

On-Line Inspection System of Integrated Automation Network Equipment in Coal Mine

Jitong Zhang

School of Information Engineering, Zhengzhou University of Industrial Technology,
Zhengzhou Henan 451150, PR China

Keywords: Coal mine; Raw socket; IP; ICMP; Automation; Ping

Abstract. Due to the improvement of information and automation level in coal mines, there are more and more network devices with IP addressing. Whether we can detect their online status in time will directly affect the monitoring and control safety of the whole integrated automation system in coal mines. Based on the raw socket according to the underlying network design technology, ICMP data packet to the target device to send ECHO_REQUEST on the network, to determine whether the target device is online according to the target device returns a result, the status of network equipment to realize real-time display and alarm function with SVG technology.

Introduction

With the development of coal mine informatization and automation, the scale of communication network is expanding and extending [1-3], the system and equipment connected to the network are more and more, especially in the coal mine comprehensive automation system, including underground pump room, underground substation, underground belt, downhole overhead passenger device, downhole winch, main and auxiliary shaft hoisting The system of main fan, fan, boiler, boiler, screening system, well substation, personnel positioning, tile phase monitoring system, these systems can be monitored, controlled, and data collected by the corresponding network equipment such as the lower computer, PLC, single chip microcomputer, TT & C main station, TT & C substation, switch and router. And transmission and other functions. The number of network equipment is becoming more and more large, their online or not will directly affect the remote monitoring and remote control of the equipment, even affect the safety of the mine equipment, and then affect the safety of mine production and the safety of the personal safety [4-5].

Present Situation

Because a large number of automation and information systems in the coal mine are connected to the industrial ring network, the information is transmitted to the centralized control center through the ring network. Due to the limitations of the human and system itself, some systems or equipment are not online for a long time and the monitoring personnel fail to find it in time, leading to some equipment damage or equipment failure or failure. The safety accidents caused by shutdown even cause accidents of personal or equipment, which cause the economic loss and personal injury of the coal mine, which seriously affects the safe operation of the coal mine.

When the monitoring personnel find that the system is not running normally, the usual method is to find the IP address of the network equipment of the corresponding system, and then use the ping command to detect whether the network device is online [6]. If not online, the relevant maintenance personnel will be informed of the network and system related equipment to be checked to determine the system is not in The cause of the line. Since the configuration software of the automatic monitoring system is usually stored by two data tables, one is a real-time table. The new data collected from the lower computer covers the data in the real-time table. The display of the real-time state of the system is the data collected in the real time table; the other is the storage and storage of historical data, which is mainly used for the generation of the calendar. History curve and equipment history data query and report generation. The data of the real time table does not update for a long time and can not cause the exception of the data of the configuration picture. Unless the

monitoring configuration screen is refreshed, it may be a long time to discover that the system is not online. The traditional method can not find out the network equipment is not online in time, resulting in a system of security problems. Even if a problem is found, it is very troublesome to confirm it, which is time-consuming and laborious. It urgently needs a system that can monitor the real-time state of each network device in real time.

Common Methods to Detect Network Equipment Online

Single ping command. The detection of a single network device is usually used in the way of entering the ping command at the command window to carry out [6]. In this way, it is usually the monitoring staff to confirm whether the network device is online, the efficiency is low, and is usually used to detect a single or a small number of network devices. This requires monitoring personnel to master some commonly used network commands and understand the computer and network related knowledge, which is more demanding for coal miners.

Batch processing ping command. For multiple network devices, the IP address of a set of network devices is usually placed in a text file, using batch files to read or directly write the IP address into multiple Ping commands and use the ping command to detect it. This case is suitable for more network devices with higher efficiency, but the results are not displayed. Intuitionistic, when the equipment is more, it is difficult to check the detection of a certain device. In addition, it is difficult to maintain the text of the IP address. At the same time, it needs to write the corresponding batch file. It is not suitable for large and medium-sized coal mines.

Ping command result redirects text file. This method can save the IP address of the related network device in the database table, use the shell command of the advanced language, read the IP address from the database table, then use the ping command, and redirect the result into the text file. Then the program reads the detection result of the Ping from the text file to judge the current network is Without connectivity, the results can be displayed graphically in the interface, making the results more intuitive. The advantage of this method is that programming is simple and the Ping commands provided by the system can be directly used to display and save the results in a variety of ways. The shortcoming is that the efficiency of program execution is low and the speed is slow. If the number of network equipment is large, it takes a long time to poll. In addition, the program needs to write and read a large number of files. The amount of IO is large and the IO fault is easy to appear. The robustness and efficiency of the program are still rare to be guaranteed.

In order to realize the efficient and timely on-line detection of network equipment, and display in GIS graphical mode, and realize the real-time alarm function when the equipment is not online, the system should adopt the underlying network programming technology based on TCP/IP protocol cluster, that is to use the original socket to send the ICMP message of ECHO_REQUEST to the target device.

Online Detection System Based on ICMP

Realization principle. The original socket can be used to program the underlying protocol of the network. It can capture the IP packet of the system, and can modify the head and data part of the IP packet arbitrarily, and the kernel system can no longer process the IP packets we have processed, and send it directly to the network. The on-line detection of network equipment is to use ICMP to send ECHO_REQUEST request message to the target host, and receive the ECHO_REPLY response message returned by the target host, and judge whether the network is connected according to the return result. And the ICMP message is in the data part of the IP packet, so to capture and construct the ICMP data message, you must first use the original socket to capture the IP packet, and fill the related data according to the head structure of the IP packet and the header structure of the ICMP message. The relationship between ICMP and IP packets is shown in table 1.

Table 1 ICMP and IP data packets

IP head	IP data section
IP head	ICMP data message
IP data package	

ICMP message head structure. The head structure of ICMP is complex, which mainly includes message type `icmp_type`, message code `icmp_code`, check and `icmp_checksum` [12-13], different ICMP types and other parts of code value are also different, the specific head structure is shown in Figure 2.

Table 2 Format of ICMP data message

Type (8bit)	Code (8bit)	Check sum (16bit)
(different types and codes are different in format)		

IP head structure. IP protocol is the most important protocol in TCP/IP protocol. It is the core of TCP/IP protocol cluster. Currently, there are two versions, one is IPv4, the other is IPv6. It provides a transmission channel [13-14] for TCP, UDP, ICMP and other protocols. Its main function is to provide the interconnection of subnetworks to form a larger network to enable the transmission of data between different subnets. The structure of the head is shown in 3.

Table 3 Format of IP data message

Version (4b)	head length (4b)	type of service (8b)	total length (16b)	
Identification (16b)			identification (3b)	slice offset (13b)
Survival time (8b)		protocol type (8b)	header checksum and (16b)	
Source IP address (32b)				
Target IP address (32b)				
Option (32b)				
Data section				

Implementation process. The system first uses `SOCK_RAW` to set the protocol type and select the `IPPROTO_ICMP` keyword to select the ICMP protocol [15-16], and to set up the `IP_HDRINCL` socket option to initialize the original socket and construct the `ECHO_REQUEST` message. The type of the message is 8, the code bit is 0, and the specific message format is shown in Figure 2. The IP address of the target device is removed from the database table, and the corresponding IP address is converted from the native byte order to the network byte order, and the corresponding target host IP address member of the IP header structure is assigned to the other data members of the IP head structure based on the IP header structure. The specific structure of the IP header is shown in Figure 3. Since the original socket sets all the relevant data sets of IP packets to the user, a function is also designed to calculate the CRC16 check sum of the IP packet and fill the corresponding position of the IP header structure. The filling of the data part of the ICMP message needs to meet the minimum length of 46 bytes of the Ethernet packet, and the data portion of the

ICMP message can be filled with arbitrary data. For the received return data message, we should first locate the initial address of the ICMP data message according to the head length and the total length of the IP data packet, and judge the type of the return message, and detect the return result to determine whether the target host is connected. If it is not connected, the information is stored in the alarm information table, and the system is also kept. The corresponding acousto-optic alarm information is given, and the equipment connection status on the GIS diagram is updated, and the green line of the access path is changed into a red line with open circuit. Then the system continues to polling the rest of the IP address, updating the latest detection state on the GIS map in real time, to achieve real-time monitoring of the connected state of all network equipment, and timely remind users that some equipment is in a state of circuit breakage, and the monitoring personnel notify the related personnel to enter the line detection and equipment maintenance, and ensure the coal mine. The normal operation of the entire automation network equipment will further ensure the safety and online operation of the entire automation system.

Conclusion

The real time on-line detection system of coal mine integrated automation network equipment is realized by using the ICMP message protocol of the original socket. It can automatically detect the online equipment online in the automatic ring network by polling. When some network devices in the ring are not online, it can be found in time and reported in the sound and light mode. The police remind the monitoring personnel to inform the maintenance personnel in time to carry out the inspection and maintenance of equipment and lines, to ensure the real-time online online equipment and the remote monitoring and automatic control of the automation equipment, so as to ensure the safety of the mine and the personal safety of the personnel. At the same time, the system shows the location, type of equipment, device name and IP address of all automatic network devices with GIS diagram, and displays the online status of the current device in different configuration forms. In addition, the history alarm data are queried according to different types of network devices according to categories, regions and time periods. The application of the system avoids the damage of the equipment caused by the long time without on-line equipment and the failure to detect the safety accidents caused by the failure of the equipment in time because the equipment is not on-line. The security of network and network equipment is the premise guarantee of coal mine information and automation. It is the foundation of digital mine. The network equipment on-line detection system based on the original socket can monitor the running state of the network in real time.

References

- [1] Li Yaru, Lu Donggui, Han an. A comprehensive analysis method for coal mine automation and early warning [J]. automation of industry and mining, 2017,43 (07): 93-96.
- [2] Chen Yunqi, Lu Yuanxiang. Research and application of collaborative management and control platform for coal mine informatization [J]. coal engineering, 2016,48 (06): 29-32.
- [3] Liu Xinjun, Yang Yanmei. Research on service and structure of coal mine Internet of things [J]. coal technology, 2016,35 (08): 241-242.
- [4] Tan Zhanglu, Li Guangda. Research and design of coal mine visual integrated management platform [J]. China coal, 2016,42 (08): 64-68.
- [5] Sun Peng. Design and implementation of coal mine integrated automation system, [D]. University of Electronic Science and technology, 2014.
- [6] Zou Huizhi, Huang Yuxue, Fu Minhui. Ship borne station measurement and control communication network microcomputer online detection system [J]. computer and modernization, 2007 (01): 71-73.
- [7] Song Jingbin. Linux network programming [M]. Beijing: Tsinghua University press, 2014.
- [8] Lawrence Berkeley. TCP/IP Vol. 1: protocol [M]. Beijing: China Machine Press, 2000.
- [9] Gary.Wrigh, W.Richard Stevens. TCP/IP detailed explanation [M]. Beijing: Machinery Industry Press, 2000.

- [10] (USA) Chappell, (USA) Titelt. TCP/IP protocol principle and application [M]. Beijing: Tsinghua University press, 2009.
- [11] (USA) BehrouzA. Forouzan. TCP/IP protocol family [M]. Beijing: Tsinghua University press, 2009.
- [12] Ren Tai Ming. TCP/IP network programming [M]. Beijing: people post and Telecommunications Publishing House, 2009.
- [13] Bob Quinn, Dave Shute. Windows Sockets network programming [M]. Beijing: Machinery Industry Press, 2012.