IPv6 for EtherNet/IP: Is the Sky Falling, or Just an Acorn?

Brian Batke  
Principal Engineer  
Rockwell Automation

Paul Brooks  
Business Development Manager  
Rockwell Automation

Presented at the ODVA  
2011 ODVA Industry Conference & 14th Annual Meeting  
March 1-3, 2011  
Phoenix, Arizona, USA

Abstract:

Despite the predictions over the last 20 years, IPv6 still has not seen widespread adoption. Will this continue? We discuss the factors that will drive IPv6 adoption, the implications for EtherNet/IP, and recommend a course of action for the EtherNet/IP vendor community.

Body:

Another Y2K?

As far back as the mid-1990s we heard warnings that we would “soon” run out of IP addresses. Consequently, we needed to prepare for the imminent coming of IPng, also known as IPv6. The fact that the “ng” in IPng was inspired by the (then current) Star Trek: The Next Generation should remind us how long we have been on the verge of running out of IPv4 addresses.

Thankfully, we learned something from another predicted disaster that failed to materialize: Y2K.

Thus far we have resisted expending the effort to formally define IPv6 support in EtherNet/IP, simply because there has not been a compelling reason to do so. But unlike Y2K, which was a one-time event now largely forgotten, IPv6 will have a lasting presence. There seems to be no dispute that IPv6 will play an important role in the Internet.

The question for industrial automation users and vendors remains: what will be the impact of IPv6, and what should we be doing about it?

Extending the Life of IPv4

Engineers working on Internet protocols, being a pragmatic bunch, have devised solutions to extend the life of IPv4. Primary among these solutions are RFC 1918 and Network Address Translation (NAT). RFC 1918 defines the now-familiar private IPv4 address ranges:
Within an enterprise or home network, it is not necessary for each node to have a public IP address. Organizations can use private IP address ranges then use NAT to present a small number of public IP addresses to the Internet.

![Figure 1. Network Address Translation.]

The widespread use of NAT greatly slowed the consumption of public IPv4 addresses, reducing the urgency to transition to IPv6.

**Drivers of IPv6 Adoption**

As of October 2010, IPv6 accounts for just one twentieth of one percent of Internet traffic\(^1\). Although it may be proceeding slowly, IPv6 is being adopted.

What factors are driving IPv6 adoption, and what will cause it to accelerate?

**Depletion of IPv4 addresses.** The pool of available IPv4 addresses is expected to be depleted sometime in mid-2011. At that time, new IPv4 addresses will cease to be assigned by IANA and the Regional Internet Registries. ISPs will continue to give out IPv4 addresses for some time, but that time is finite (estimated to be an additional 8-12 months).

The depletion of IPv4 addresses does not mean that end nodes must immediately support IPv6. A number of different solutions have been proposed to shield end users from IPv6.

**Government or industry policy.** A number of governments and governmental agencies have policies, incentives, or programs to promote or mandate the support of IPv6. The U.S. and China are most notable with explicit IPv6 adoption programs and policies. At present these programs seem aimed primarily at infrastructure and external (Internet) content. As an example, in September, 2010, the U.S. government announced requirements\(^2\) for all federal agencies to:

- Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012;
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;

At present there are no mandates for automation devices or related software to support IPv6, but this is a possibility at some point in the future.
Network evolution: new applications and devices. Related to the issue of IPv4 address depletion, new applications such as Smart Grid and Internet-connected 4G (and whatever comes next) mobile phones will continue to add hundreds of millions of new devices to the Internet. Servicing these applications will be much easier with an IPv6 infrastructure.

More than Just Bigger IP Addresses
The most significant aspect of IPv6 is of course its bigger address space – 128 bits versus IPv4’s 32 bits. But IPv6 includes additional capabilities that improve upon shortcomings in IPv4.

New address space architecture. The IPv6 address space has been divided into different allocations (unlike the IPv4 notion of address “class”) based on the value of prefix bits in the IPv6 address. Currently only a small portion of the address space has been allocated – for global unicast, link-local unicast, multicast, etc. Multicast addresses are further divided into different scopes. Note that IPv6 does not define a broadcast address. The equivalent of a broadcast is accomplished by sending to the link-local “all nodes” multicast address.

Simplified and extensible header format. The IPv6 header is simpler than IPv4, with unneeded items removed. IPv6 then defines extension headers for specific purposes such as fragmentation. This extensible format allows for new headers to be defined in the future.

ICMPv6. The overall function and packet format of ICMPv6 is essentially the same as in IPv4. An important difference is that ICMPv6 is also used for Multicast Listener Discovery (MLD), and Neighbor Discovery protocols.

Autoconfiguration. IPv6 provides for stateful configuration via DHCPv6, and also for stateless autoconfiguration where a node self-assigns itself a link-local IP address.

Neighbor Discovery. The IPv6 Neighbor Discovery protocol is a sub-protocol of ICMPv6. Neighbor Discovery allows nodes on the same link to discover information about each other, including their link addresses and router information. Neighbor Discovery eliminates the need for ARP, and for a separate address conflict detection mechanism.

Multicast Listener Discovery (MLD). IPv6 uses MLD instead of IGMP for multicast group management. Similar in function to IGMP, MLD is a sub-protocol of ICMPv6 rather than a separate protocol.

Mobile IPv6. Mobility support in IPv6 allows a node to maintain a persistent “home address” as it moves to different network locations.

Security. IPv6 formally requires that nodes support IPsec. Initially defined for IPv6, IPsec has to date mostly been used for IPv4 traffic, e.g., for VPN tunnels, and is optional for IPv4 nodes.

IPv6 Application Scenarios for EtherNet/IP
The majority of discussion on IPv6 deployment scenarios seems to be oriented towards Internet Service Providers and IPv6 clients accessing an IPv4 Internet. Most EtherNet/IP applications reside within an enterprise network. What are the EtherNet/IP application scenarios most likely to require IPv6 support?

RTU applications. One for EtherNet/IP over IPv6 would be an RTU application (e.g., water/wastewater, oil and gas, etc.) where the remote device is connected via a 4G wireless
network. A remote device connected in such a manner would almost certainly require an IPv6 address.

**Smart Grid.** It has been suggested that Smart Grid may be the “killer app” for IPv6. If millions of new Smart Grid devices require Internet connectivity, it seems clear that they will need IPv6 addresses. If EtherNet/IP is to play a role in Smart Grid applications, then IPv6 support is likely required.

**New enterprise network based on IPv6.** While not a likely scenario in the short term for industrial networks, it is not inconceivable that a new enterprise might build its network starting with IPv6. Since Microsoft and major infrastructure vendors now support IPv6, the “IT side” of the network has removed a major obstacle. In such a scenario it would be advantageous if the plant floor network were not an obstacle to IPv6 adoption.

**Making EtherNet/IP Support IPv6**

Simply including an IPv6 stack in an EtherNet/IP device is not sufficient to enable the devices to then communicate via EtherNet/IP. A number of changes to the protocol are required, as well as definition of how certain IPv6 features should be commonly used by EtherNet/IP devices.

The following list shows the anticipated changes to the EtherNet/IP protocol and specification required to support IPv6:

- **ListIdentity response.** The response to the ListIdentity command (used for network browsing) includes the IPv4 address of the responding device. Either a new command or a new response item is needed.

- **Fwd Open Request/Response.** The Fwd Open request and response (used to establish CIP connections between devices) typically includes IPv4 addresses – in particular when multicast connections are being established. New structures are needed to communicate IPv6 addresses in the Fwd Open request/response.

- **TCP/IP Interface Object.** An EtherNet/IP device’s IPv4 address and related items are configured via the TCP/IP Interface Object. At present this object has no support for IPv6 configuration. Either new object attributes are required, or more likely, a new object needs to be defined to support IPv6 configuration and diagnostics.

- **IP Address Conflict Detection.** IPv4 Address Conflict Detection (ACD) is currently defined for EtherNet/IP. For IPv6, ACD is defined as part of the Neighbor Discovery Protocol. In order to support IPv6 the EtherNet/IP specification will need to clarify the usage of the Neighbor Discovery Protocol in the specific context of EtherNet/IP device behavior.

- **IP Multicast Usage.** EtherNet/IP devices use IP multicast when transmitting data on a multicast CIP connection. At present only IPv4 multicast usage is defined, including mechanisms for assigning
IPv4 multicast addresses and device behavior for IGMP usage. In order to support IPv6 the specification must include details on usage of IPv6 multicast addresses and the Multicast Listener Discovery protocol (MLD), which replaces IGMP.

Device Level Ring (DLR) Protocol. Several aspects of DLR would be impacted by IPv6 support:

- 4-byte source IP address field in DLR header
- 4-byte IP address field in Sign-On message payload
- 4-byte IP addresses in DLR Object attributes: Last Node on Port 1, Last Node on Port 2, Ring Supervisor Address, Ring Participants List.

IPv6 Features and Options for EtherNet/IP. In order to provide for device consistency, the EtherNet/IP specification should clarify what aspects of IPv6 – including whether to use a dual IPv4/IPv6 stack – are required, recommended, and optional for EtherNet/IP devices. In addition, further investigation work is needed to assess the impact of required features such as IPsec on resource-limited devices.

Potential Benefits to EtherNet/IP
While incorporating IPv6 support into EtherNet/IP is largely a future-proofing exercise, a number of potential user benefits could result from work to include IPv6 support:

- Simplified Device Commissioning. While some invention would likely be required, adding IPv6 support would be an opportunity to make use of IPv6 Autoconfiguration and Neighbor Discovery features to define common behavior to simplify IP configuration during device commissioning and device replacement scenarios.

- Security. The requirement that IPv6 nodes implement IPsec has the potential to address the security issues of device authentication and message encryption in a proven and standard way. Further work would be needed to determine whether IPsec is an appropriate answer to EtherNet/IP security questions.

- Opportunity for Protocol Improvements. Definition of IPv6 support in EtherNet/IP would create a new class of EtherNet/IP implementation, and would present the opportunity for additional protocol and feature improvements not bound by backward-compatibility concerns.

Making EtherNet/IP Implementations IPv6-ready
While EtherNet/IP has not been made IPv6-ready, a number of common network applications have been ported to use IPv6\(^4\). Mozilla Firefox, Internet Explorer, and many open source implementations of network services (e.g., BIND 9) now support IPv6. These efforts have provided information on the issues that developers face when implementing IPv6 application support.

An EtherNet/IP developer at a minimum would need to consider the following when making an implementation – either software or an embedded device – support IPv6:

- IPv6 network stack. Some operating systems (e.g., Windows 7) already provide built-in IPv6 support. Embedded implementations most likely would need a new or upgraded IP stack, and likely a dual IPv4/IPv6 stack. For some embedded devices, flash memory and/or RAM space could be an issue.
EtherNet/IP stack with IPv6 support. As mentioned above, a number of EtherNet/IP additions are needed in order to support IPv6.

Socket interface and supporting functions. The socket interface (whether BSD, Winsock, etc.) for IPv6 is in general the same as in IPv4 however the socket address structures for IPv6 are different. In addition supporting address conversion functions are different in IPv6.

IPv4 addresses embedded in application protocols. In addition to EtherNet/IP changes, any additional application level protocols that embed IPv4 address need to account for IPv6 addresses.

IPv4 address structures in code. Most code written for IPv4 simply uses 4-byte entities anywhere an IP address is used or stored. All such code must be modified to support the larger IPv6 address.

IPv4 addresses exposed in user interfaces. Many applications expose IPv4 addresses via user interfaces. For example, a scanner configuration tool typically includes an interface to configure a list of target IP addresses. Any such interface would need modification for IPv6.

Exposing IPv6 features. Beyond simply making IPv6 work, certain IPv6-specific features might be exposed for user configuration or diagnostics. For example IPsec might be implemented and exposed as optional capability.

**Recommendations for the EtherNet/IP Community**

IPv6 has often been spoken of as a “disruptive technology”. One could question whether IPv6 has now lost its disruptiveness since it has shown up on such lists year after year. For EtherNet/IP vendors, the disruption will come when customer applications demand the use of IPv6. Although such a demand is not strong at present, it seems prudent for ODVA and EtherNet/IP vendors to at least be prepared.

What should ODVA be doing?

*Add IPv6 support to the EtherNet/IP specification.* Because of the lead time required to add material to the specification, it is desirable for the EtherNet/IP specification to be “IPv6-ready” in the event that vendors need to implement IPv6. Such work would also position ODVA and EtherNet/IP as technology leaders.

*Prototype an IPv6 EtherNet/IP Implementation.* In conjunction with defining the specification work, a prototype implementation of EtherNet/IP over IPv6 would help uncover any unforeseen issues and prove feasibility.

*IPv6 Whitepaper(s).* One or more whitepapers would benefit EtherNet/IP vendors and end users. Topics could include:

- Overall ODVA position on IPv6
- Summary of EtherNet/IP changes to support IPv6
- Practical guidance for vendors in supporting IPv6
- EtherNet/IP applications scenarios for IPv6

What should individual vendors be doing?
**Assess the need for IPv6 support.** Considering the application space that the vendor serves, is IPv6 support likely to be required?

**Assess the likely impact to software and device implementations.** An assessment of impact to existing software and embedded device implementations would give the vendor information on the magnitude of effort required to support IPv6. Where are IPv4 addresses used in code or exposed in user interfaces? Where are IPv4 addresses embedded in application protocols? Does the chosen TCP/IP stack support IPv6, or can it be upgraded to support IPv6? Do embedded devices have enough resources to support additional code for IPv6?

**Develop a high-level plan.** Even if vendors do not need to support IPv6 in the immediate future, developing a high-level plan would allow vendors to better respond when customers ask questions about IPv6 implications, and to respond more quickly in the event that IPv6 support is required.

**Is it Just an Acorn?**

While the sky is clearly not falling, the unsatisfying answer at present is “we don’t know yet”. The topic of IPv6 adoption still raises many questions, yet it seems clear that IPv6 will not fade into a forgotten technology. The current best course of action is for the EtherNet/IP community to at least be prepared should the acorn turn out to be something much bigger.

**References (optional):**


**************************************************

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of CIP Networks and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because CIP Networks may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying CIP Networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use. Copyright ©2011 ODVA, Inc. All rights reserved. For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on: TEL +1 734-975-8840 FAX +1 734-922-0027 EMAIL odva@odva.org WEB [www.odva.org](http://www.odva.org).

CIP, Common Industrial Protocol, CIP Motion, CIP Safety, CIP Sync, CompoNet, CompoNet CONFORMANCE TESTED, ControlNet, ControlNet CONFORMANCE TESTED, DeviceNet, EtherNet/IP, EtherNet/IP CONFORMANCE TESTED are trademarks of ODVA, Inc. DeviceNet CONFORMANCE TESTED is a registered trademark of ODVA, Inc. All other trademarks are property of their respective owners.