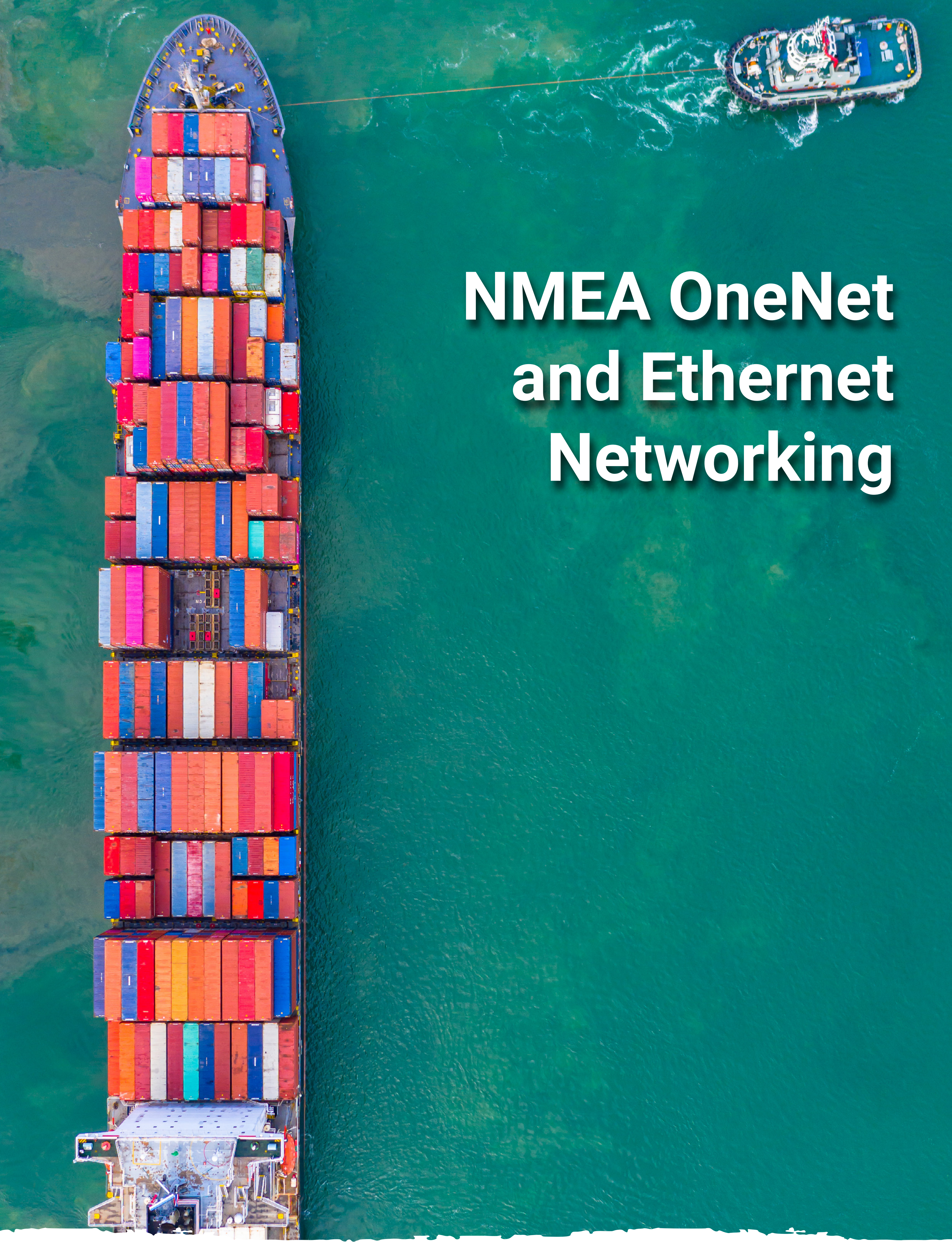


NMEA OneNet and Ethernet Networking

NMEA® OneNet Actisense®

Contents

What is NMEA OneNet?

Who are the NMEA?

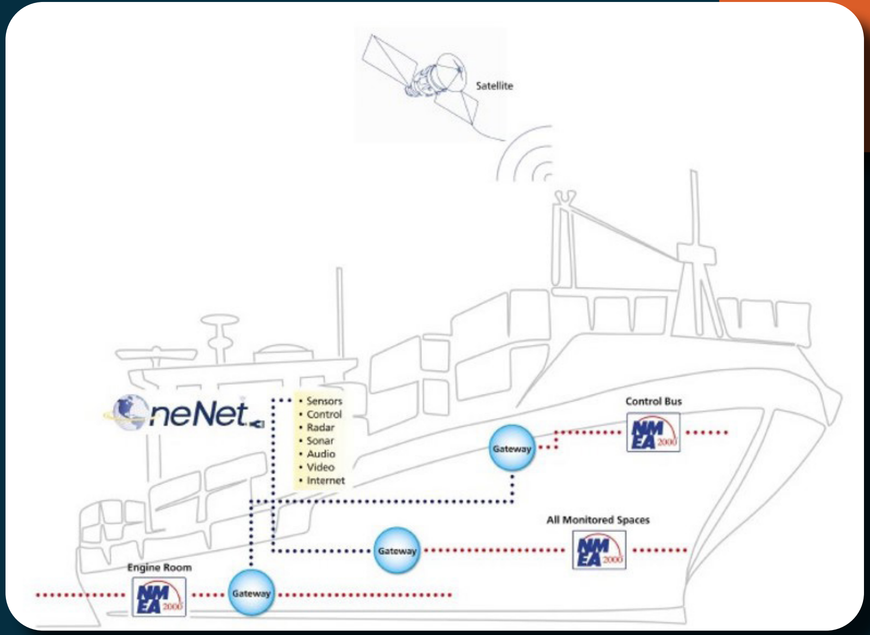
The NMEA stands for National Marine Electronics Association. In a nutshell, they're a not for profit organisation whose mission is to improve data communications between marine electronics manufacturers. Read more at www.nmea.org

What is OneNet?

NMEA OneNet is the third generation NMEA Standard for marine data interfacing and networking, operating on Ethernet, it has the power to bridge all three NMEA Standards together into a combined data network. OneNet is an open industry standard, based on the power of Internet Protocol v6 (IPv6), it provides a standard method for sharing NMEA 2000 data over a Local Area Network (LAN) today and globally in the future.

OneNet is not designed to replace NMEA 2000, instead the purpose is to enhance NMEA systems, and overcome some of the limitations we have seen with NMEA 0183 and NMEA 2000. By adopting Ethernet, we can connect multiple different networks together via switches and gateways, creating one synchronised network, containing 0183, 2000, Radar, Sonar and Video.

> *"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 parallel on the same network (including other marine standards such as IEC 61162-450). The standard also specifies mechanisms for connecting OneNet networks, NMEA 2000 networks, and other networks via gateway devices. Like NMEA 2000, all OneNet products will need to be certified by the manufacturer and verified by NMEA."* – **NMEA**



Key Terms

OneNet Device - A physical device that executes at least one NMEA-certified OneNet Application.

OneNet Network - Two or more OneNet Applications connected via Internet Protocol, Version 6 (IPv6).

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.

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. The message contains a message priority code, a Parameter Group Number, a destination address, a source address, and data fields. The destination address may be unicast or multicast (refer to the NMEA Network Message Database).

Mapped - A virtual representation, managed by a gateway, of a device on a different network.

Connectors

There are 3 types of defined connector for NMEA OneNet certified devices:

1 The Standard connector and those for use in exposed environments is an X-Coded M12. This X-Coded connector must be rated to a minimum of IP67.

2 For protected environments, a standard RJ45 can be used. There is an option to use a female RJ45 connector in an exposed environment, but the connector itself must be in a 'cavity' which is protected. The design of the cavity must be submitted to the NMEA for approval before the product can be released.

3 The third connector type is **Fibre Optic**. These are special use case connectors, however there are currently no specifics around how this connector must look, work and integrate. The NMEA states that they must reach the requirements of ANSI/TIA/EIA 568D. In future, we will see a OneNet standardised connector set-out for Fibre Optics.

Ethernet Basics

Ethernet is the typical method used for creating wired networks, either LAN (local area network) or WAN (wide area network).

Networks have 7 layers, which are defined as the following:

1. **Physical Layer**
2. **Data Link Layer**
3. **Network Layer**
4. **Transport Layer**
5. **Session Layer**
6. **Presentation Layer**
7. **Application Layer**

Physical Layer

There are a number of different variants of the physical layer, but the most commonly used is a category 5 or 6 cable, with an 8P8C (RJ45) connector. These can be made up of coax cable, twist-ed pair cabling, or optical fibre. Usually, we see twisted pair cabling for the 'standard' style home network which is 10BASE-T or 100BASE-T.

Data Link Layer

The Ethernet Data Link Layer is split into two parts, the Logical Link Control (LLC) and the Media Access Control (MAC). LLC is responsible for routing the data between devices or nodes, and the MAC address is done using hardware addresses assigned via Network Interface Cards (NIC) to identify individual devices on a network.

Ethernet has two units of data transmission and receival; Packets and Frames. Data sent over an Ethernet network is split into Frames, which contains both a header and a payload.

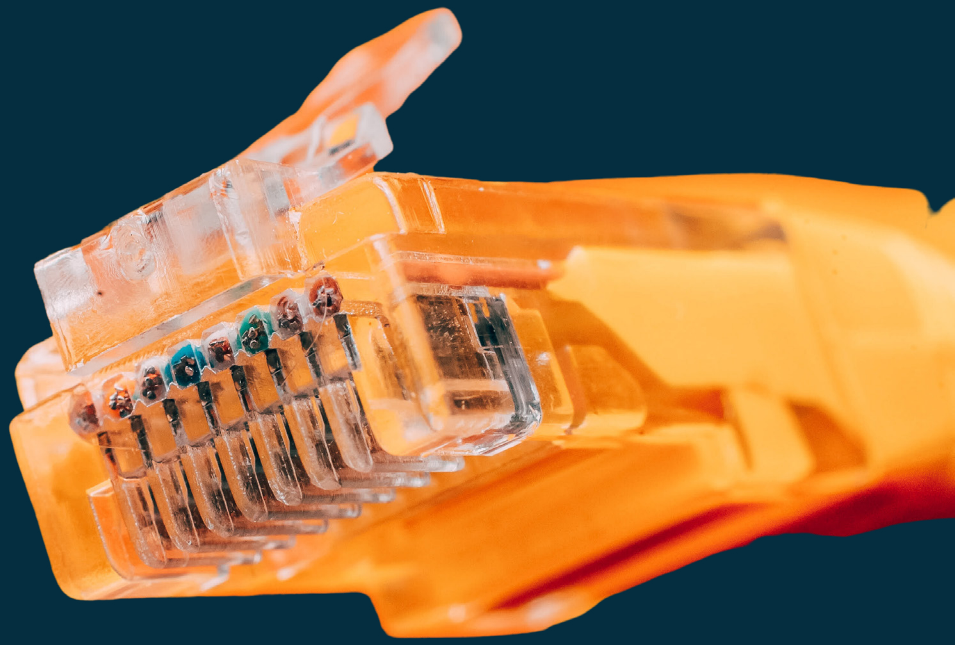
The header is 14 bytes, compiled with 3 parts;

- The first 6 bytes is the destination MAC address, the second set of 6 bytes are the source MAC address, and the final two bytes are the length.
- The data or payload section of a frame is where real data is contained. This can be 46 – 1500 bytes long.
- Each frame is wrapped in a packet which contains several pieces of information to correctly establish connection with another device, and also to indicate where each frame starts and stops.

There is a crucial algorithm running underneath the data link layer, called Carrier Sense Multiple Access with Collision Detection (CSMA/CD). CSMA/CD is standard in Ethernet networks, and is used to reduce data collisions and increase success rates.

The algorithm will send a bit of information onto the network to see if any collisions occur. If this first bit does not collide, then it will send the rest of the bits out, but will also continue to monitor for collisions whilst doing so.

If there is any data collision, then the algorithm will stop sending data, wait for a calculated period of time, and then make a second attempt at sending the data from the first bit again until they are all sent with no collisions.



IPv6 Explanation

OneNet utilises Internet Protocol Version 6 (IPv6), the latest IP Standard. A home network typically uses IPv4, and this is what we are familiar with. Unfortunately, we have now reached the maximum number of available IPv4 addresses.

To overcome this issue with IPv4, and hopefully never run into the same problem with IPv6, the addresses were changed from 32-bit to 128-bit.

To provide a comparison between the two Protocols, here's the number of available addresses when both standards were created:

IPv4: 4,300,000,000

IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456

Understanding IPv4 and IPv6 addresses

Due to IPv6 changing to 128-bit addresses, they look very different when compared to IPv4 32-bit. As a 128-bit address would be extremely long, it is displayed as Hexadecimal, rather than the decimal standard we are familiar with on a 32-bit address. To understand this better, we must first grasp the concept of 'bytes', 'bits' and 'nibbles', and how these differ between decimal, binary and hex.

Hex, Decimal and Binary

The common unit for computing and networking is a byte. A byte is comprised of 8-bits. For exam-ple, a 32-bit OS is 4 bytes (4*8=32). Bits and bytes can be displayed in many different methods of numerical systems, which include decimal, binary and hex.

- Decimal is base 10, where a single byte can contain a value of 0-255.
- Binary is base 2, where each value (0 or 1) is 1 bit.
- Hexadecimal is base 16, where one hex character is 4 bits (0 – F, or 0-15 decimal),

Note: 4 bits (one hex character) is called a 'nibble', which is a small or half byte.

Hex Value	Decimal Value	Binary Value
00	0	0000 0000
01	1	0000 0001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
09	9	0000 1001
0A	10	0000 1010
0B	11	0000 1011
0C	12	0000 1100
0D	13	0000 1101
0E	14	0000 1110

This becomes relevant when we look at an IPv6 address. As hex values use 4 bits per character, and the address is 128-bits, this means the IP address displayed in Hex is only 32 characters long... (You can imagine how long it would be if you were to use the decimal equivalent!).

Unlike an IPv4 address which uses dotted decimals (192.168.4.1), an IPv6 Hex address uses Colons (':') as the separation method. These values are grouped into blocks containing 4 characters each (16-bit), meaning we have 8 overall groups.

Here is an example of an IPv6 address in full: FE80:CD00:0000:0CDE:1257:0000:211E:729C

It is acceptable to shorten these addresses as they allow for 'leading zero omission' and shortening of any 4 character sequence containing only zeros. This would result in the following:

FE80:CD00:0000:0CDE:1257:0000:211E:729C

↓

FE80:CD00:0:CDE:1257:0:211E:729C

It is also acceptable to shorten consecutive blocks only containing zeros using two '::'. This can only be done once per address, and in a scenario where multiple occur, only the furthest left sequence may be shortened.

The IP address is split into 2, where the first (upper) 64 bits are for network and routing. The second (lower) 64 bits are taken from the MAC address. A MAC Address is 48 bit, which is then converted to the 64-bit EUI (Extended Unique Identifier) format.

Linking IPv4 and IPv6 together

The adoption of IPv6 will be fairly slow, and thus a large percentage of systems and networks will be using IPv4 for some time yet. Unfortunately, they can't just 'work' together, and require some transition mechanisms or gateways. Fortunately, there are ways to achieve this. These are;

- Dual IP Stacks
- Tunnelling
- Dual Stack Proxy servers using NAT-64 (Network Address Translation)
- IPv4 Mapped IPv6 addresses

There are other methods, some still being developed and some already deprecated, thus this list is not extensive. Dual stack implementation is currently regarded as the easiest and most fluid way to integrate and eventually migrate to IPv6. Essentially this means the device or network object has both an IPv4 address and an IPv6 address, allowing it to communicate with both IPv4 and IPv6 devices.

Power Over Ethernet (PoE)

Power over Ethernet is technology that enables power to be sent via Network cables. This enables PD (Powered Devices) to operate with just the network cable connected, rather than a separate cable for power.

PoE works with no special cables or connectors, it utilises the 8 wires (4 pairs) already found in a standard Cat5e cable. They can be used to send both power and data over the same pair, or separated between power pairs and data pairs depending on the connection method and speed.

Methods of transmitting power

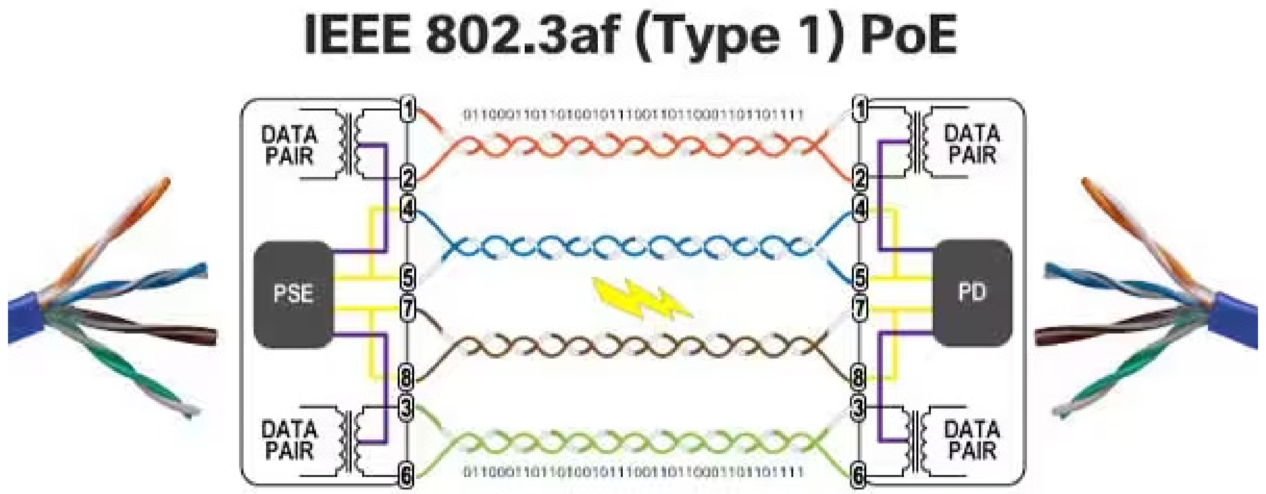
There are 3 standard methods for transmitting power, which are '**Alternative A**', '**Alternative B**' and **4PPoE**. These are standardized in IEEE 802.3.

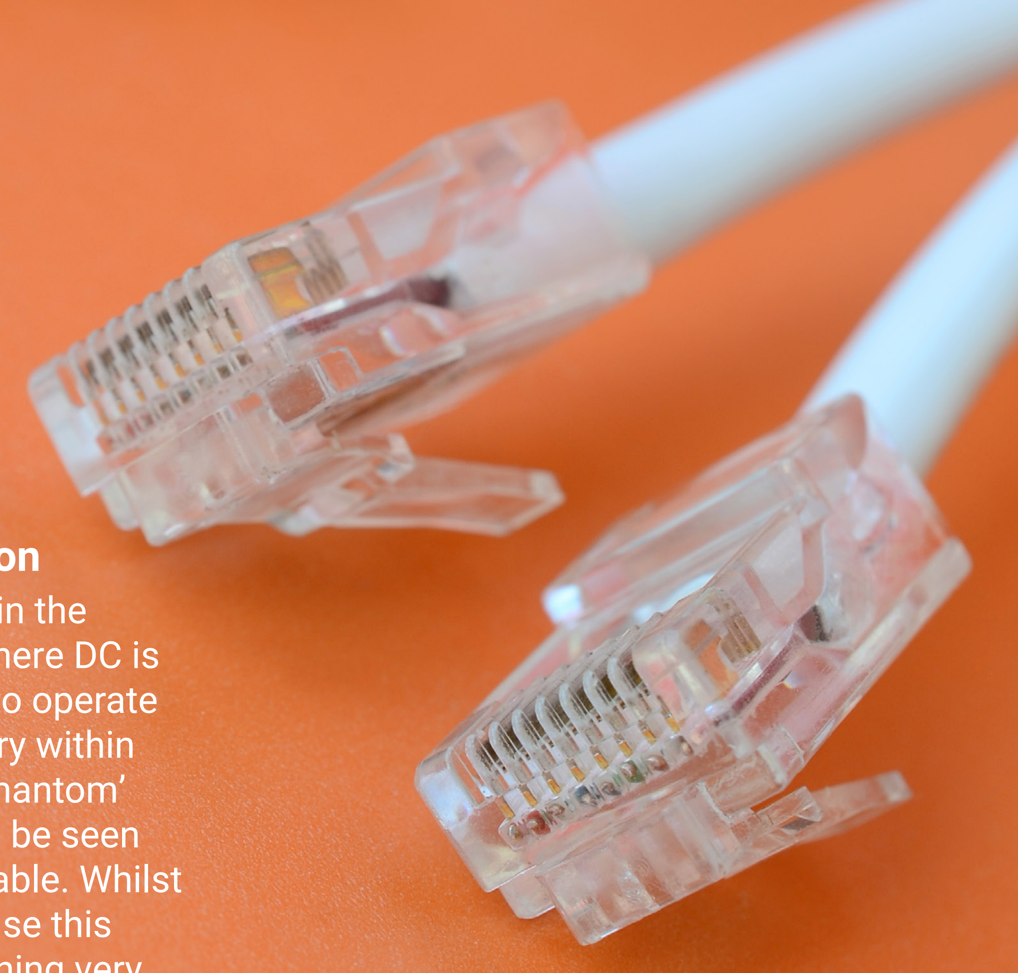
Alternative A and B are utilised for 10BASE-T, 100BASE-T and 100BASE-TX where only two of the four pairs in a cable are being used for data transfer. 4PPoE is used for higher speed connections of 1000BASE-T, 2.5GBASE-T, 5GBASE-T and 10GBASE-T because all four pairs are being used for data transfer.

Alternative A (common-mode) uses the same wires for data and power in both 10 and 100Mbit connections. This is achievable using a technique very similar to Phantom Power (see page 11).

Alternative B (spare-pair) makes use of the spare two pairs not being used for data transfer, by transmitting power over the two un-used pairs.

4PPoE (4 pair) utilises all 8 wires (4 pairs) within a category cable for data transfer, allowing for much higher speeds. This also allows for all 4 pairs to have power added to them, which enables much higher power devices to utilise PoE.





A short geek mode section

Phantom Power is common in the audio equipment industry, where DC is sent via microphone cables to operate the internal electronic circuitry within the microphone. The term 'phantom' is because the power cannot be seen because there is no power cable. Whilst Common-Mode (A) doesn't use this exact method, it uses something very similar.

The way this works is the power is applied to each pair of the data wires using a common voltage. As differential signaling is used with twisted-pair Ethernet, it means that the power won't interfere with the data. The common voltage is taken off / extracted via the Centre Tap, leaving only the differential voltages. This voltage is usually between 44 and 57 volts, typically at 48-50V.

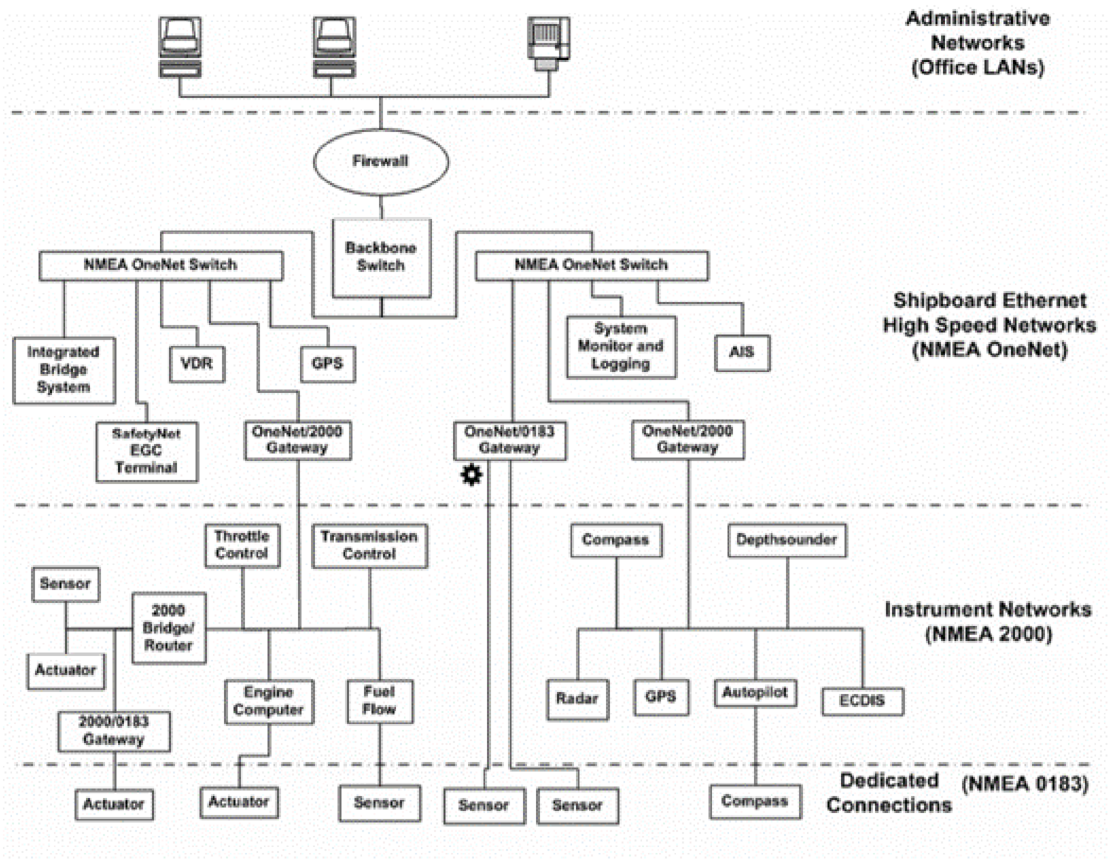
For example; If 50V is applied, then the power signal (lets say bit 0) is 50V, whilst the data signal (bit 1) is now 55V. When this 50V common voltage is removed at the other end, left is bit 0 @ 0V and bit 1 @ 5V. This 0V and 5V is your data, which is then sent to the differential receiver for data.

PoE With OneNet

OneNet supports PoE as the standard is based upon IEEE 802.3 Ethernet Local Area Network. Specifically, it will allow up to 25.5W of power to be transmitted via Ethernet, following IEEE 802.3at PoE+. This offers a much greater power capacity.

It is worth highlighting here that whilst there are older Category 3 (Cat3) cables etc. being used for PoE, the OneNet standard details that a minimum of Cat5e cable is to be used. Everything referenced to Ethernet cables and wiring in OneNet is from Cat5e or higher. Cat6 and Cat6e cable for example is also supported for higher speeds.

Cables that pre-date Cat5 such as Cat4 are untwisted pairs of wires, which are more susceptible to interference than twisted pair wires.



PoE Benefits

Network Expansion

Having power available on the network already means that expansion of the network is simple with the use of PoE Injectors, and switches. The maximum length of an Ethernet network is not unlimited, but it is far greater than that of NMEA 2000 when Ethernet switches are used.

Flexible Installations

A device which requires power from a battery or wall socket is limited on the installation location. Having devices which are powered via a network connection means there is no longer a restriction on installation location or distance from a socket / battery. Alongside this, when installing in tight areas such as bulkheads, two cables will always be more difficult to fit than one. Halving the cable number creates double the space to work with.

Time + Cost

As there is no requirement for socket or battery connection with power cables, the time of installation is reduced alongside the cost of installation thanks to having no separate power cabling. A lower installation time means a lower cost when looked at from a rate/hr perspective.

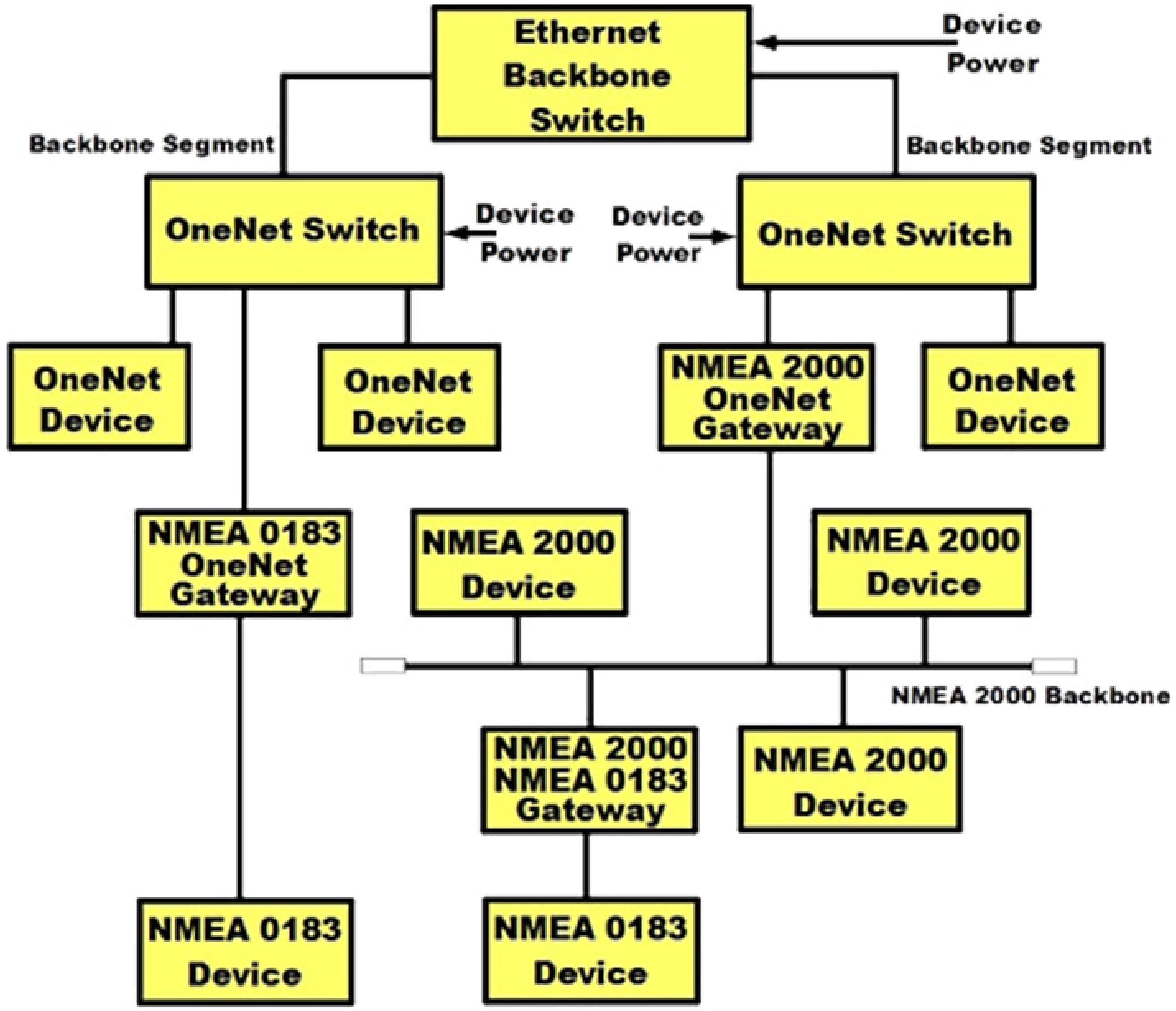
Reliable and Safe

Any power delivered over Ethernet is safe as PoE technology is intelligent, with an interfacing process between the PSE (Power Sourcing Equipment) and the PD (Powered Device) which enables the device to be detected by the source, and determine how much power is needed to avoid over-loading and wasting power. This is a process called 'signature detection' where the PSE will supply a lower voltage to detect a 25KOhm resistance before providing a higher voltage once the PSE has determined the device is a PoE PD. This is a characteristic of IEEE 802.3 PoE Devices.

On larger installations with a higher number of devices, power management is important to ensure all devices are reliably powered. The power budget allocation is done using the negotiation between the PD and the PSE, allowing only the required amount of power to be allocated.

Using OneNet with NMEA 0183

OneNet is designed to work with both NMEA 0183 and NMEA 2000. As shown in the diagram below, there will be OneNet Gateways for both NMEA 0183 and NMEA 2000. This can reduce networks costs by a significant amount for the owner / installer, as there is no need to replace existing NMEA 0183 instruments with NMEA 2000.



NMEA OneNet Block Diagram

OneNet security

Network security is a priority on any network today, especially when it comes to commercial vessels. NMEA OneNet has made security a priority from the very beginning and uses a security model where the user creates a OneNet Secure Network and then adds OneNet Applications to that network using a process called 'pairing' to create a robust secure data network.

Each OneNet Application (running on a physical device) must successfully pass the NMEA Certification Tool tests in order to be issued a certificate that can be used to join a secure OneNet network. It is an important distinction to make that whilst the physical device, such as a tablet or mobile phone is not NMEA Certified, the OneNet Application running on it must be NMEA Certified for it to join a secure OneNet network and gain access to the data on it.

The OneNet network can optionally be left in an open (unsecure) state to allow use with non-certified devices if the user should require this.

- OneNet Applications operate with Secure Mode enabled or disabled
- Once paired, a device can both receive and transmit data to other devices that are also in Secure Mode
- Applications with Secure Mode enabled possess a copy of a 2048-bit symmetric Master Key
- Master Key serves as the basis for securing the network
- Master Key is unique to each network
- Does not rely on public key infrastructure (PKI), avoiding problems with certificates and revocation
- Secure Mode enabled from a Human Interface Device (HID)
- Secured with Transport Layer Security (TLS)

Benefits of OneNet

NMEA OneNet is in no means designed to replace NMEA 2000, rather it is meant to work along side NMEA 2000 (and NMEA 0183), to bring several benefits to a pre-existing 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 parallel on the same network.

The standard also specifies mechanisms for connecting OneNet networks, NMEA 2000 networks, and other networks via gateway devices. Like NMEA 2000, all OneNet products will need to be certified by the manufacturer and verified by NMEA.

Increased Bandwidth

OneNet has a much larger bandwidth than NMEA 2000. Whilst NMEA 2000 operates at 250Kbits/sec, OneNet will range from 100Mbit to 10Gbit/sec directly to OneNet devices, making it 400-40,000 times faster. Due to this greater bandwidth, OneNet will be able to support high Bandwidth messages such as radar, video, and sonar (these will be future standardised PGNs).

Greater Physical Device Limit

Alongside the bandwidth improvement with OneNet, comes the increase in the number of physical devices that can be on the network. NMEA 2000 is limited to 60 physical devices per network section. This physical device limit can be expanded by adding NMEA OneNet switches. NMEA 2000 network bridges are required to join sections of networks together, whilst OneNet can join multiple NMEA 2000 networks together using their gateway technology.

Increased PGN Limit

OneNet realistically has no PGN limit. Whilst NMEA 2000 is limited to 411 standard, and 512 proprietary PGNs, in theory, OneNet does not have a limit.

Power Over Ethernet (PoE)

Something which often adds complexity to large NMEA 2000 networks is power implementation. High power (high current draw) devices need to be powered independently, whilst low power devices can be powered from the backbone directly. This means that on larger installations, network power limits can be reached quickly. OneNet can overcome this using PoE. PoE is available for devices which support it, and the network power limit can be expanded using network switches. Each OneNet device may be powered separately up to 25.5Watts from the Ethernet switch.

Useful NMEA Resources

Need further support with your NMEA network? Here is a directory of useful contacts:

National Marine Electronics Association

Email: info@nmea.org

Tel: 410-975-9425

Website: www.nmea.org

Actisense (Active Research Ltd)

Technical Support: support@actisense.com

Stock availability & distributor enquiries: sales@actisense.com

Tel: +44 (0) 1202 746682

Website: www.actisense.com

Visit our extensive Knowledge Base for frequently asked questions: www.actisense.com/knowledge-base