE

As a participating BETA Test company, further benefits to consider include:

- Being amongst the leading edge development and implementation of a new International Standard
- Assisting in debugging a new product
- Developing one of the earliest OneNet products in the market

Other: A tentative Product Certification list is attached (See Appendix C) This list approximates the tentative OneNet product certification generalities. This Appendix C provides a rough insight into some the technical requirements which may be part of the OneNet Product Certification Program. This listing was derived by studying the detailed requirements in the BETA Standard. The items in Appendix C are subject to change.

Contact: To become a BETA Test participant, please contact Steve Spitzer, NMEA Director of Standards.

Steve Spitzer
Phone: (425) 417-8042
E-mail: sspitzer@nmea.org

APPENDIX A
APPLICATION
FOR PARTICIPATION IN
ONENET BETA DRAFT STANDARD
BETA TEST PROGRAM

We have read and agree with the conditions as expressed in this three (3) page document.

MANUFACTURER NAME:

_____

MANUFACTURER AUTHORIZED PERSON: (PRINT NAME AND TITLE)

NAME: _____

TITLE: _____

MANUFACTURER ASSIGNED ENGINEER (S) FOR BETA TEST PROGRAM (PRINT NAME)

NAME: _____

NAME: _____

NAME: _____

MANUFACTURER AUTHORIZED PERSON: (SIGNATURE)

_____

DATED:
_____

ACCEPTED BY NMEA: _____

DATED: _____

APPENDIX B
ONENET BETA DRAFT STANDARD
BASE DOCUMENT MODULE
And
DEVICE ARCHITECTURE MODULE

NATIONAL MARINE ELECTRONICS ASSOCIATION

INTERNATIONAL MARINE ELECTRONICS ALLIANCE

IMEA OneNet® Standard

for

IP Networking of Marine Electronic Devices

IMEA OneNet Base Module

Version 0.013

October 2016

Trademark References:

IMEA OneNet – is a Registered Trademark of the National Marine Electronics Association, Inc.
NMEA 2000 – is a Registered Trademark of the National Marine Electronics Association, Inc.
NMEA - is a Registered Trademark of the National Marine Electronics Alliance, Inc.
IMEA – is a Registered Trademark of the International Marine Electronics Alliance, Inc.

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction

The need exists for standardized data communications between various electronic devices onboard vessels which will enhance communications for safety aboard vessels. This IMEA OneNet® standard was created by an international consortium of marine electronic manufacturers, government and private industries, and the IMEA OneNet Standard Committee. It represents the natural technological evolution of marine interface standards from NMEA 0183 to NMEA 2000 to NMEA OneNet. This standard is maintained by the IMEA OneNet Standard Committee and interested marine electronics manufacturers, expert groups like the United States Coast Guard, and other interested organizations for the primary purpose of boating safety. NMEA 0183 (IEC 61162-1) provides serial-data distribution from a single transmitter to multiple receivers. NMEA 2000 (IEC 61162-3) is Controller Area Network (CAN) based open real-time deterministic CAN networking standard for the maritime industry.

The OneNet Standard for IP Networking of Marine Electronic Devices Network Standard is an open industry standard based upon Internet Version IPv6 and the IEEE 802.3 Ethernet Local Area Network. OneNet provides a common network infrastructure for marine devices and/or services on IPv6. All OneNet application protocols, such as PGN Messages, are designed to use a standard IPv6 network protocol stack. This allows OneNet to coexist with other protocols and services that operate in parallel on the same network (including other marine standards such as IEC 61162-450).

Finally, the standard also specifies mechanisms for connecting NMEA OneNet networks, NMEA 2000 networks, and other networks via gateway devices.

1.1 OneNet Goals

- To specify the transport of NMEA PGN Network Messages over IPv6
- To utilize standard IP network and addressing infrastructure
- To facilitate the safe and secure communication and operations among equipment
- To co-exist with other IP protocols / services on the same cable
- To discover devices and services automatically to create an extendible and scalable network architecture
- To define an open interface to interoperate with current and upcoming open services
- To deliver interoperability with the established industry standards including NMEA 2000 (i.e., establishing gateway rules between NMEA 2000 and OneNet and other protocols)
- To support high-bandwidth applications such as audio/video data transport

1.2 Key Benefits

- **Standardized architecture.** Transport of NMEA PGN Network Messages as well as other protocols over IPv6-based networks (this aligns with M2M, IoT industry trends).
- **Greater bandwidth**. With a range of 100 Megabit to 10 Gigabit transfer speeds directly to OneNet Devices, Ethernet is about 400 to 40,000 times faster than NMEA 2000.
- **Much greater number of potential devices (addresses).** NMEA OneNet allows larger and more complex networks to be created than can be achieved with the 252 address limitation on NMEA 2000. NMEA OneNet contains PGN Virtual Devices that communicate on the network through a single OneNet Device.
- **Greater power capacity.** With Power over Ethernet (PoE), each Physical Device may be separately powered up to 25.5 Watts directly from the Ethernet Switch.(Refer to IEE 802.3at)
- **Ubiquitous technology**. Ethernet is used everywhere in homes, offices and industrial environments and is well understood. Many marine electronic products already implement and support Ethernet.

2 Organization of the Standard

OneNet contains separate but interrelated documents called “modules.” Each module defines minimum requirements and identifies specific capabilities for product development. Normative and informative references are included in each module as appropriate. The complete set of the modules constitutes an Edition. The OneNet Standard, as a whole, will have its own Edition Number. Each individual module will also have its own version number and change history. Any change in a module will effect a change in its version number as well as in the Edition Number (See Figure 1: OneNet EditionsFigure 1 below).

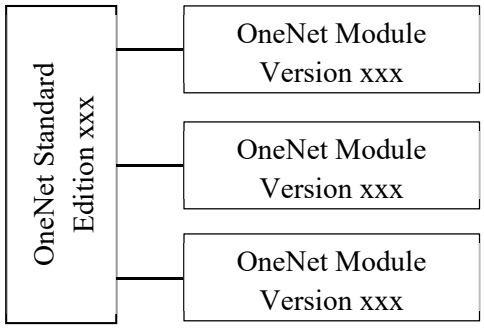


Figure 1: OneNet Editions

Any device that a manufacturer desires to be OneNet Certified must adhere to the requirements within the modules of this edition through validation by NMEA or IMEA.

For this edition of OneNet, the current modules are as follows:

"OneNet Base Module" – provides context for the OneNet standard, defines the basic scope, and explains requirement terminology used throughout all of OneNet Standard modules. Lastly, the Base Module will also contain all definitions for all of the OneNet Standard modules.

"OneNet Device Architecture Module" – introduces the components that comprise a OneNet Device, explains how they are related to each other, and lists the module where the component is described in detail. Also contains requirements for the network protocol stack that each OneNet Device must use to communicate on a OneNet network.

"OneNet Physical Layer Module" – includes the environmental considerations, EMI, Auto-negotiation, MDIX and signaling rates. This module provides a recommendation for a standard connector on the device.

"OneNet Discovery Module" – identifies OneNet discovery of devices, applications and services on the OneNet Network. Discovery provides clients on a local area network with an extendable way to learn what OneNet Devices are present on a network, what each device is, and what its capabilities and services are. Discovery is built on top of the widely adopted protocols mDNS (RFC 6762 Multicast DNS), DNS-SD (RFC 6763 DNS-Based Service Discovery), HTTP (RFC 2616 Hypertext Transfer Protocol), and JSON (RFC 7159 JavaScript Object Notation).

"OneNet Application Information Service Module" – This module describes a service, the OneNet Application Information Service, which provides information about a OneNet Application including product name, NMEA product code, model, NMEA manufacturer code, manufacturer name, serial number, and other metadata.

"OneNet Datagram Protocol Module" – is built on top of IP's User Datagram Protocol (UDP), but defines the extension header mechanisms needed to support security and the PGN transport.

"OneNet PGN Transport Module" – specifies the minimum requirements for implementing NMEA Parameter Group Messages identified by their Parameter Group Number (PGN). These requirements include the IPv6 PGN extension header, utilizing discovery services with the NMEA NAME, application of the ISO Address Claim PGN (NMEA NAME), and minimum required PGNs.

"OneNet Application Security Module" – describes the security model used in OneNet and the protocols needed for OneNet Applications to operate within that model. By default, OneNet Applications operate in an insecure state. The user may transition them into a secure state, known as Secure Mode. Once in Secure Mode, Applications are in possession of a Master Key, which is then used by other modules to authenticate and encrypt network communications.

"OneNet Datagram Security Module" – describes how Datagram Services operating in Secure Mode safeguard the datagrams they send using authenticated encryption. The Master Key is used to establish secure relationships between Datagram Services, known as Security Associations. All datagrams are encrypted and transmitted within the context of a Security Association.

"OneNet Gateway Module" – A OneNet certified gateway will need to meet the requirements in the following modules "Datagram, "Discovery", "Gateway" "PGN Transport", "Physical", " "Datagram Security", "Certification and Test" and "Certification Verification". Gateways connected to OneNet convert data bi-directionally to and from the OneNet protocol format with other protocols, such as NMEA 2000.

"OneNet Certification Verification Module" – describes how a Public-Key Infrastructure is used to verify the certification status of OneNet Applications. It contains requirements for storing and distributing a digital certificate issued as part of the certification process, as well as requirements for retrieving certificates from other Devices or Applications and reporting on their certification status.

"OneNet Certification and Test Module" – contains test method documentation and required results for certifying OneNet Devices. In future versions, OneNet certification may include requirements from other modules than those in this version.

Future versions of this standard may resolve outstanding issues or integrate other technologies. Additional modules will be created and published to meet technology innovations and continual changing needs of the market. Topics may include:

- Functionality to deliver data to remote devices (WAN connectivity)
- OneNet switches, including power and protocol
- OneNet Application configuration through web pages
- Redundant implementation of OneNet networks
- Wireless connectivity

The OneNet standard utilizes the PGN Messages documented in the NMEA PGN Network Message Database. It is not the intention of the IMEA OneNet Standard Committee that the reader possess either a full copy or any prior knowledge of the NMEA 2000 standard. To that end, certain aspects of NMEA 2000 operation are described in the OneNet documents.

2.1 Requirements Terminology

The keywords "MAY", "MUST", "OPTIONAL", "RECOMMENDED, "REQUIRED", "SHALL", "SHALL NOT", and "SHOULD" are to be interpreted as follows in all modules of the NMEA OneNet Standard:

- **May.** The OneNet standard observes the following convention for use of the word "may" related to OneNet requirements: Alternatives and optional items that are allowed in a OneNet Device.
- **Must.** The OneNet standard observes the following convention for use of the word "must" related to OneNet requirements: Items that are required in the device.
- **Optional.** The OneNet standard observes the following convention for use of the word "optional" related to OneNet requirements: Alternative items that are allowed in an NMEA device.
- **Recommended.** The OneNet standard observes the following convention for use of the word "recommended" related to OneNet requirements: A suggestion that if followed could ease development or improve the operation of the device in some manner.
- **Required.** The OneNet standard observes the following convention for use of the word "required" related to OneNet requirements: Items that are mandatory in the device.
- **Shall.** The OneNet standard observes the following convention for use of the word "shall" relate to OneNet requirements: Items that are mandatory in the device.
- **Shall not.** The OneNet standard observes the following convention for use of the words "shall not" related to OneNet requirements: Items that are prohibited in the device.
- **Should.** The OneNet standard observes the following convention for use of the word "should" related to OneNet requirements: A suggestion that if followed could ease development or improve the operation of the device in some manner.

An implementation is not compliant if it fails to satisfy one or more of the MUST, REQUIRED or SHALL or SHALL NOT level requirements for the protocols it implements.

3 Definitions

- **CAN (Controller Area Network)** - A Controller Area Network (CAN bus) is a vehicle bus standard designed to allow microcontrollers and devices to communicate directly with each other. It is a message-based protocol, designed originally in 1983 at Robert Bosch GmbH.
- **Headless Device** - A OneNet Application that does not possess the capabilities of a Human Interface Device.
- **Human Interface Device (HID)** - A OneNet Application that provides the combined capability of accepting basic user input and presenting non-rudimentary output.
- **NMEA NAME** - A unique 64-bit entity that identifies a specific instance of a PGN Virtual Device on NMEA OneNet or a NMEA 2000 Virtual Device on NMEA 2000 networks. It contains information regarding the manufacturer, the device function, and the instance of that function on a

given network. Instance fields of the NMEA NAME may be programmed by the installer of the equipment. The NMEA NAME is described fully in the PGN Transport Module.

- **OneNet Application** - Software that satisfies the requirements documented in these OneNet modules:
  - Device Architecture
  - Discovery
  - Application Information
  - Datagram Service
  - PGN Transport
  - Application Security
  - Datagram Security
  - Certification Verification
  - Certification and Test

  This could be an application on a general-purpose computing device or software on an embedded system.
- **OneNet Datagram Service** - A function of the OneNet Application which implements the OneNet Datagram Protocol Module. A OneNet Application may contain multiple independent OneNet Datagram Services.
- **OneNet Device** - A physical device that executes at least one NMEA-certified OneNet Application.
- **OneNet Network** - Two or more OneNet Devices connected via Internet Protocol, Version 6 (IPv6).
- **PGN** - Abbreviation for Parameter Group Number. Identifies a specific PGN Message.
- **PGN Message** - A single packet message as specified in IPv6 that contains the Parameter Group information to be communicated from a Network Address. The message contains a message priority code, a Parameter Group Number, a destination Network Address, a source Network Address, and data fields. The destination Network Address may be a specific unicast or multicast (Refer to the NMEA PGN Network Message Database).
- **PGN Virtual Device** - A PGN Virtual Device is a OneNet Datagram Service that implements the PGN Transport Module. A OneNet Application may contain multiple independent PGN Virtual Devices. PGN Virtual Device functionality is identified by the Product Class and Function codes in the NAME field of the Address Claim PGN.

4 Revision History

Date	Section	Description

End of the Base Document

NATIONAL MARINE ELECTRONICS ASSOCIATION

INTERNATIONAL MARINE ELECTRONICS ALLIANCE

IMEA OneNet® Standard

for

IP Networking of Marine Electronic Devices

IMEA OneNet Device Architecture

Version 0.003
October 2016

TABLE OF CONTENTS

TABLE OF FIGURES

1 References

1.1 Normative References

- IEEE Standard for Ethernet (IEEE Std. 802.3)
- IEEE 802.1Q-2011: Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks
- RFC 768: User Datagram Protocol
- RFC 793: Transmission Control Protocol
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 4291: IP Version 6 Addressing Architecture
- RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration

1.2 Informative References

- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

2 Scope

OneNet Devices consist of several components that coordinate to provide all required functionality. This module introduces each of these components, explains how they are related to each other, and lists the module where the component is described in detail. It also contains requirements for the network protocol stack that each OneNet Device must use to communicate on a OneNet network.

3 OneNet Device Architecture

OneNet Devices are composed of a series of interrelated elements. The predominant element of a OneNet Device is the OneNet Application. The OneNet Application is a software process that both satisfies the requirements put forth in the OneNet standard and provides some domain-specific functionality for the user. The exact relationship between the OneNet Device and the OneNet Application depends on the nature of the OneNet Device. Certain OneNet Devices are dedicated for maritime use and in most cases these will contain a single OneNet Application. Other OneNet Devices are general-purpose computing platforms that may execute one or more OneNet Applications in parallel with general-purpose software applications.

Both designs require the OneNet Application to interact with a network protocol stack (see §4 of this module) and an mDNS service (described in the Discovery module). These components may be provided by a host

operating system, by third-party software integrated into the OneNet Device, or embedded into OneNet Application firmware (again, depending on the nature of the OneNet Device).

In addition, OneNet Applications must provide several services that communicate through an HTTP connection:

- Application Information Service (see the module of the same name)
- Certification Service (see the Certification Verification module)
- Key Service (see the Application Security module)
- Session Key Service (see the Datagram Security module)

The first two services provide metadata about the OneNet Application and the second two help facilitate the secure communication of application data.

Finally, each OneNet Application contains one or more Datagram Services that are responsible for transmitting and receiving application data (see the Datagram Service module). Each Datagram Service has its own ephemeral UDP port to send & receive unicast messages and send multicast messages. All Datagram Services share IANA-assigned UDP port 10111 to receive multicast messages.

The only Datagram Service currently supported is the PGN Virtual Device, which sends application data formatted as PGN Messages (see the PGN Transport module). Future versions of standard may define additional Datagram Service types.

Note: The formats of all PGN Messages are documented in the NMEA PGN Network Message Database. Within this database each message is assigned a Destination. Messages marked as “Global” are sent as multicast messages on OneNet. Messages marked as “Address” (as in “addressable”) may be sent either as unicast or multicast (see the PGN Transport module for more detail).

The various components that comprise a OneNet Device are summarized in Figure 1(below)

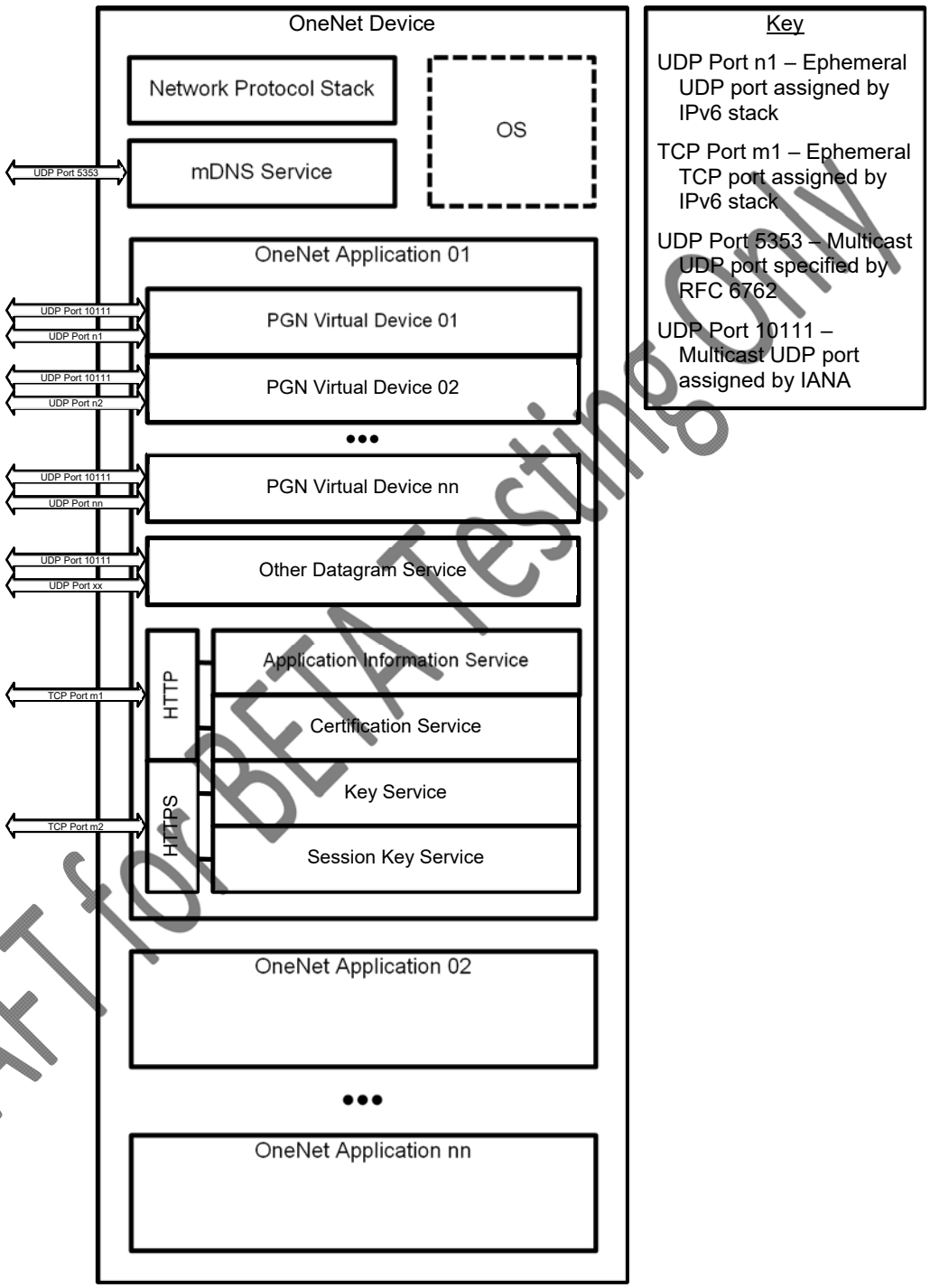


Figure 1: OneNet Device Architecture

4 Network Protocol Stack

OneNet Applications shall utilize a network protocol stack to facilitate communication with the network. This section documents requirements for each layer of the protocol stack.

4.1 Data Link Layer

All OneNet communications shall use 802.3 Ethernet frames. In addition, Devices shall support receiving Ethernet frames with IEEE 802.1Q tags.

4.2 Network Layer

The network layer of the protocol stack shall support the following functionality:

- Internet Protocol Version 6 (IPv6) as described in RFC 2460
- ICMPv6 Echo Request and Echo Reply as described in RFC 4443
- Link-Local Addressing as described in RFC 4291
- Neighbor Discovery as described in RFC 4861
- IPv6 Stateless Address Autoconfiguration as described in RFC 4862
- Duplicate Address Detection as described in RFC 4862
- Multicast Listener Discovery Version 2 (MLDv2) as described in RFC 3810

4.2.1 IPv6 Link-Local Addressing

All OneNet Devices shall have at least one IPv6 Link-Local address as described in RFC 4291. This address shall be configured with IPv6 Stateless Autoconfiguration and Duplicate Address Detection as described in RFC 4862.

OneNet Applications shall use the Link-Local address for all OneNet communications.

4.2.2 IPv6 Global Addresses

If the local network contains an IPv6 router or DHCPv6 server then it is possible that one or more global unicast addresses (as defined by RFC 4291 §2.4) may be assigned to the OneNet Device. OneNet Applications must remain operable in this occurrence but are otherwise not required to support global unicast addresses.

4.3 Transport Layer

The protocol stack shall provide the following transport layer protocols:

- User Datagram Protocol (UDP) as described in RFC 768
- Transmission Control Protocol (TCP) as described in RFC 793

5 Revision History

Date	Section	Description

End of the Device Architecture Module

APPENDIX C

ONENET BETA TEST
GENERAL ONENET PRODUCT CERTIFICATION CATEGORIES
TENTATIVE LIST

Certification Configuration Information

- Model Number
- Description
- NMEA OneNet Edition Number
- NMEA OneNet Modules Versions
- NMEA Device Class & Function Code Database Version
- NMEA PGN Message Database Version
- PGN Virtual Device
- NMEA PGN Messages Transmitted
- Proprietary Message Certification
- Custom PGN Settings (When Different than Default Settings)
- Enhanced Features or Capabilities

Physical Layer

- Environmental
- Extended Storage Temperature
- Radio Frequency Interference Unwanted EMI
- Immunity to Electromagnetic Environment
- Power over Ethernet (PoE)
- External Power
- Standalone switches shall provide PoE capability
- Embedded Switch PoE
- OneNet Physical Device Connector Requirements
- Alternative Connector
    - Connector Documentation
    - Auto_MDIX
    - Fiber Optic Connecor
    - Signaling Rate

Discovery

- Responder
- Application ID
- DNS-SD Service Instance Name
- Services

Application Information

- Application Information Service

Datagram Protocol

- Multicast Listener Socket
- Ephemeral Port
    - Multicast Messages
    - Unicast Messages
- Publishing through OneNet Discovery
- OneNet Fixed Datagram Header

- OneNet Extension Header

PGN Transport

- Datagram Protocol Compliance
- PGN Virtual Device Class and Function
- PGN Extension Header
    - PGN Number
    - PGN DB Version
    - PGN Sequence Number
    - PGN Priority
    - PGN Reserved
- NMEA NAME
    - Encoding NAME for Discovery
- PGN Transport Protocol NAME Implementation
    - Unique Number
    - Manufacturer Code
    - Device Instance
    - Device Function
    - Reserved
    - Device Class
    - System Instance
    - Industry Group
    - Reserved Field
    - Field Programmability of the NAME Instance Fields.
    - Non-Volatile Memory
- PGN Transport Requirement Destination Address
    - Multicast Message Request
    - Unicast Message Request
- Required OneNet PGN Virtual Device Messages
    - Multicast Address Claim Request
    - Unicast Address Claim Request
- OneNet PGN Virtual Device Proprietary Messages
    - Proprietary format
    - Proprietary Certification
    - Proprietary Messages 8 Bytes or Less
    - Proprietary Messages 9 Bytes of More
- Address to NAME Association
- Presence Announcement
    - Response to Request
    - Requesting NAME – Initial Multicast Request
    - Requesting NAME – Subsequent Unicast Request
    - Presence Announcement Process Restart

Application Security

- OneNet Application Requirements
- Master Key
- OneNet Key Service
- Enabling Secure Mode
- Disabling Secure Mode on a HID
- Disabling Secure Mode on the Network
- Forcing Secure Mode to be Disabled on Headless Devices

Datagram Security

- Application Requirement
- Security Associations
    - Creation
    - Transition
- OneNet Session Key Service
- OneNet Message Encryption and Decryption
- Encryption
- Decryption
- ESP Message Format

Gateway

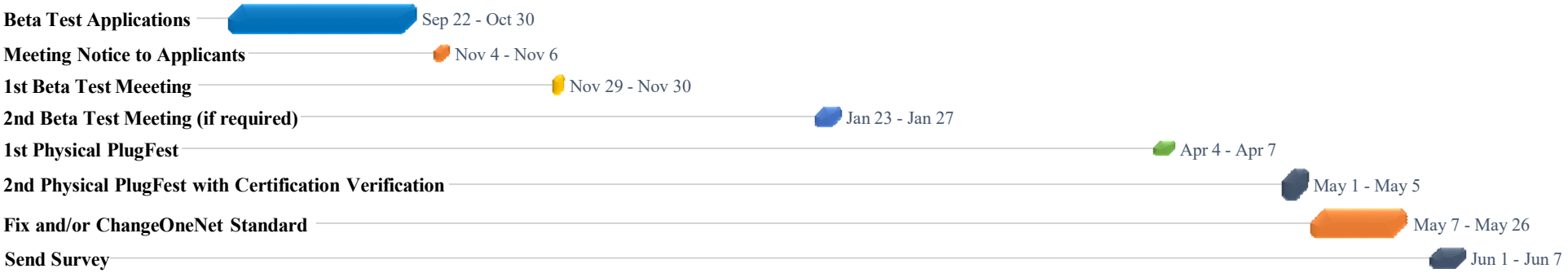
- Gateway between NMEA 2000 and OneNet
- NMEA 2000 Virtual/PGN Virtual Creation
    - OneNet Discovery and NMEA 2000 Virtual Device Creation
    - NMEA 2000 address claim and PGN Virtual Device Creation
- PGN Translation Requirements
    - Rules for Broadcast PGN Conversion
    - Rules for Destination Address PGN Conversion
    - Fast Packet on NMEA 2000
    - Transport Protocol on NMEA 2000
- Field Configurable Capability
- Buffering
- Gateway between NMEA 0183 and OneNet

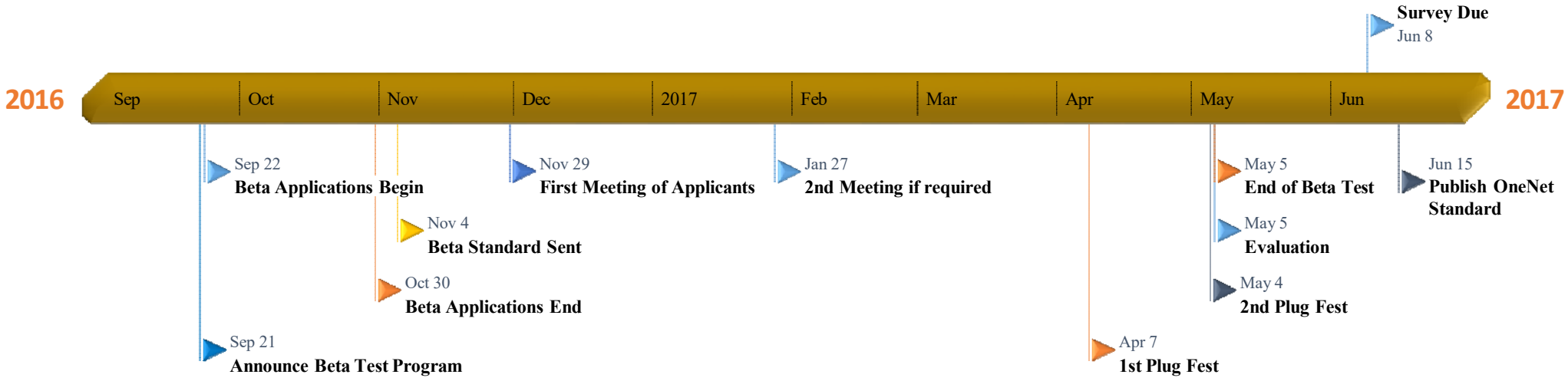
Certification Verification

- OneNet Application Requirements

Appendix D
OneNet Beta Test Timeline
September 21, 2016
to
June 15, 2017

Note: This timeline is subject to change based on a number of factors including, participant input, meeting requirements and Plug Fest evaluations.





Appendix D OneNet Beta Test Timeline

Milestone(s)	
Date	**Description**
09/21/2016	Announce Beta Test Program
09/22/2016	Beta Applications Begin
10/30/2016	Beta Applications End
11/04/2016	Beta Standard Sent
11/29/2016	First Meeting of Applicants
01/27/2017	2nd Meeting if required
04/07/2017	1st Plug Fest
05/04/2017	2nd Plug Fest
05/05/2017	End of Beta Test
05/05/2017	Evaluation
06/08/2017	Survey Due
06/15/2017	Publish OneNet Standard

Task(s)			
Duration	**Start Date**	**End Date**	**Description**
39	09/22/2016	10/30/2016	Beta Test Applications
3	11/04/2016	11/06/2016	Meeting Notice to Applicants
2	11/29/2016	11/30/2016	1st Beta Test Meeeting
5	01/23/2017	01/27/2017	2nd Beta Test Meeting (if required)
4	04/04/2017	04/07/2017	1st Physical PlugFest
5	05/01/2017	05/05/2017	2nd Physical PlugFest with Certification Verification
20	05/07/2017	05/26/2017	Fix and/or ChangeOneNet Standard
7	06/01/2017	06/07/2017	Send Survey

APPENDIX E

ONENET BETA TEST
BETA ISSUES TABLE
(BIT)
TENTATIVE LIST

MANUFACTUTER:	COMMENT ENTERED BY:	DATE ENTERED:	ISSUE: SECTION NAME LINE NUMBER	PROPOSED SOLUTION