Paper No. T4-2.8, pp. 1-4

15th INTERNATIONAL SYMPOSIUM on POWER ELECTRONICS - Ee 2009
XV Međunarodni simpozijum Energetska elektronika – Ee 2009
NOVI SAD, REPUBLIC OF SERBIA, October 28th - 30th, 2009

CONTROL OF INDUSTRIAL SYSTEMS BASED ON IP ADDRESSING

Aleksandar Radonjić
Faculty of Technical Sciences, Novi Sad, Serbia
sasa_radonjic@yahoo.com

Abstract: *Centralized control of industrial systems represented a great problem for a long time, because the communication between industrial devices was based on outdated field-bus protocols. In the end of the 1990s, when industrial ethernet was implemented, this situation has been dramatically changed. As a result of new technologies, control of working state of the device through IP address, which is assigned to every device connected to the network, was enabled. However, considering that IP address assignment is still not standardized, this work will show possibilities of DHCP Option 82 and Auto-IP methods, i.e. methods which are mostly used in practice. While the first one of them represents a modification of classical DHCP, which is used in local area networks, the other method is based on different and much more flexible principle. Thanks to that, it accomplishes a set of advantages such as Plug & Play principle, localization of network traffic, the possibility of integration with SCADA software, etc.*

Key words: ***Industrial ethernet, IP address assignment, DHCP Option 82, Auto-IP.***

1. INTRODUCTION

Thanks to great achievements in the field of electronics and computing, at the begining of the 70s of the last century marked a certain kind of revolution in industrial system work. In addition to direct control over the production process the appearance of intelligent devices such as programmable logical controllers (PLC) has led to the generation of large quantities of information, which needed to be collected and subsequently processed by the use of communication infrastructure [1]. Up to the end of 90s, the trend of connecting industrial system's components into networks, was being based on developing different communication protocols which prevented the introduction of unique standard. On the other hand, communication over internet and ethernet networks was widely spread and standardized that indirectly initiated the introduction of these technologies into industrial systems. However, before it happened, ethernet had to undergo some major changes – stochastic approach to medium has been eliminated [2], standard IEEE 1558 [3] that allows synchronization among devices has been defined, etc . (Fig.1.).

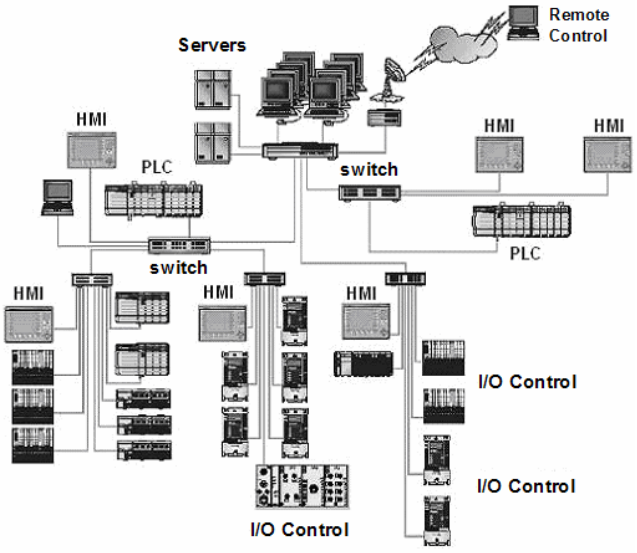

Fig. 1. *Network based on industrial ethernet*

Apart from adapting to real-time communication demands [4], [5] the introduction of ethernet into industrial systems also meant the use of great number of services based on TCP/IP protocol and among them also IP addressing. As it is known, for identification purpose, in computer networks every device (PC station, router, switch, etc.) is given an IP address, temporarily assigned from local DHCP server [6]. It is also known that this procedure always initiates the device in the moment of its connection to the network in the way that through DHCP protocol (DHCP - Dynamic Host Configuration Protocol) requesting information from local DHCP server about network configuration, including IP address. In most cases the exchange of messages between the device and DHCP server will take place without the mediator, because within every subnetwork there is almost always at least one DHCP server. However, if that is not the case, the request for IP address will be taken over by an appropriate DHCP agent (switch) that knows the exact location of DHCP server based on which the received request is being forwarded.

In contrast to this approach, which enables that with every subsequent connection to the network the same computer is assigned a new IP address, in case of

industrial environment devices must be assigned a fixed IP address. This approach appeared from the need that in every moment it is possible to have a simple insight into working condition of every device, regardless of its location. Additionally, this approach enables fast search in case of certain device's failure, whereby the time necessary for system recovery is reduced to the minimum and with it also the loss of productivity.

In order to find the solution that will fulfill all of these requests, in the last couple of years several steps in that direction have been made (the use of configuration tools for local application, the use of ARP/RARP protocols, Port-specific DHCP, etc.), but none of them has been proved completely successful in terms of performances as well as profitability. Considering that segment of IP addressing still has not been officially standardized, research that would provide the most acceptable solution for this sort of problem still continues. When it comes to topical methods, in industrial systems we find the use of DHCP Option 82 and Auto-IP method.

2. DHCP OPTION 82 METHOD

In contrast to standard LAN networks, in which client computer in most cases gets to DHCP server without the use of DHCP agent, industrial systems have hierarchical organization where DHCP servers are set in for that purpose designed places. To simplify the process of getting the IP address in that kind of surrounding, DHCP Option 82 method [7], [8] is often applied in practice, whose work is based on communication between three standard components:

1) *DHCP client* (HMI, PLC, U/I device, etc.)

2) *DHCP agent with Option 82 support* (switch)

3) *DHCP server with Option 82 support*

As it can be seen, the difference between this method and standard DHCP is related to Option 82 support that has to be implemented in every DHCP agent and DHCP server. In other words, besides standard fields that are found in DHCP packet, at DHCP Option 82 method we also meet three additional fields (Circuit ID, Remote ID and GiAddr) which allow DHCP server to identify the location of DHCP agent in a unique way and the port number from which it received the request for IP address.

To clarify the working principle of this method, let us assume that in the network shown in Fig. 2. PLC_1 represents predstavlja DHCP client, and a $switch_1$ an appropriate DHCP agent. In that case, immediately after connection to the network PLC1 will initiate process of getting the IP address that involves the exchange of the following DHCP messages:

1) *DHCP_Discover* – broadcast message sent by PLC_1, which is received by every adapters on subnetwork

2) *DHCP_Discover_Option_82* – unicast message which is sent by $switch_1$ towards DHCP server

3) *DHCP_Reply_Option_82* – unicast response from DHCP server towards $switch_1$

4) *DHCP_Reply* – unicast message sent by $switch_1$ towards PLC_1

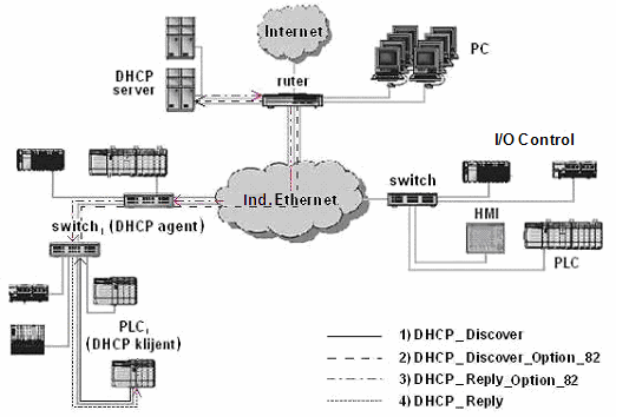

Fig. 2. *IP addressing based on DHCP Option 82 method*

When it comes to this method, it is important to emphasise that the exchange of DHCP messages is preceded by configuration of an appropriate switch as DHCP agent. It is done either remotely or automatically, in such a way that a chosen switch addresses to an adequate file server asking for information about DHCP server location as well as ports at which it will receive incoming requests.

3. AUTO-IP METHOD

While DHCP Option 82 method uses DHCP messages in process of assigning IP address, Auto-IP method is based on combined use of two application level protocols - BOOTP and SNMP protocol [6]. Considering this fact, at the beginning it can be probably thought that with the use of two protocols the situation will become more complicated compared to previous method, especially considering the number of messages that network devices exchange. However, observing from the angle of functionality, combined use of two protocols enables number of other advantages [9] which are not seen at first sight, for example:

a) BOOTP protocol, because of its earlier wide use is supported by almost every industrial device (unlike the DHCP which is supported only by the most recent ones)

b) the elimination of DHCP server enables localization of network traffic (transfer of information no longer goes “from bottom to the top“ and vice versa)

c) there is a possibility of introducing an efficient redundancy within the network using more servers with identical data bases

d) full coexistence with SCADA software with the possibility of integration within the same computer

e) the need for additional configuring of switches as it is in DHCP Option 82 method is unnecessary (all switches support SMNP protocol)

f) simplicity of implementation through "Plug & Play" principle, etc.

In order to realize all these possibilities, every network which has implemented Auto-IP method must have three characteristic components:

1) *BOOTP client* (HMI, PLC, U/I device, etc.)

2) *SNMP agent* (switch)
3) *Auto-IP server (modified BOOTP server)*

At the moment when BOOTP client is connected to the network it will a initiate process of getting the IP address which in most cases implies communication with local Auto-IP server. However, to present additional possibilities, which this method gives in Fig. 3. the redundancy implementation case is shown, which implies communication not only with local, but also with remote Auto-IP server. Therefore, if we suppose that PLC1, which contains two network cards, represents BOOTP client, the procedure of assigning IP address will imply sending the following configuration messages:

1) *BOOTP_Request* – broadcast message sent by PLC1 which through switch1 is being forwarded to Auto-IP server 1, i.e. through switch2 to Auto-IP server 2.

2) *SNMP_Query* – message which is sent by appropriate Auto-IP server to adequate switch

3) *SNMP_Response* – response of every switch individually sent to Auto-IP servers

4) *BOOTP_Response* – response of Auto-IP server which contains IP address intended for PLC_1

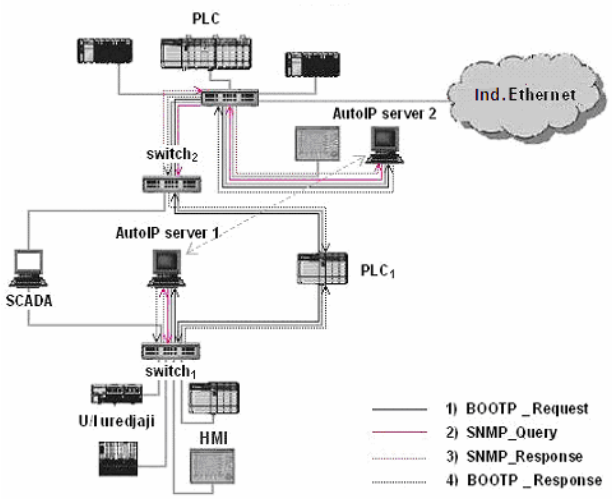

Fig. 3. *IP addressing based on Auto-IP method*

With this way of industrial device addressing i.e. use of more Auto-IP servers, besides introducing redundancy, network traffic is significantly localized. Observing from the angle of implementation, it implies configuration with one primary and one or more secondary Auto-IP servers. Apart from the difference in physical location, primary server, which is put in the central part of the network, gets also the function of refreshing data base on every secondary server (thick discontinuous line in Fig. 3). This provides the solution where every BOOTP request will reach addresses on both Auto-IP servers, but as a valid response will be accepted only the one that gets to the adapter of that particular device first.

4. COMPARISON OF DHCP 82 METHOD WITH AUTO-IP METHOD

As it was said at the beginning, DCHP Option 82 and Auto-IP represent two equal and sole topical methods today. Considering that none of them has been yet standardized, it would be interesting to compare them and see the advantages and disadvantages that the implementation of every one of them brings with it. If we consider the main principles based on which both methods are functioning and if we assume that one network based on industrial ethernet implies the configuration and adequate interventions in cases of incorrect work, their comparisons can be made on following issues:

a) Complexity of device configuration

a1) DHCP Option 82 method implies the use of modern switches and the DHCP server with Option 82 support. This implies additional configuration of switches, as well as data input into data base on the DHCP server for every device individually.

a2) Auto-IP method uses standard switches without any need for additional configuration. Still, because insufficient information which is contained within such an approach (absence of information on the port from which a BOOTP request arrived), in this case there is an exchange of additional messages.

b) Detecting of device failure

b1) DHCP Option 82 method uses a complex software for monitoring ports on switches which imply preventing the possibility to assign wrong IP addresses to devices in cases of failure or appearance of reset function.

b2) Auto-IP method utilizes standard messages on availability of certain devices (ICMP packet is sent on every 30 seconds) for malfunction detection, while in cases of reset, rebooting of operating system is followed by sending the BOOTP request with the MAC address of the corresponding device. Because of information that Auto-IP servers already contain in their data bases, every possibility that those devices get a wrong IP address is prevented.

c) The existence of redundancy

c1) The introduction of redundancy within the network that utilizes DHCP Option 82 method is hardly feasible, because for IP address distribution it is necessary to use at least one more server. Therefore, the solutions which are used at standard LAN networks are also being used here.

c2) Auto-IP method implies the possibility of introducing redundancy principle which contains primary and secondary Auto-IP servers with identical data bases.

d) Connection to hub

d1) Because of the need that every connected device is assigned with an adequate port, the use of less intelligent network devices such as hub, using the method DHCP the Option 82 is not enabled.

d2) Thanks to the use of the SNMP protocol, which is supported by every network device, the Auto-IP method implies the use of classic hubs and switches, etc.

By observing all those situations that can happen in practice, it can be easily concluded that the Auto-IP method represents a better solution in relation to at this time more represented DHCP Option 82 method.

To support that there is Table 1, and also very efficient software implementation done by Network Vision, Inc. [10].

Table 1. *DHCP Option 82 i Auto-IP method capabilities*

Perfomance and capabilities	**DHCP Option 82**	**Auto-IP**
Detection of device failure	Not easily	Yes
Support for BOOTP enabled devices	No	Yes
Redundancy support of the IP address server	Not easily	Yes
Work with all existing networking equipment	No	Yes
Requiring of configuration at each switch	Yes	No
Support for devices connected to hub	No	Yes

5. CONCLUSION

Considering the problem of IP addressing of industrial devices, it can be easily noticed that the basis of such idea lies in methods which are also used today in up to date LAN networks. This is primarily related to the use of DHCP protocol, which has with the appearance of mobile computing completely suppressed BOOTP protocol, as **its** direct predecessor. However, unlike today's computer networks, in which the assignment of IP addresses is being made by dynamical principle, i.e. on certain period of time, industrial devices have been given exclusively fixed IP addresses. Such circumstances prompted the development of the idea to reuse BOOTP protocol at IP addressing, so that contemporary networks based on industrial ethernet use DHCP Option 82 method, based on modification of standard DHCP and Auto-IP method which is further based on combined use of BOOTP and SNMP protocol.

Taking into account that these methods are different in their way of functioning, they are characterized by certain advantages and disadvantages as well: DHCP Option 82 method requires the use of modern switches that can enable the exchange of DHCP messages on relation between industrial devices, while Auto-IP method allows the use of less intelligent devices, but because of insufficient information which it provides the additional use of SNMP protocol is required. When the rest of the characteristics are added to all that was previously said, such as: the easy way of implementing, introduction of redundancy through parallel work with other types of servers, timely diagnostic of network etc. then it can be concluded that Auto-IP method is, after all, practically and at this moment economically the most acceptable solution.

6. REFERENCES

[1] A. Radonjić, *Kontrola savremenih mernih sistema zasnovana na IP adresiranju,* Seminar work on Intelligent measurement, Ph.D. studies, Faculty of Techical Sciences, Novi Sad, June 2009. (In Serbian)

[2] *Information Technology - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications,* IEEE 802.3-2000, 2000.

[3] *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, IEEE 1588, 2002.

[4] J. Jasperneite, P. Neumann, *Switched Ethernet for Factory Communication,* IEEE Conf. on Emerging Technologies and Factory Automation (ETFA´01), pp. 205-212, 2001.

[5] M. Felser, "*Real-time Ethernet – Industry Perspective,* Proc. IEEE (Special Issue on Industrial Communication Systems), vol. 93, no. 6, pp. 1118-1129, Jun. 2005.

[6] D. Comer, *Internetworking with TCP/IP, Vol. I: Principles, Protocols and Architecture*, Prentice Hall, Inc., 2000.

[7] J. D. Wendorf, *EtherNet/IP Addressing Issues and Recommendations,* ODVA Global Networks, Conf. & 8th Annual General Meeting, 2002.

[8] *Recommended Functionality for Switches running Relay Agent and Option 82*, ODVA Inc., Ethernet/IP Implementer Workshops, 2004.

[9] A. Swales: *IP Address Assignment in Large Industrial Networks*, Network Vision Inc., 2003.

[10] Network Vision Inc., *IntraVUE Enterprise and IntraVUE Lite*, http://intravue.net/, 2008.