IEMP\_CLIENT documentation

Author: Qian Cheng

Contents

[IEMP\_CLIENT documentation 1](#_Toc83745555)

[1. Main communication module 2](#_Toc83745556)

[1.1 Communication specification 2](#_Toc83745557)

[1.2 dynamic password 2](#_Toc83745558)

[1.3 System operation module (0x00) 3](#_Toc83745559)

[1.3.1 Shutdown (0x01) 3](#_Toc83745560)

[1.3.2 Restart (0x01) 3](#_Toc83745561)

[1.3.3 Sleep (0x04) 3](#_Toc83745562)

[1.3.4 Execute the specified cmd command line (0x06) 3](#_Toc83745563)

[1.4 File operation class (0x02) 3](#_Toc83745564)

[1.4.1 Server download file to local (0x00) 3](#_Toc83745565)

[1.4.2 Local upload file to server (0x01) 4](#_Toc83745566)

[1.4.3 List the list of files (0x02) 4](#_Toc83745567)

# Main communication module

## Communication specification

The primary communication module uses TCP communication, the default monitoring 48280 port, this listener cannot be modified or off via the configuration file. When communicating with the main module, the server is communicating, the maximum instruction length is 65537 bytes, wherein the front two bytes (i.e., 0-1 bytes) have the total length of data. For example, if the total length of the instruction is required to be 25 bytes, the value of the first two bytes is 0x17, 0x00, and the valid data length of the representative is 23 bits, and the program will prepare 23 CHAR memory space to receive. These data. The after 8 bytes (ie 2-9 bytes) are dynamic passwords. Dynamic password related technology, see the "Dynamic Password" section of this module. Then 2 bytes (ie 10-11 bytes), for the actual instruction type, the 10th byte is a class, the 11th byte is a small class of the instruction type. The subsequent byte is empty according to the actual instruction or the data required by the actual instruction, and is handed over to the small class.

## dynamic password

Dynamic password first relies on a 16-byte length fixed password and a native time. The 16-bit fixed password is stored by the configuration file, which is randomly generated by the deployment program, and the configuration file related information, see the "Profile" section of this module. The program will calculate the corresponding UTC time through this machine time, and removed at 30 to obtain a value plus 1 per 30 seconds. Then this value will be converted to 4-bit char (like the memory size, you can copy this value directly). The 16-bit password is connected to this 4-bit char connection as a 20-byte data, which will be calculated by the MD5 value. The MD5 value is 16 bits, but only 8 digits are required here, so this program will take the 0th byte with the 8th word, and save the 0th byte, the first byte and the 9th byte Take it and save back to the first byte, and so on, finally get an 8-byte data, which is the encrypted dynamic password, because only 90 seconds of the validity period (see annotation 1), and cannot be reversed, so Plateaus communication.

\* Note 1: To avoid problems caused by communication delay and time error, IEMP\_CLIENT will try to compare with the current time, + 30 seconds, -30 seconds when receiving dynamic passwords and verify, arbitrarily compared with the current time, + 30 seconds, -30 seconds Password matches will be considered successful.

## System operation module (0x00)

### Shutdown (0x01)

Windows operating system execution: "shutdown -p" \* This command is not available under WinPE

LINUX operating system under: "Shutdown -h Now"

### Restart (0x01)

Windows operating system execution: "shutdown -r -t 0" \* This command is not available under WinPE

LINUX operating system execution: "restart"

### Sleep (0x04)

Windows operating system under instructions: "shutdown -h" \* This command is not available under WinPE

### Execute the specified cmd command line (0x06)

When this operation is performed, the command line you need to perform is connected to the necessary 11-byte communication content, the program will be directly charged by the command line.

## File operation class (0x02)

### Server download file to local (0x00)

The 12th bit of incoming data is set (the first 11 bits is the transmission must be byte), which is the 0th bit of the effective data of this method. First, in the complete file path in the C language standard. This string ends at 0x00, followed by the value of 8-bit char types, which represents the length of the file with a length of 8 bytes, which is a long long int type in Windows, to support large-capacity files (this The program has strongly referred to using the program to transmit too large files, and the internal network group is 100MB or more files. It is recommended to use the "BitTorrent module" to increase efficiency). Then accept the file according to this file and store it into the corresponding path, such as the path originally presented file, then execute a prompt coverage.

### Local upload file to server (0x01)

### List the list of files (0x02)

The 12th bit of incoming data is set (the first 11 bits is the transmission must be byte), which is the 0th bit of the effective data of this method. First, the path that needs to list the folder is ended at 0x00 with the C language standard. When the file is listed, a string is generated according to each file and connected to each file, for each file or folder, the first bit is the file type, 0x04 is a folder, 0x08 is a file, if the folder is folder, then After the type, there is an integer representing the length of the file name, following a full file name. If you are file, then follow the file size information, the minimum is 0, the maximum is a long long int, indicating that the file name is like a folder.