Remote interaction with devices through hardware and software extended Wake On LAN server to ensure their access and work

Gencho Stoitsov, Zhelyan Guglev

Abstract— The article describes hardware changes and software innovations applied to an original cheap and economical server platform, that is IEEE 802.3 compatible with HARVARD architecture and based on 8 bit microcontroller PIC18F67K22. Two controllable ports with relays have been added to the platform, designed specifically to remotely reboot or turn on hardware devices and to perform remote power control of photovoltaic plants by acting on their ControlBox specialized devices.

Index Terms— ENC28J60, Local Area Network, Microprocessor, SNMP, OSI model, PIC18F67K22, Wake on LAN, WOL packets.

1 Introduction

THE technology Wake On Local Area Network or else WOL provides a standard way of remotely switching or bringing out of standby mode IEEE 802.3 compatible devices [1].

To identify the device that you will interact with, its Media Access Control (MAC) address is used and the transporter of the generated request in most cases can be Ethernet or the User Datagram Protocol (UDP) [1]. When using the UDP, a common practice is the indication of the broadcast address of the recipient. One of the reasons is that the devices receive their IP address after they are switched on. This inefficient approach was used in previous versions of the developed platform and in combination with a complex network topology and often send WOL packets addressed to a large number of devices, excessive traffic is generated which in the absence of filtration reaches all network nodes including those that do not have devices objective to Wake on LAN packets.

Although Wake On LAN technology has existed for a long time now, a significant number of Ethernet 802.3 compatible devices do not support it.

Manufacturers of WOL compatible devices have different implementation approaches on how to respond to a WOL packet, obtained after being earlier suddenly turned off and then restored to power.

2 General functional characteristics of the developed platform ections

By using the latest version of Microchip TCP/IP Stack, supporting 8-bit PIC microcontrollers, an easily integrating miniature server platform was created via DHCP and NetBIOS. ICMP and SNMP allow for remote diagnostics and control of the device. Its main purpose is to provide functionality for manual or automatic generation of WOL packets. As part of the automatization, the platform can store its own list of target devices for the generated Wake On LAN packets. As a physically possible replacement for Wake On LAN protocol, 2 controllable hardware, galvanically separated ports with a common purpose are provided. They have the ability to remember their last state and to restore it after system reboot. Administering the platform happens through a web-based user interface using the HTTP1.1 protocol.

3 Peculiarities in the use of DHCP client for integration in the local network

The presence of Dynamic Host Configuration Protocol greatly facilitates the integration of new devices on the LAN [13]. For this purpose, DHCP compatible devices have their own DHCP clients that request for new IP addresses or renew the ones they have already received.

The request, sent by the client, contains parameters such as: code of the type operating hardware, length of the hardware address, number of references (hops), a unique identifier of executed transactions to identifying all requested by the client parameters, leasing time for reserving the IP address, IP addresses of the client and server, as well as a number of other voluntary options [12], [13].

In the process of testing the DHCP client of TCP/IP Stack of Microchip it has been found that the lack of the voluntary DHCP option, registering the host name of the client in the DHCP server often hampers and slows down the process of acquiring the IP address. Often a device with an assigned IP address does not appear in the list of registered devices on the server. Such effects were observed when using a DHCP server implementations in devices running software on TP-LINK and DD-WRT.

After adding the missing option in the code of the DHCP client, the above problems disappeared, and the registration process is accelerated.

- *Corresponding author: Dr. Gencho Stoitsov is currently Assistant professor in Plovdiv University "Paisii Hilendarski", 236 Bulgaria Blvd., 4003 Plovdiv, Bulgaria, (Email: stoitzov@uni-plovdiv.bg)*
- *Zhelyan Guglev. is currently pursuing doctoral degree program in Plovdiv University "Paisii Hilendarski", 236 Bulgaria Blvd., 4003 Plovdiv, Bulgaria, (Email: jelian_g@mail.bg*

4 Integration and Extension of a NetBIOS Server Module

Supporting NetBIOS in the current implementation of the platform greatly facilitates discovering and turning to a given device on the local network. Using datagram protocol mode, the device can respond to requests containing its NetBIOS name. This allows customers to turn to it not only by IP address but by name, without needing the presence of a DNS server [9].

In the process of experimentation it was found that the NetBIOS server provided by TCP/IP Stack of Microchip does not have the ability to respond to requests of type NBSTAT (0x0021), which are used for diagnostic purposes and through which the NetBIOS name can be extracted from a specific IP address.

The implementation of a NetBIOS support in NBSTAT made it possible to address by NetBIOS name and to announce the NetBIOS name of the device. The mere requirements of the protocol regarding the name length limit it to 16 characters. In Microsoft implementations, the sixteenth character is reserved to identify the type of services provided by the given device, but the current work does not comply with this Convention [8], [9], [10].

The current implemented procedure when registering a NetBIOS name from a country, the platform includes a constant string of 6 symbols, followed by the last four hexadecimal digits of the MAC address of the network interface, which makes a total of 10 characters. The remaining unused positions are filled with spaces. The chosen approach ensures easy recognition of identical devices and practical uniqueness of their NetBIOS names within the local network. Changing the MAC address of the device allows tackling problems caused by the collision of NetBIOS names.

5 Avoiding the Inconveniences Connected with the Use of Wake On LAN Protocol

In the latest version of the UDP based WOL packet generator of the platform, the user is given the opportunity when sending a WOL package to specify not only the MAC address but any IP address. This extends the control that can be applied to recipients of the package by:

1. Broadcast address - all hosts on the local network are recipients.
2. Multicast address - hosts of the subnet of the local network are recipients.
3. A specific IP address:
    a. Possibility to limit, at the physical port level in intelligent routers and switches.
    b. Possibility to send authentic WOL over Internet packets with a destination outside the local network.

For the convenience of the user, the platform allows the storage of a list of up to 42 hosts, for which it can be manually triggered sending a WOL package or they to be marked as part of the process of automatically sending packages to them every five minutes. The last option is a convenient alternative to keeping them constantly on, and to prevent them from falling in a standby mode for a long time.

In cases where software interaction via Wake On LAN technology is not possible, but the device and the platform are physically close, turning it on, rebooting it etc. can be done in a hardware manner. For this purpose, the platform has 2 controllable ports, filled with relays that can control the DC voltage to 24 volts 0.7 amps. The change of the status of the relays is stored, so that it can be restored after restarting the platform.

For the convenience of the user, in the Web interface is supported the so-called "Toggle x 2" action for a particular relay, which is a double inversion of the relay state with a guaranteed time interval between the separate inversions of at least 500 milliseconds. The result of the performed operations is designed to simulate a pressed/released physically button, depending on the original state of the relay.

6 An Alternative Interaction via SNMP

Supporting SNMP protocol allows the user to monitor the state of the platform (availability of connection, work time, free memory, CPU temperature etc.) and it gives limited options to control some of its functions. Supporting a configurable read community string, entitling only reading, and a write community string allowing to change the data, contributes to a more strict control on the use of Wake On LAN server.

Currently, using the SNMP protocol, only an alternative control of the state of the relays is supported. The perfect use of this option is in its combination with a network control system. Example:

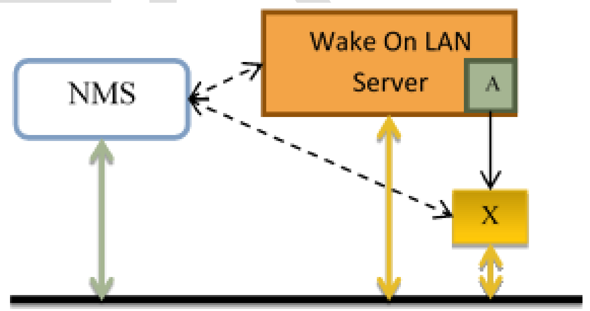

Fig. 1. Sample scenario

The continuous work of the device “X” in the local network must be ensured. The device supports ICMP or another method that allows regular inspection of its status. The system administrator has connected a controllable port (relay) "A" from the Wake On LAN server the physical button for restarting the device "X", so that it can be restarted with it.

In addition, the administrator has a system for managing networks, which is configured to monitor "X", and through the SNMP protocol to interact with the developed platform. The actions, configured for the system to take for controling networks in establishing that the device "X" is not available for more than 10 minutes, is to send three requests to change the state of the hardware port "A" of Wake On LAN server with an interval between requests of about 200 milliseconds and corresponding set values for the state of the port "A" 0, 1 and 0.

Thus restarting the system is automated, without the need for any human intervention, by simulation of pressing its physical button.

7 Hardware changes

From the general scheme of the new hardware version of the platform [2], [3], we see that the minimum supply voltage is 5V. This is due to the fact that there are already available relays, for which the recommended control voltage is 5V. When submitting just as much to the power inputs of the scheme, the voltage which reaches the managing coils of the relays is lower, but nevertheless sufficient to activate them. For reliable operation of the device, it is recommended a supply voltage of 7.5V to 25V, which will ensure 3.3V for the primary and network microcontroller and also 5V for the relays.

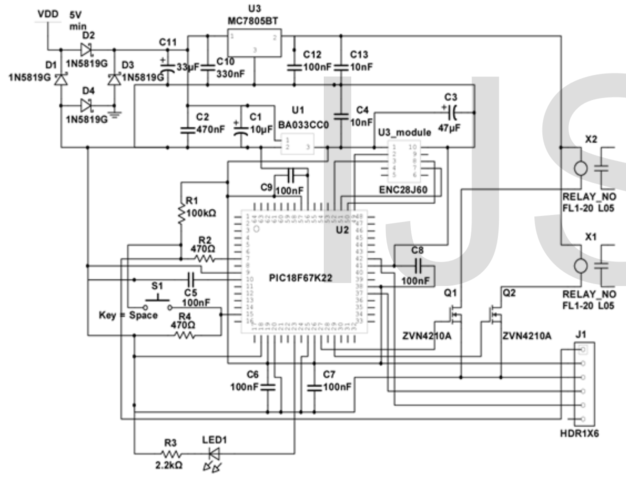

Fig. 2. General scheme of the new hardware version.

The power protection implemented through a full bridge rectifier with Schottky diodes 1N5819G, with a low voltage drop, which at 120 mA were measured about 0.2V for a diode. In comparison with the same current, full protection with only 1 Schottky diode SF16 was measured to have a drop of 0.7V. That is particularly for this part of the scheme, the protection is improved without it making the requirement for the voltage higher.

Novelty in power components is the added 5 volt linear voltage regulator 7805. Its presence is necessary because there are relays, which are controlled with 5V voltage and it provides them with power. Finding 3.3 volt relays at a price close to that of the 5 volt their analogues, proved to be a difficult task, making the choice of 5 volt relays less expensive.

Managing the relays themselves cannot be performed directly by the microcontroller, as its outputs can not provide the required amount of electricity, which is about 35 to 40 mA for a relay. That is why, for their management are used N-channel enhanced MOSFET transistors, which are sufficient to manage with a voltage of 3.3V, electricity consumption is minimal and only reaches a few tens of microamps.

Another innovation is the switch (hardware implemented with a touch button) connected to pin 15 of the microcontroller, which serves to reset the device to its factory settings (IP address, MAC address, passwords, a list of saved devices etc.) and is software protected from accidental activation. The protection implementation is simple - the button is active only a few milliseconds after turning on the device, then it becomes unusable. This forces the user to use it to press before plugging the device into the electric grid and to keep it in the same position for a short time after the device has been turned on.

7 CONCLUSION

The above changes and improvements significantly help in installing and configuring new devices for LAN-type "Wake On LAN server", as well as the software and hardware aspect of the process of interaction between them.

The limited use of the SNMP protocol as a standard alternative to the graphical user interface hints at the possibility of further integration of the platform with other systems and software, as this is one of the possibilities for a future development.

Adding new hardware elements makes the prototype 23% more expensive and increases the maximum power consumption in the worst case by 35%. However, its parameters and price,taking into account its narrow specialization,can be defined as adequate and preferred to those of other platforms having such a potential as Raspberry Pi, Orange Pi, C.H.I.P. and Arduino.

References

[1] AMD, "Magic Packet Technology," November 1995, [Online], Available: http://support.amd.com/TechDocs/20213.pdf., [Accessed 08 December 2015]

[2] G. Stoitsov and Z. Guglev, "Server for Remote Generation of Wake On LAN Packets in the LAN", International Journal of Recent Development in Engineering and Technology, vol. 3, no. 2, p. 6, 27 August 2014

[3] G. Stoitsov and Z. Guglev, „Integrating a Server for Remote Generation of Wake on LAN Packets to Network Management Systems“, International Journal of Software and Web Sciences (IJSWS), vol.1, № 13, pp. 17 - 21, August 2015

[4] IETF, "INTERNET CONTROL MESSAGE PROTOCOL: DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION", September 1981, [Online], Available: https://tools.ietf.org/html/rfc792, [Accessed 08 December 2015]

[5] Microchip, "Microchip PIC18F87K22 Family Data Sheet", 10 June 2011, [Online], Available: http://ww1.microchip.com/downloads/en/DeviceDoc/39960d.pdf, [Accessed 05 December 2015]

[6] Microchip, "Microchip v2013-06-15 TCPIP Stack Help", 2013

[7] Microsoft, "TechNet - How SNMP works", [Online], Available:

https://technet.microsoft.com/en-us/library/cc783142%28v=ws.10%29.aspx, [Accessed 01 December 2015]

[8] Microsoft, „TN NetBIOS Over TCP/IP“, [Online], Available: https://technet.microsoft.com/en-us/library/cc940063.aspx, [Accessed 08 December 2015]

[9] Network Working Group, „PROTOCOL STANDARD FOR A NetBIOS SERVICE: CONCEPTS AND METHODS“, March 1987, [Online], Available: http://www.networksorcery.com/enp/rfc/rfc1001.txt, [Accessed 08 December 2015]

[10] Network Working Group, „PROTOCOL STANDARD FOR A NetBIOS SERVICE: DETAILED SPECIFICATIONS“, March 1987, [Online], Available: http://www.networksorcery.com/enp/rfc/rfc1002.txt. [Accessed 08 December 2015]

[11] Network Working Group, IETF, "A Simple Network Management Protocol (SNMP)", May 1990, [Online], Available: https://wiki.tools.ietf.org/html/rfc1157, [Accessed 08 December 2015]

[12] Network Working Group, R. Droms, Bucknell University, „BOOTP / DHCP Options“, [Online], Available: http://www.networksorcery.com/enp/protocol/bootp/options.htm, [Accessed 08 December 2015]

[13] Network Working Group, R. Droms, Bucknell University, „DHCP, Dynamic Host Configuration Protocol“, [Online], Available: http://www.networksorcery.com/enp/protocol/dhcp.htm, [Accessed 08 December 2015]

[14] Rajbharti, Nilesh; Microchip, "AN833 - The Microchip TCP/IP Stack", 2002, [Online], Available: http://ww1.microchip.com/downloads/en/AppNotes/00833b.pdf, [Accessed 08 December 2015]

[15] Shirbhate, Amit; Microchip, "AN870 - SNMP V2c Agent for Microchip TCP/IP Stack", 2009, [Online], Available: http://ww1.microchip.com/downloads/en/AppNotes/00870b.pdf, [Accessed 08 December 2015]