

EtherNet/IP Interoperability Recommendations

Kevin Knake – HMS Industrial Networks &
Jim Gilsinn – NIST

Presented at the ODVA
2009 Conference & 13th Annual Meeting
February 24-26, 2009
Howey-in-the-Hills, Florida USA

Abstract

The EtherNet/IP™ interoperability recommendations are a result of work generated by the ongoing series of EtherNet/IP Implementors Workshops. The recommendations were created to promote EtherNet/IP device interoperability through product functionality recommendations and interoperability validation events called PlugFest. The document *Recommended Functionality for EtherNet/IP Devices* has been updated to include product implementation clarifications, performance metrics and new interoperability recommendations. This paper describes the new performance and interoperability recommendations for EtherNet/IP devices.

Keywords

EtherNet/IP, interoperability, recommendations, performance, plugfest, implementors workshop, functionality

Introduction

The EtherNet/IP™ Implementors Workshop series started shortly after the release of the EtherNet/IP¹ standard. Industrial Ethernet was relatively new and device vendors understood that EtherNet/IP was more complex than DeviceNet and other traditional fieldbus networks. Building on the experience from DeviceNet and the initial interoperability issues found with its early adopters, several vendors proposed a workshop concept with the following objectives:

- Educate product developers on EtherNet/IP and Industrial Ethernet technologies.
- Provide a collaborative forum for developers to discuss common issues and solutions.
- Promote EtherNet/IP device interoperability through product design recommendations and interoperability validation events (PlugFest).
- Provide a better vendor and end-user experience implementing an EtherNet/IP network.

The EtherNet/IP Implementors Workshops are a series of technical meetings attended by vendors and end-users interested in developing or using EtherNet/IP products. Meetings are typically two days in length and held three times per year. There are currently two workshop series, one is held in North America and the other is held in Europe.

One of the primary work products from the Workshop is a set of EtherNet/IP interoperability recommendation documents. The interoperability recommendations are not part of the EtherNet/IP specification and thus are not required to be implemented by vendors. Rather, the documents provide product design recommendations to vendors on what EtherNet/IP functionality they should implement in their device to help ensure interoperability between devices and provide a minimum level of functional capability required for most user applications. The

¹ Certain commercial products and services are mentioned in this paper for informational purposes only and do not represent a recommendation or endorsement by the National Institute of Standards & Technology or the U.S. Department of Commerce.

recommendations have been validated through vendors' EtherNet/IP experiences, workshop discussions, and PlugFest testing results.

PlugFest is a multi-vendor EtherNet/IP interoperability testing event. It provides feedback to the developer in regards to any possible interoperability problems before they are discovered in the field. Testing is conducted based on a formal set of procedures that test products for compliance to interoperability recommendations. PlugFests are held twice a year, typically in the spring in North America and the fall in Europe.

The EtherNet/IP Interoperability Advisory Test is administered at PlugFest events. Devices with a valid Declaration of Conformity are eligible for the EtherNet/IP Interoperability Advisory Test. If the device successfully passes interoperability testing, the passing results are indicated on the product's Declaration of Conformity. The advisory mark indicates that a product implements the additional functionality recommended in the EtherNet/IP Interoperability Recommendation documents. Elements of the current advisory test *may* become part of the standard conformance test.

Information and scheduling of all workshops and PlugFests can be found on the Open DeviceNet Vendor Association (ODVA) website at <http://www.odva.org>.

Further revisions of the EtherNet/IP interoperability recommendation documents are anticipated as work progresses in the EtherNet/IP Implementors Workshop and other ODVA Special Interest Groups (SIGs). The document *Recommended Functionality for EtherNet/IP Devices* [2] was revised in November 2008 to include product implementation clarifications, performance metrics, and new interoperability recommendations. The remainder of this paper describes the new performance and interoperability recommendations for EtherNet/IP devices.

Performance Testing History

EtherNet/IP products are based on standard Transmission Control Protocol / Internet Protocol (TCP/IP) and Ethernet technologies and can be implemented with commercial off-the-shelf (COTS) technology. Ethernet is the world's most popular networking technology and vendors have many low-cost and widely available hardware and software options to choose from when developing an EtherNet/IP product. While COTS hardware and software can provide acceptable performance, the product developer must take proper care in hardware and software design to achieve optimal performance for the intended control application.

When EtherNet/IP and other industrial Ethernet networks were being developed, questions arose as to how well they would operate on large networks with a variety of traffic conditions. In older implementations of Ethernet using 10 Mbps, shared-media bus networks, the network was the bottleneck for communications. A small number of devices could easily outpace the ability for the network to support their desired bandwidth. Also, the back-off and retransmission features built-in to the TCP/IP stack worked well for normal desktop computers, but were not deterministic enough for the types of communication needed in the industrial environment. With more recent network architectures using 100 Mbps and faster switching technology, the network is no longer the bottleneck that it once was. The main issue that remains for users of industrial Ethernet equipment is how well the device itself will perform under different network traffic loads.

While devices are in development, performance may not be a consideration for the vendor. Vendors are concerned with making a device functionally correct and may not consider the device's performance until the final stages during robustness testing. Many factors can affect a device's network performance, including microprocessor choice, Ethernet controller choice, network stack design, and operating system overhead. Problems may not be noticeable on the laboratory bench or even in prototype networks, but may only show up in user's plant floor networks as intermittent problems.

The EtherNet/IP Implementors Workshop series started working on developing performance tests, recommendations, and requirements at Workshop #5 in May of 2002. A working group developed a series of documents that outlined performance test terms and methodologies for EtherNet/IP devices. [4][5] During that process, tests were conducted at the PlugFests to verify that the terms and methodologies produced the desired results.

In 2006, ODVA and the National Institute of Standards & Technology (NIST) signed a cooperative agreement to develop and commercialize an EtherNet/IP performance testing system capable of conducting the tests described in the methodology document. The project finished at the end of 2007 with the development of the EtherNet/IP Performance Test Tool. ODVA is using this test tool as the basis for its performance testing service, which began in the fall of 2008.

PlugFest Performance Tests

EtherNet/IP real-time communications typically use cyclic message streams sent between the adapter and scanner. Control loops based on this type of communications count on both devices to maintain the desired packet interval to operate correctly. Standard digital design states that the communications used in the control loop should operate much faster than the overall loop; however, this is not always the case. For tightly coupled control loops, errors in the packet interval may affect the performance of the entire control system in unusual ways.

The performance test system has been developed to connect directly to the device under test (DUT) without any need for additional network connectivity hardware. The only piece of network hardware utilized in the performance test system is a network tap that allows the test system to capture all of the packets in the test with minimal latency. Figure 1 shows a representation of the hardware setup for the performance testing.

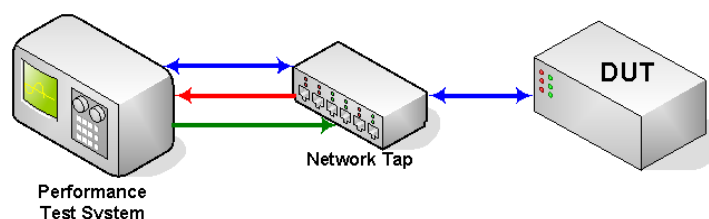


Figure 1 – Performance Test System Setup

The performance test cases chosen for the PlugFests have been tailored to provide the greatest benefit to vendors in the time allotted. The PlugFest tests can be conducted in the 30 to 45 minutes allotted for each device participating in the PlugFests and give the vendor feedback based on actual test cases encountered by vendors in the field.

Each of the tests uses the same basic methodology.

1. Begin recording traffic.
2. Establish a connection with the DUT.
3. Begin transmitting background traffic based on the particular test.
4. Wait for a given amount of time.
5. Stop transmitting background traffic.
6. Close the connection with the DUT.
7. Stop recording traffic.
8. Analyze the traffic and report the results.

The five test cases chosen for the PlugFest performance tests can be grouped into three main categories: baseline testing, steady-state testing, and burst testing. The first test run on any device during the performance testing is a baseline test. Baseline testing establishes the best performance a device is capable of achieving. This situation is similar to prototype or laboratory bench testing of the device. Steady-state testing establishes how well the device performs while in the presence of a moderate amount of background traffic. Steady-state testing is broken into two subcategories: managed and unmanaged. Managed steady-state testing simulates a running industrial network that utilizes managed switches that are setup to filter multicast traffic. Unmanaged steady-state testing simulates a running industrial network that utilizes unmanaged switches or managed switches that are not setup to filter multicast traffic. Burst testing adds a short burst of network packets to the two steady-state background traffic cases to determine how well the device reacts to random events that may occur on a plant floor network.

The amounts of background traffic for each test were chosen specifically to simulate cases that have been found on vendor's networks. The steady-state background traffic cases simulate a large flat network with approximately two hundred industrial devices. While this number may seem excessive, it is not uncommon and can easily occur in networks with multiple industrial cells attached to the same broadcast domain. During the development of the test

system, the number 180 was chosen. This allows for simulated devices outside that range to be used by the performance test system without the possibility of interfering directly with the DUT.

The burst background traffic cases simulate the same large flat network from the steady-state cases. The specific situation that was chosen for the burst test cases simulates a mobile laptop being attached to the industrial network with an EtherNet/IP configuration tool installed and setup to automatically scan the network. Once the laptop is connected to the network, it will transmit an EtherNet/IP ListIdentity broadcast message over the network. Any device that is EtherNet/IP-capable is required to support the ListIdentity message and will respond to that message. Before each device responds directly to the laptop, it will need to locate the laptop using an Address Resolution Protocol (ARP) broadcast message to locate the laptop's hardware address. This will result in a burst of ARP broadcasts on the network that may interfere with the real-time communications of some devices. Additional devices were added to the burst cases to simulate devices that may not use real-time communications but may have an EtherNet/IP-capable network stack.

Table 1 – Network Traffic Amounts for the PlugFest Performance Test Cases

Test Case	Rate	Baseline	Steady-State Managed	Steady-State Unmanaged	Burst Managed	Burst Unmanaged
ARP Request Broadcasts	180 packets/s	✗	✓	✓	✓	✓
Gratuitous ARP Broadcasts	180 packets/s	✗	✓	✓	✓	✓
DHCP Request Broadcasts	100 packets/s	✗	✓	✓	✓	✓
ICMP (ping) Request Broadcasts	100 packets/s	✗	✓	✓	✓	✓
NTP Multicasts	10 packets/s	✗	✓	✓	✓	✓
EtherNet/IP ListIdentity Requests	10 packets/s	✗	✓	✓	✓	✓
EtherNet/IP Connected Class 1 I/O	1800 packets/s	✗	✗	✓	✗	✓
ARP Request Burst	240 packets @ 4000 packets/s = 60 ms burst	✗	✗	✗	✓	✓

The amount of data collected by the performance test system is limited based on the internal hardware, so the individual tests have to be limited in duration. Depending on the desired packet interval chosen for the test, the duration can be anywhere from 30 to 120 seconds. This allows the test tool to gather enough data to have a statistically significant sample to use during the data analysis.

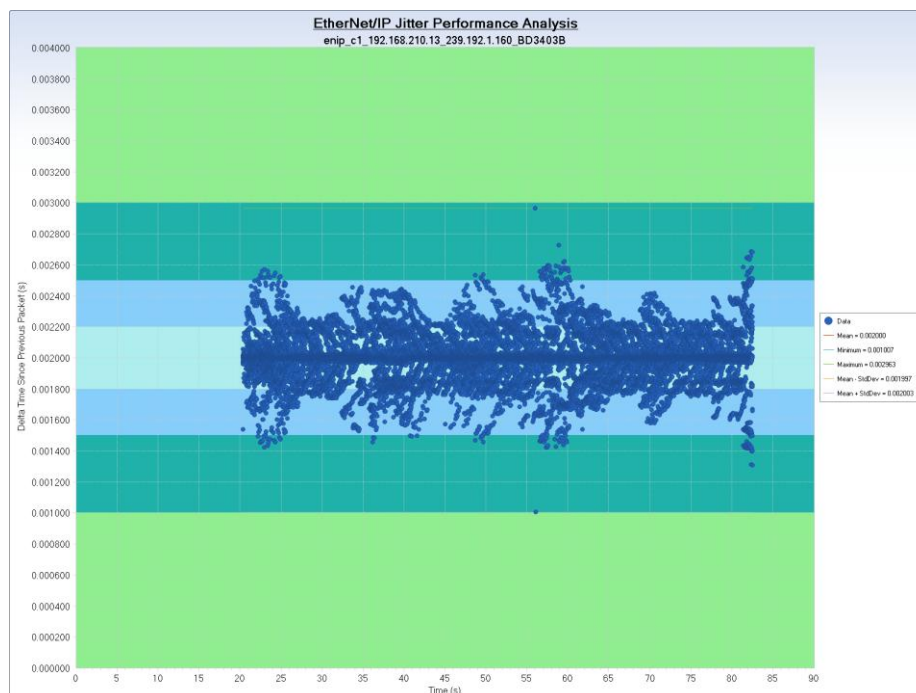


Figure 2 – Example Performance Test Results Data Graph

One result of the data analysis is graphs that show the vendors how their device performed during each of the particular tests. Figure 2 shows a representative graph from a recent PlugFest. The Y-axis of the graph shows the time difference between subsequent real-time network packets, or measured packet interval, and the X-axis shows the time that the particular point occurred during the test. Colored bars are used to represent different percentages of the measured packet interval ($\pm 10\%$, $\pm 25\%$, and $\pm 50\%$ in this particular example). One of the interesting things to note about this graph is the beat pattern to the measured packet intervals. This beat pattern would not cause the device to drop its connection or to lose a single packet, however, it may indicate a performance issue internally that the vendor may need to investigate. There may be an issue with the network stack or some microprocessor overhead that takes longer than expected or there may be nothing wrong at all. Unless the vendor had specifically generated these types of graphs before, they may not have been aware of these types of events or issues other than by the number of service calls they received about a particular device.

Before 2008, the performance testing was completely optional. The data captured during the testing and any reports were presented to the vendors that chose to participate in performance testing. During the two PlugFests held in 2008, performance testing became a required element of the testing for each device attending the PlugFest, however, it was still an informational test. The test data was reported to the vendor and to ODVA, but the results did not affect whether a device passed or failed the overall interoperability testing. Starting in 2009, performance testing will become an integral part of the interoperability testing, required of all devices attending the PlugFest, and will affect their ability to pass or fail the PlugFest.

Interoperability Recommendations

When developing an EtherNet/IP-connected device, there are many questions a vendor needs to consider:

- Is the device a scanner, adapter, or an explicit messaging device?
- What EtherNet/IP functionality should be included in the device?
- How well does the device interoperate with other vendors' devices?
- What real-time network performance should the device have?

All of these questions need to be considered up-front before development begins. Being conformant to only the minimum requirements of the EtherNet/IP specification may not be enough to satisfy a customer's expectations. To assist vendors, the EtherNet/IP Implementors Workshop has provided a series of documents with recommendations

to provide guidance to vendors for the functional specification, implementation, and testing phases of product development.

The EtherNet/IP Implementors Workshop recommendations consist of the following documents:

- *Recommended Functionality for EtherNet/IP Devices* [2]
- *Recommended IP Addressing Methods for EtherNet/IP Devices* [7]
- *IPv4 Address Conflict Detection for EtherNet/IP Devices* [8]

Recommended Functionality for EtherNet/IP Devices is the primary document. Vendors should start with this document. The document describes functionality and performance recommendations based on the EtherNet/IP device classification. The types of recommendations include the number of encapsulation sessions, Common Industrial Protocol (CIP) connections and TCP connections, Ethernet interface, and physical layer recommendations. The document also provides recommendations for adapter devices to allow interoperability with most programmable logic controller (PLC) scanner implementations. Much of this information is not detailed in the EtherNet/IP specification.

Recommended Functionality for EtherNet/IP Devices, version 2.0 has added some important new interoperability recommendations. These new interoperability recommendations are summarized below:

1. All devices **shall** support duplicate IP address detection by implementing the algorithm described in *IPv4 Address Conflict Detection for EtherNet/IP Devices*. This document specifies a common mechanism that EtherNet/IP devices can use to detect and act upon IPv4 address conflicts. Unpredictable and undesirable behavior can result when multiple devices attempt to use the same IP address. The address conflict detection (ACD) mechanism is based on the Internet Draft authored by Stuart Cheshire. In addition to specifying the use of the Cheshire IPv4 ACD mechanism, the document specifies additional requirements for EtherNet/IP devices with respect to the timing of ARP probes, address defense behavior, Identity Object state, and device fault behavior.
2. Scanner and adapter devices **shall** support CIP Transport Class 1 unicast target to originator (T->O) connections. This recommendation will allow users to configure the devices within their EtherNet/IP network to use the most efficient communication message type (producer-consumer vs. point-to-point) based on their application needs. Use of unicast Class 1 connections from the target device to the originator device will reduce multicast traffic within the network and simplify the configuration of the switches.
3. The device **shall** conform to the new input/output (I/O) performance measures.

The EtherNet/IP interoperability testing performed at PlugFests consists of testing products for compliance to the EtherNet/IP Implementors Workshop recommendations. The testing follows a formal test plan *EtherNet/IP Interoperability Test Procedures* [3]. Vendors can download the test plan from the ODVA website to better understand and prepare for PlugFests. Formal testing for the new interoperability recommendations will begin with PlugFest #11, tentatively scheduled for May, 2009. PlugFest #11 will be held at the ODVA headquarters in Ann Arbor, Michigan, USA.

Summary:

The interoperability recommendations are optional but they add value to products. Vendors should download the interoperability recommendations from the ODVA website and reference these documents in their functional specifications. Implementing the recommendations and attending the PlugFests will improve the interoperability of devices and may reduce support and maintenance costs later.

References:

- [1] *General Recommendations for EtherNet/IP Developers*, PUB00100, v2.0, January 28, 2005
- [2] *Recommended Functionality for EtherNet/IP Devices*, PUB00070, v2.0, November 10, 2008
- [3] *EtherNet/IP Interoperability Test Procedures*, PUB00095, v2.0, November 10, 2008
- [4] *Performance Test Terminology for EtherNet/IP Devices*, PUB00080, v1.1, March 14, 2005
- [5] *Performance Test Methodology for EtherNet/IP Devices*, PUB00081, v1.0, March 14, 2005

- [6] *EtherNet/IP Quick Start for Vendors Handbook*, PUB00213
- [7] *Recommended IP Addressing Methods for EtherNet/IP Devices*, PUB00028, v1.0, June 10, 2003
- [8] *IPv4 Address Conflict Detection for EtherNet/IP Devices*, PUB00127, v1.5, June 6, 2006

DeviceNet, DeviceNet Safety, CIP, CIP Motion, CipNet, CipNet SA, CIP Safety and CIP Sync are trademarks of ODVA. EtherNet/IP is a trademark of ControlNet International under license by ODVA. Other trademarks are property of their respective owners.