PUB00028R1

Recommended IP Addressing Methods for EtherNet/IP™ Devices

Version history

Version	Date	Description
PUB00028R0	2003-06-10	Initial release
PUB00028R1	2026-05-25	First revision Contains the following changes: • General: content added throughout document to describe in-Cabinet. • Removal of section 1.3 “Future Revision of the Recommendation”: content obsolete • Section 1.3 moved from another location. • Section 3 update to better define Standard EtherNet/IP and to correct grammar. • Section 4 added to include In-Cabinet EtherNet/IP information. • Section 5 was removed due to content being obsolete. • Appendix A was removed due to content being obsolete.

Contents

1 Introduction

1.1 Scope of Document

The purpose of this document is to recommend common mechanisms related to IPv4 address assignment and management for EtherNet/IP devices. The recommendations are a result of the work generated by EtherNet/IP Implementors Workshops and the EtherNet/IP Infrastructure SIG.

1.2 Interpreting the Recommendations

The recommendations cannot be interpreted as “requirements” from the perspective of the EtherNet/IP specification. However, from the perspective of the Implementors Workshop, it is useful to be able to state whether or not a device adheres to the IP Addressing Recommendations (and future workshop recommendations).

Therefore, this document uses language similar to the EtherNet/IP specification to make clear what is required and what is optional in order for a device to adhere to the IP Addressing Recommendations.

1.3 EtherNet/IP™ Device Types

The Standard EtherNet/IP devices use the original multi-usage EtherNet/IP standard. The Addressing Methods used in these devices are described in Section 3.

The In-Cabinet EtherNet/IP devices exclusively use of the UDP-Only EtherNet/IP transport profile for the transmission of all CIP messages. The Addressing Methods used in these devices are described in Section 4.

1.4 Description of Problem

Since the initial development of TCP/IP, numerous methods for configuring a device's IP address have evolved. Not all of these methods are suitable for industrial control devices. In the office environment for example, it is common for a PC to obtain its IP address via DHCP, potentially getting a different address each time the PC reboots.
This is acceptable because the PC is typically a client device that only makes requests, so there is no impact if its IP address changes.

However, for an industrial control device that is a target of communication requests, the IP address can't change at each power up. If you're talking to a particular PLC, you want that PLC to be at the same address the next time it powers up.

To further complicate matters, the only interface common to all EtherNet/IP devices is an Ethernet communications port. Some devices may also have a serial port, or a user interface display, or hardware switches, or other interfaces, but these are not universally shared across all devices. Since Ethernet is the common interface, the initial IP address must at least be configurable over Ethernet.

The Standard EtherNet/IP specification, via the TCP/IP Interface Object, defines several ways to configure a device's IP address. A device may obtain its IP address via BOOTP, or via DHCP, or via an explicit Set_Attribute (single or set-all) service. None of these methods are mandatory. As a result, vendors could choose different methods for configuring IP addresses.

When using EtherNet/IP In-Cabinet media (a multidrop Single Pair Ethernet), DHCP and BOOTP are not allowed, and an alternate address management method of TCP/IP Interface Object configuration is specified.

From the user's perspective, it is desirable for vendors to support some common mechanism(s) for IP address configuration.

1.5 Existing EtherNet/IP Configuration Mechanisms

1.5.1 TCP/IP Interface Object

The TCP/IP Interface Object maintains a device's TCP/IP-related configuration information. The TCP/IP Interface Object allows the following configuration items to be set:

- IP Address
- Network Mask
- Gateway Address
- Name Server Address
- Secondary Name Server Address
- Default Domain Name
- Host Name

The Standard EtherNet/IPTM device provides an optional Duplicate IP address detection feature defined as Address Conflict Detection.
The TCP/IP Interface Object provides several options for a device on a standard Ethernet physical link to obtain its initial TCP/IP related configuration:

- from non-volatile memory
- via BOOTP
- via DHCP

These options are settable via the Configuration Control attribute.

The TCP/IP Interface Object obtains its initial TCP/IP related configuration for In-Cabinet Media network segments via the services of an In-Cabinet Commissioning Object and its related objects.

1.5.2 Ethernet Link Object

The Ethernet Link Object maintains configuration and diagnostic counters related to the Ethernet communications port. The Ethernet Link Object allows the following configuration items to be set:

- Whether auto-negotiation (per IEEE 802.3) is enabled.
- Port Speed and duplex mode (if auto-negotiation is not enabled)

1.5.3 Additional Device Configuration

Devices may require additional device-specific configuration in order to be fully functional. The mechanism for obtaining this information is beyond the scope of this recommendation.

1.5.4 Industrial EtherNet/IP In-cabinet Media Addressing Mechanism

An automatic addressing mechanism is specified for the In-cabinet media system. Each media uses the SEL line and related protocol to determine relative node positions. LLDP is used to assign addresses.

2 General Application Requirements

The following list describes the general requirements that apply to the majority of application scenarios and devices.

1. There must be one common mechanism (the TCP/IP Interface Object) for IP address configuration supported by all EtherNet/IP vendors, so the user is not forced to do things differently for each vendor's device. Vendors are not prohibited from providing additional mechanisms (such as Web-Server, SNMP, etc.), but must at least provide the common mechanism

2. IP address assignment must be consistent and predictable.
    a. Once assigned, the device's address must not change.
    b. Device's IP address must survive node reset and/or cycling of power.
    c. Exceptions are Configuration tools and other transitory devices (such as portable HMI).

3. When a device fails, the replacement device must be assigned the same IP address with minimal user intervention.

4. It is desirable to make use of standard Internet Engineering Task Force (IETF) mechanisms wherever possible.

5. A common addressing solution must not require special hardware (e.g., switches or jumpers). Vendors are allowed to provide such solutions, so long as they also implement the one common recommended mechanism.

6. There are a number of different configuration scenarios. A solution to one scenario must not create a problem for a different scenario.

7. Recognize that address assignment and maintenance may also have site- specific IT policies and practices.

3 Application Scenarios and Recommended Mechanisms for Standard EtherNet/IPTM Devices

3.1 Requirements for Standard EtherNet/IPTM Devices

In order to support the scenarios and mechanisms outlined above, the following is required for EtherNet/IP devices:

1. The device shall by default issue BOOTP or DHCP requests at initial power up “out-of-box” (from the vendor). The use of BOOTP or DHCP out-of-box allows a device to be given an IP address by a server on the user’s network, or via an interactive utility (e.g., the free utility provided by Rockwell)

   DHCP is recommended, since it allows for devices to make use of DHCP Option 82 as a device replacement mechanism. DHCP also allows for further enhancements such as DHCP-DNS updating. BOOTP is acceptable since it is recognized that products may need to support BOOTP (e.g., for backwards-compatibility reasons, or because the operating system does not support DHCP client). Note that client devices implementing only BOOTP CANNOT make use of any of the DHCP advanced services such as Option 82.

   Other methods for acquiring an IP address are not precluded. In addition to BOOTP / DHCP, a vendor may choose, for example, to provide a set of switches for configuring an IP address.

2. The device shall allow the user to make a valid IP address persistently stored in non-volatile memory, via attributes and services of the TCP/IP Interface Object.

3. For 100BASE-TX devices, the device shall allow the user to select auto-negotiation or manual setting of duplex mode and port speed, per the Ethernet Link Object.

4. The Ethernet MAC address shall be visible on the device (e.g., on a label).

3.2 Configure Initial IP Address (“Out of Box”)

3.2.1 Application Scenario

As part of system commissioning, a device needs to be given an IP address. Assignment of addresses could be done at the site of deployment or could be done by an OEM or integrator off-site.

3.2.2 Recommended Mechanisms

Out of the box, devices must support issuing either BOOTP or DHCP requests to obtain an initial IP address. It is recognized that some operating systems do not support both BOOTP and DHCP, but generally will support one of the two.

The use of BOOTP/DHCP for initial IP address configuration does not require the user to set up a complicated BOOTP/DHCP server. The simplest and most user-friendly option is

to use an interactive utility that allows the user to enter an IP address to “answer” the device’s BOOTP/DHCP request. Such a utility is freely available from Rockwell Automation.

Alternatively, the user can make use of a commercially available server such as found on Windows and UNIX systems. Fortunately, all of the common DHCP servers (e.g., Windows, Linux, etc.) are able to service BOOTP requests.

The user may elect to have a BOOTP/DHCP-capable server permanently resident on the network. If so, the user should configure the server to give out static IP addresses for EtherNet/IP devices.

Once given an initial IP address, the user may elect to make the address persistent (i.e., saved in non-volatile storage) by setting the Configuration Control attribute of the TCP/IP Interface Object to static. This may be done using the Interactive BOOTP/DHCP Utility or another configuration tool that supports the TCP/IP Interface Object.

3.3 Move System to Production Site

3.3.1 Application Scenario

A system has been configured and staged off-site (or on-site but isolated from the production network). The system then needs to be brought on-line and put into production. Typically, devices will continue to use the IP addresses they were assigned during initial configuration and staging of the system. It is also possible that devices are given new IP addresses to match the user’s network addressing scheme.

3.3.2 Recommended Mechanisms

If BOOTP/DHCP is being used, then the configuration file(s) from the staging system’s BOOTP/DHCP server must be incorporated into the production system’s BOOTP/DHCP server configuration. This will be dependent on site-specific usage of BOOTP/DHCP. If persistent IP addresses stored in devices are being used, then nothing further needs to be done. Devices power up with their stored IP addresses.

3.4 Add New Device to Existing System

3.4.1 Application Scenario

A new device needs to be added to a system that is already operational and has IP addresses assigned. The IP address of the new device needs to be consistent with the existing assigned addresses.

3.4.2 Recommended Mechanisms

Same as “Configure Initial IP Address”.

3.5 Reconfigure IP Address

3.5.1 Application Scenario

IP addresses for one or more devices need to be changed. This could be a result of moving from public to private IP addresses (or vice-versa), changing the organization of subnets, etc.

3.5.2 Recommended Mechanisms

If BOOTP/DHCP is being used, the user must edit the BOOTP/DHCP configuration file to specify a new IP address for the device and then restart the device.

If persistent IP addresses stored in devices are being used, the user connects to the device via a programming or standard EtherNet/IP-based configuration tool and changes the IP address. The underlying mechanism used by the programming/configuration tool is get/set services to the TCP/IP Interface Object.

3.6 Cycle Power to System

3.6.1 Application Scenario

An existing system loses power, and then has power applied again. This could be expected, for example because of planned maintenance, or system restart (“warm start”) during integration, or troubleshooting process, or could be an unexpected power loss. Upon restoring power, devices must obtain the same IP addresses as before. No assumptions should be made on the order in which devices power up. Also, it is highly desirable for devices to continue to operate even if a BOOTP/DHCP server (assuming one is in use) does not power up properly.

3.6.2 Recommended Mechanisms

If BOOTP/DHCP is being used, devices power up and make BOOTP or DHCP requests. Assuming the server has been configured as recommended (see section 3.1, “Configure Initial IP Address), the device will receive the same IP address it received on previous power cycles.

If BOOTP/DHCP is being used and for some reason the server is not present (e.g., server fails to power up), the device may elect to use the IP address it previously received from the server.
If persistent IP addresses stored in devices are being used, then nothing further needs to be done. Devices will power up with their stored IP addresses.

3.7 Move Device to New Location

3.7.1 Application Scenario

A device needs to be moved to a different location and given a new IP address, e.g. swapped with another device. The new location could be on the same subnet, or on an entirely different subnet.

3.7.2 Recommended Mechanisms

Same as “Reconfigure IP Addresses”.

3.8 Replace Failed Device

3.8.1 Application Scenario

A device fails and is replaced with a new or a used device. The replacement device needs to obtain the same IP address as the device it is replacing. Device failure could occur during hours when network support personnel are available, or during “off” hours when network support is unavailable.

3.8.2 Previously Used Device

If the used device does not have its previous configuration stored in the non-volatile memory, then it should be treated as a new device.
If, despite the recommendation presented in the “Move Device to Stock” scenario, the used device has its previous configuration stored in the non-volatile memory, then it must be reconfigured as described in the “Reconfigure IP Address” scenario. If the used device has its previous configuration stored in the non-volatile memory and it is an unknown address, then it has to be reconfigured in accordance with the procedure described in the “Recover Device with Unknown or Unusable Address” scenario prior to be being used as a replacement of the failed device.

3.8.3 Optional Mechanisms

3.8.3.1 With User Intervention

The replacement device, upon power up, issues BOOTP or DHCP requests. If BOOTP/DHCP is the user’s standard mechanism for address configuration, the user must edit the BOOTP/DHCP server’s configuration file to specify the Ethernet hardware address of the replacement device. This means the (potentially unskilled) user must have access to the BOOTP/DHCP server configuration and have knowledge in how to change the configuration. Alternatively, the user can assign an IP address using the Interactive BOOTP/DHCP Utility and then have network support personnel change the production BOOTP/DHCP server configuration.

If persistent IP addresses stored in devices are being used, the user can specify the IP address using a simple Interactive BOOTP/DHCP Utility and then make the address permanent.

3.8.3.2 DHCP Option 82

DHCP Option 82 (Relay Agent Information) can be used to enable the DHCP server to assign a specific IP address to a specific physical switch port. This mechanism requires Option 82 support in both the switch and the DHCP server.

This mechanism works as follows. When a device fails, the user plugs the replacement device into the same switch port as the failed device. The replacement device issues DHCP requests. The switch (if Option 82 enabled) inserts the Option 82 information into

the DHCP request, indicating the switch port that is making the DHCP request. The DHCP server replies with the IP address that corresponds to the requesting switch port.

The use of DHCP Option 82 in such a manner requires the following:

- The requesting device must use DHCP and not BOOTP.
- The switch to which the end device is connected must support Option 82
- The DHCP server must support Option 82

Note that the details of how to configure the Option 82-capable switch and DHCP server are product and vendor specific. The user must consult the appropriate documentation for the switch and DHCP server.

NOTE: This mechanism has the potential for dangerous unintended consequences if the user swaps Ethernet cables between devices without also swapping the cables at the switch ports (or vice-versa). The use of this mechanism would require that all cables be clearly labeled at both the switch port and the device port.

3.9 Move Device Back to Stock

3.9.1 Application Scenario

A device that has been in use needs to be returned back to stock (e.g., returned to a pool of spare modules).

3.9.2 Recommended Mechanisms

If persistent IP addresses are being used, the user should return the device to the recommended out-of-box configuration (i.e., issue BOOTP or DHCP at startup). The device can be returned to out-of-box configuration, via the Interactive BOOTP/DHCP utility or other EtherNet/IP-based configuration tool.

3.10 Recover Device with Unknown or Unusable Address

3.10.1 Application Scenario

A device has been configured with a persistent IP address, stored in non-volatile memory. The IP address is no longer known, or the user has mistakenly entered a “bad” IP address (not reachable from the user’s network). The user needs to give the device a known and usable IP address (otherwise the device becomes “a brick”).

3.10.2 Recommended Mechanisms

The unknown address problem can be avoided completely if BOOTP/DHCP is used. The user can simply restart the device and give it a known address via a BOOTP/DHCP server (including the interactive utility).

Device vendors may wish to provide a physical mechanism for resetting configuration to factory defaults. If so, the user may employ the physical mechanism to recover the device.

If the device has no physical mechanism for resetting the configuration, and a persistent IP address is stored in the device's non-volatile memory, the burden is on the user to determine the device's configured IP address, connect to the device with an EtherNet/IP-based configuration tool, and change the device configuration.

An Ethernet "sniffer" can be used to capture and determine the IP address being used by the device in question. Several sniffer packages are freely available (refer to section 7, "References"). The user would typically employ the following procedure:

1. Set up an Ethernet sniffer to capture packets. A "packet filter" may be configured so that the sniffer only captures packets from the MAC address of the device of interest.

2. Stop the sniffer and examine the captured packets. Find the sender IP address in the captured packets. If no packets were captured, then continue.

3. Cycle power to the device with the unknown address. Wait for the device to power up and begin its network operations. Many devices will issue a "gratuitous ARP" request upon network initialization. Capturing a gratuitous ARP request with the sniffer will allow the user to determine the device's IP address. Alternatively, the user can broadcast an EtherNet/IP ListIdentity command (e.g., with a software configuration tool). Using the sniffer, the user can capture the device's response to the ListIdentity command.

4. Once the IP address has been determined, connect to the device with the Interactive BOOTP/DHCP Utility or other EtherNet/IP-based configuration tool of choice. The user can then give the device a new IP address, or enable BOOTP or DHCP and cycle power to the device.

5. Note that if the device's IP address is such that it is not reachable from the user's PC (e.g., it has been erroneously configured to be on an unreachable subnet) the user must change his PC's IP address and subnet mask such that it is on the same subnet as the target device.

3.11 Variations on Application Scenarios

There are many variations on the application scenarios listed above, arising from different network architectures and site-specific policies and procedures:

- Network topology. Is there one flat network, or is the network segmented into subnets (separated by routers)
- Network management responsibility. Is the production network managed by dedicated LAN/IT staff? When IP addresses are needed for new devices, how are they allocated, and by whom? How are new subnets added to the network?
- Isolated vs. integrated network. Is the production network connected to the corporate IT network?
- TCP/IP expertise. Does the user have experience in setting up an Ethernet and TCP/IP network, or is this something new? What about the users who might have to make configuration changes or replace modules?

- Use of BOOTP or DHCP. Is the user willing to have a BOOTP or DHCP server active on the network? Or must addresses be assigned and stored in device non-volatile storage?

It is not the intent of this document to examine each of these in detail and propose any recommendations for each one. End users must apply the recommendations presented in this document to their application and network architecture.

4 Application Scenarios and Recommended Mechanisms for In-Cabinet EtherNet/IPTM devices

4.1 Requirements for In-Cabinet EtherNet/IP Devices

In order to support the scenarios and mechanisms described in this section, the following is required for EtherNet/IP devices on multidrop links:

1. The end device shall implement the In-Cabinet EtherNet/IP Usage Profile.

2. On power up the device responds by use of LLDP to a signal periodically relayed from node-to-node on the physical layer cable “Select Line” – indicating its presence and its relative location on the bus.

3. The LLDP messages are received and processed by an Actual Topology Object and a Commissioning Object that are situated within a Gateway, Tool, PLC, or other node that can communicate with the network segment. The end device then receives updated LLDP messages that include its TCP/IP Object Interface Configuration.

   The Select Line protocol determination of Actual Topology along with the Commissioning Object act in a similar manner to DHCP Option 82 to assure the same TCP/IP Object Interface Configuration (including IP Addressing) is applied when a device is replaced.

4. The device shall store the Interface Configuration in non-volatile memory.

4.2 Configure Initial IP Address (“Out of Box”)

4.2.1 Application Scenario

As part of system commissioning, a device needs to be given an IP address. Assignment of addresses could be done at the site of deployment or could be done by an OEM or integrator off-site.

4.2.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

Out of box, devices must support the In-Cabinet EtherNet/IP Usage Profile to obtain an initial TCP/IP Object Interface Configuration.

A Gateway, Commissioning Tool, PLC, or other node that can communicate with the network segment must be present.

The Interface Configuration is stored in non-volatile memory on the device.

4.3 Move System to Production Site

4.3.1 Application Scenario

A system has been configured and staged off-site (or on-site but isolated from the production network). The system then needs to be brought on-line and put into production. Typically, devices will continue to use the IP addresses they were assigned during initial configuration and staging of the system. It is also possible that devices are given new IP addresses to match the user's network addressing scheme.

4.3.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

The Commissioning Object configuration should be moved to the production site. This configuration may move by virtue of being stored in a Gateway, Commissioning Tool, PLC, or other entity that is part of the control hardware.

4.4 Add New Device to Existing System

4.4.1 Application Scenario

A new device needs to be added to a system that is already operational and has IP addresses assigned. The IP address of the new device needs to be consistent with the existing assigned addresses.

4.4.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

A new device may be added at the end of the multidrop cable or interposed in the middle. End addition extends the relative positions along the bus, and a new address can be assigned in sequence. Mid-bus addition changes the relative positions along the bus. The Commissioning Object has a mechanism to maintain the original addressing information for devices that have their relative positions altered by the addition.

4.5 Reconfigure IP Address

4.5.1 Application Scenario

IP addresses for one or more devices need to be changed. This could be a result of moving from public to private IP addresses (or vice-versa), changing the organization of subnets, etc.

4.5.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

The addressing information assigned to a relative position can be altered by updating the Commissioning Object attributes.

4.6 Cycle Power to System

4.6.1 Application Scenario

An existing system loses power, and then has power applied again. This could be expected, for example because of planned maintenance, or system restart (“warm start”) during integration, or troubleshooting process, or could be an unexpected power loss. Upon restoring power, devices must obtain the same IP addresses as before. No assumptions should be made on the order in which devices power up. Also, it is highly desirable for devices to continue to operate even if a BOOTP/DHCP server or In-cabinet Commissioning Object (assuming one is in use) does not power up properly.

4.6.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

The addressing information is persistent in the devices.

4.7 Move Device to New Location

4.7.1 Application Scenario

A device needs to be moved to a different location and given a new IP address, e.g. swapped with another device. The new location could be on the same subnet, or on an entirely different subnet.

4.7.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

New addressing information is assigned, based on the relative position of the device in the new network segment, into a new Commissioning Object. Actual Topology discovery determines the addressing information does not match, and the Commissioning Object changes the addressing information.

4.8 Replace Failed Device

4.8.1 Application Scenario

A device fails and is replaced with a new or a used device. The replacement device needs to obtain the same IP address as the device it is replacing. Device failure could occur during hours when network support personnel are available, or during “off” hours when network support is unavailable.

4.8.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

New addressing information is assigned to a new out of box device or to a previously used device. The addressing information is based on the relative position of the device in the network segment as recorded in the Commissioning Object. Actual Topology discovery determines the presence of the replacement device. The Commissioning Object determines that the right device is being used as a replacement.

4.9 Move Device Back to Stock

4.9.1 Application Scenario

A device that has been in use needs to be returned back to stock (e.g., returned to a pool of spare modules).

4.9.2 Recommended EtherNet/IP In-Cabinet Bus Mechanisms

Since the device will always receive proper addressing in a new network segment, there is no need to clear its addressing information.

5 Implications for Standard EtherNet/IP Users

The vendor requirements above have the following implications for the EtherNet/IP user:

1. Users will generally have to select one of the two primary mechanisms for configuration – either BOOTP/DHCP, or configure devices with persistent IP addresses. Vendors may at their choosing provide other mechanisms, for example, a set of switches. Users of course may elect to use those mechanisms.

2. If BOOTP/DHCP is being used, a BOOTP/DHCP server must be resident on the network. The server should be capable of servicing both BOOTP and DHCP requests since it is possible for devices to issue either BOOTP or DHCP requests. The user should configure the server to give out static IP addresses for EtherNet/IP devices. Infinite lease times should be used, so devices don't have to renew their DHCP leases (and possibly have their addresses change). The actual details of the configuration mechanism will vary depending on the DHCP server and options configured.

3. For device replacement, if DHCP Option 82 is not used, whoever replaces a failed device must either have access to the BOOTP/DHCP server configuration, or have working knowledge of a configuration utility such as the Interactive BOOTP/DHCP utility if permanently configured addresses are being used.

4. The details of deployment of BOOTP/DHCP servers on the user's network depend on site-specific policies, procedures, network design and topology as well as the actual BOOTP/DHCP server in use. It is beyond the scope of this document to discuss BOOTP/DHCP implementation in detail. There are many good resources on the web and in print regarding BOOTP/DHCP administration.

6 References

6.1 DHCP and BOOTP:

RFC951 Bootstrap Protocol
RFC1534 Interoperation between BOOTP and DHCP
RFC2131 Dynamic Host Configuration Protocol
RFC2132 DHCP Options and BOOTP Vendor Extensions
RFC3046 DHCP Relay Agent Option (Option 82)

RFCs may be found at:
www.ietf.org