

**GPS Tracker  
Communication Protocol**

**CONFIDENTIAL**

---

## CONTENT

I.	COMMUNICATION PROTOCOL .....	4
II.	TERMS, DEFINITIONS .....	4
III.	BASIC RULES .....	6
IV.	DATA PACKET FORMAT .....	8
4.1.	START BIT .....	8
4.2.	PACKET LENGTH .....	8
4.3.	PROTOCOL NUMBER .....	8
4.4.	INFORMATION CONTENTS .....	8
4.5.	INFORMATION SERIAL NUMBER .....	8
4.6.	ERROR CHECK .....	8
4.7.	STOP BIT .....	9
5.1.	LOGIN MESSAGE PACKET .....	9
5.1.1.	Terminal Sending Data Packet to Server .....	9
5.1.1.1.	Start Bit .....	9
5.1.1.2.	Packet Length .....	9
5.1.1.3.	Protocol Number .....	9
5.1.1.4.	Terminal ID .....	9
5.1.1.5.	Information Serial Number .....	9
5.1.1.6.	Error Check .....	9
5.1.1.7.	Stop Bit .....	10
5.1.2.	Server Responds the Data Packet .....	10
5.1.2.1.	Start Bit .....	10
5.1.2.2.	Packet Length .....	10
5.1.2.3.	Protocol Number .....	10
5.1.2.4.	Information Serial Number .....	10
5.1.2.5.	Error Check .....	10
5.1.2.6.	Stop Bit .....	10
5.1.3.	Examples .....	10
5.2.	LOCATION DATA PACKET (COMBINED INFORMATION PACKAGE OF GPS AND LBS) .....	11
5.2.1.	Terminal Sending Location Data Packet to Server .....	11
5.2.1.1.	Start Bit .....	12
5.2.1.2.	Packet Length .....	12
5.2.1.3.	Protocol Number .....	12
5.2.1.4.	Date Time .....	12
5.2.1.5.	Length of GPS information, quantity of positioning satellites .....	12
5.2.1.6.	Latitude .....	12
5.2.1.7.	Longitude .....	13
5.2.1.8.	Speed .....	13
5.2.1.9.	Course & Status .....	13

---

5.2.1.10.	MCC .....	14
5.2.1.11.	MNC .....	14
5.2.1.12.	LAC .....	14
5.2.1.13.	Cell ID .....	14
5.2.1.14.	Information Serial Number .....	15
5.2.1.15.	Error Check .....	15
5.2.1.16.	Stop Bit .....	15
5.2.2.	Examples of Packet Sent from Terminal to Server .....	15
5.3.	ALARM PACKET (COMBINED INFORMATION PACKET OF GPS, LBS AND STATUS) .....	16
5.3.1.	Server Sending Alarm Data Packet to Server .....	16
5.3.1.1.	Start Bit .....	16
5.3.1.2.	Packet Length .....	16
5.3.1.3.	Protocol Number .....	16
5.3.1.4.	Date Time .....	16
5.3.1.5.	Length of GPS information, quantity of positioning satellites .....	16
5.3.1.6.	Latitude .....	16
5.3.1.7.	Longitude .....	16
5.3.1.8.	Speed .....	16
5.3.1.9.	Status and Course .....	17
5.3.1.10.	MCC .....	17
5.3.1.11.	MNC .....	17
5.3.1.12.	LAC .....	17
5.3.1.13.	Cell ID .....	17
5.3.1.14.	Terminal Information .....	17
5.3.1.15.	Voltage Level .....	17
5.3.1.16.	GSM Signal Strength Levels .....	17
5.3.1.17.	Alarm/Language .....	18
5.3.1.18.	Information Serial Number .....	18
5.3.1.19.	Error Check .....	18
5.3.1.20.	Stop Bit .....	18
5.3.1.21.	Examples .....	18
5.3.2.	Server responding alarm data packet to terminal .....	19
5.3.2.1.	Start Bit .....	19
	For details see Data Packet Format section 4.1 .....	19
5.3.2.2.	Packet Length .....	19
	For details see Data Packet Format section 4.2 .....	19
5.3.2.3.	Protocol Number .....	19
	For details see Data Packet Format section 4.3 .....	19
5.3.2.4.	Serial Number .....	19
	For details see Data Packet Format section 4.5 .....	19
5.3.2.5.	Error Check .....	19
	For details see Data Packet Format section 4.6 .....	19
5.3.2.6.	Stop Bit .....	19
	For details see Data Packet Format section 4.7 .....	19

---

---

5.3.2.7.	Examples .....	19
5.3.3.	Server responding alarm data address packet to Terminal .....	20
5.3.3.1.	Response package in Chinese .....	20
5.3.3.2.	Response package in English .....	21
5.4.	HEARTBEAT PACKET (STATUS INFORMATION PACKET) .....	23
5.4.1.	Terminal Sending Heartbeat Packet to Server .....	23
5.4.1.1.	Start Bit .....	23
5.4.1.2.	Packet Length .....	23
5.4.1.3.	Protocol Number .....	23
5.4.1.4.	Terminal Information .....	23
5.4.1.5.	Voltage Level .....	24
5.4.1.6.	GSM Signal Strength Levels .....	24
5.4.1.7.	Alarm/Language .....	24
5.4.1.8.	Information Serial Number .....	24
5.4.1.9.	Error Check .....	24
5.4.1.10.	Stop Bit .....	24
5.4.2.	Server Responds the Data Packet .....	25
5.4.2.1.	Start Bit .....	25
5.4.2.2.	Packet Length .....	25
5.4.2.3.	Protocol Number .....	25
5.4.2.4.	Information Serial Number .....	25
5.4.2.5.	Error Check .....	25
5.4.2.6.	Stop Bit .....	25
5.4.3.	Examples .....	25
<b>VI.</b>	<b>DATA PACKET SENT FROM SERVER TO TERMINAL .....</b>	<b>26</b>
6.1.	PACKET SENT BY SERVER .....	26
6.1.1.	Start Bit .....	26
6.1.2.	Packet Length .....	26
6.1.3.	Protocol Number .....	26
6.1.4.	Length of Command .....	26
6.1.5.	Server Flag Bit .....	26
6.1.6.	Command Content .....	26
6.1.7.	Information Serial Number .....	26
6.1.8.	Error Check .....	26
6.1.9.	Stop Bit .....	26
6.2.	PACKET REPLIED BY TERMINAL .....	26
6.2.1.	Start Bit .....	27
6.2.2.	Packet Length .....	27
6.2.3.	Protocol Number .....	27
6.2.4.	Length of Command .....	27
6.2.5.	Server Flag Bit .....	27
6.2.6.	Command Content .....	27
6.2.7.	Language .....	27
6.2.8.	Information Serial Number .....	27

---

6.2.9.	Error Check .....	27
6.2.10.	Stop Bit .....	27
6.3.	Looking Up Location Information .....	27
6.4.	Cutting Oil and Electricity .....	28
6.5.	Connecting Oil and Electricity .....	28
6.6.	Address Querying Information Sent by the Server .....	28
6.7.	GPS, Phone Number Querying Address Information Package (0X1A) .....	30
6.7.1.	Information from Terminal to Server .....	30
6.7.1.1.	Start Bit .....	30
6.7.1.2.	Packet Length .....	30
6.7.1.3.	Protocol Number .....	30
6.7.1.4.	Date Time .....	30
6.7.1.5.	Length of GPS information, quantity of positioning satellites .....	30
6.7.1.6.	Latitude .....	30
6.7.1.7.	Longitude .....	30
6.7.1.8.	Speed .....	31
6.7.1.9.	Course .....	31
6.7.1.10.	Phone Number .....	31
6.7.1.11.	Language .....	31
6.7.1.12.	Information Serial Number .....	31
6.7.1.13.	Error Check .....	31
6.7.1.14.	Stop Bit .....	31
6.7.2.	Response of Server .....	31
6.7.2.1.	Response package in Chinese .....	31
6.7.2.2.	Response package in English .....	32
<b>VII. APPENDIX A: CODE FRAGMENT OF THE CRC-ITU LOOKUP TABLE ALGORITHM IMPLEMENTED BASED ON C LANGUAGE .....</b>		<b>34</b>
<b>VIII. APPENDIX B: A FRAGMENT OF EXAMPLE OF DATA PACKET OF COMMUNICATION PROTOCOL</b>		<b>35</b>
<b>IX. APPENDIX C: COMPLETE FORMAT OF THE INFORMATION PACKAGE .....</b>		<b>38</b>

## Communication Protocol

### Introduction

This document defines instructions about interface protocol on application layer of vehicles GPS tracker and location-based service platform. Related interface protocol only applies in the interaction between the platform and the position terminal.

#### i. Terms, Definitions

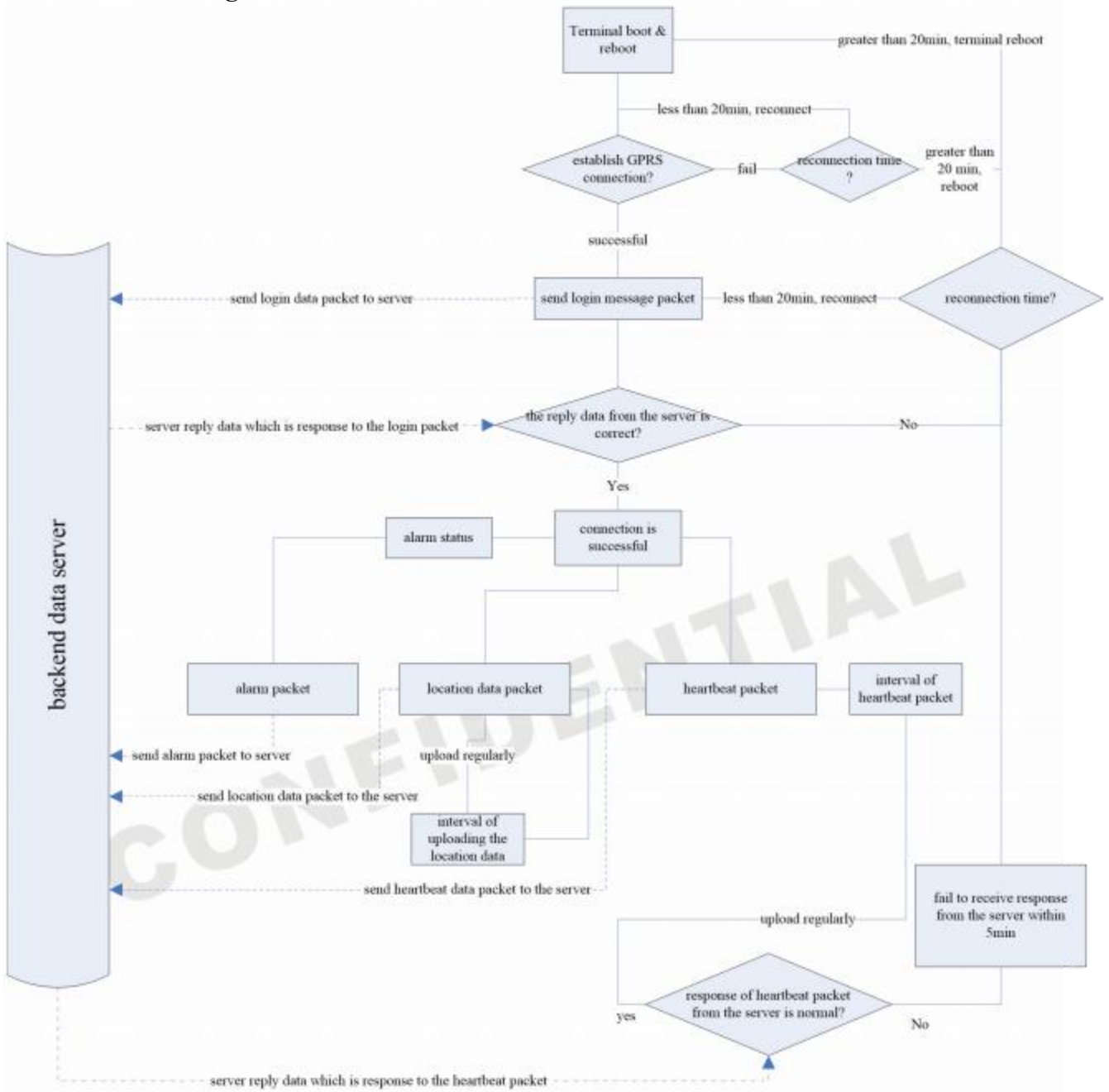
Terms, Abbreviation	Definition in English	Definition in Chinese
CMPP	China Mobile Peer to Peer	中国移动点对点协议
GPS	Global Positioning System	全球卫星定位系统
GSM	Global System for Mobile Communication	全球移动通信系统
GPRS	General Packet Radio Service	通用无线分组业务

TCP	Transport Control Protocol	传输控制协议
LBS	Location Based Services	辅助定位服务
IMEI	International Mobile Equipment Identity	国际移动设备识别码
MCC	Mobile Country Code	移动用户所属国家代号
MNC	Mobile Network Code	移动网号码
LAC	Location Area Code	位置区码
Cell ID	Cell Tower ID	移动基站
UDP	User Datagram Protocol	用户数据报协议
SOS	Save Our Ship/Save Our Souls	遇难求救信号
CRC	Cyclic Redundancy Check	循环冗余校验
NITZ	Network Identity and Time Zone,	时区
GIS	Geographic Information System	地理信息系统

**ii. Basic Rules**

1. If a GPRS connection is established successfully, the terminal will send a first login message packet to the server and, within five seconds, if the terminal receives a data packet responded by the server, the connection is considered to be a normal connection. The terminal will begin to send location information (i.e., GPS, LBS information package). A status information package will be sent by the terminal after three minutes to regularly confirm the connection.
2. If the GPRS connection is established unsuccessfully, the terminal will not be able to send the login message packet. The terminal will start schedule reboot in twenty minutes if the GPRS connection is failed three times. Within twenty minutes, if the terminal successfully connects to the server and receives the data packet from the server as the server's response to the login message packet sent by the terminal, the schedule reboot will be off and the terminal will not be rebooted; otherwise, the terminal will be rebooted automatically in twenty minutes.
3. After receiving the login message packet, the server will return a response data packet. If the terminal doesn't receive packet from the server within five seconds after sending the login message packet or the status information package, the current connection is regarded as an abnormal connection. The terminal will start a retransmission function for GPS tracking data, which will cause the terminal to disconnect the current GPRS connection, rebuild a new GPRS connection and send a login message packet again.
4. If the connection is regarded to be abnormal, and the data packet as a response from the server is failed to be received three times after a connection is established and a login message packet or status information package is sent, the terminal will start schedule reboot and the scheduled time is ten minutes. Within ten minutes, if the terminal successfully connects to the server and receives the data packet responded by the server, the schedule reboot will be off and the terminal will not be rebooted; otherwise, the terminal will be rebooted automatically in ten minutes.
5. In case of the normal connection, the terminal will send a combined information package of GPS and LBS to the server after the GPS information is changed; and the server may set a default protocol for transmission by using commands.
6. To ensure the effectiveness of the connection, the terminal will send status information to the server at regular intervals, and the server will return response data packets to confirm the connection.
7. For the terminal which doesn't register an IMEI number, the server will reply the terminal with a login request response and heartbeat packet response, rather than directly disconnect the connection. (If the connection is directly disconnected or the server doesn't reply to the terminal, it will lead to a continuous reconnected by the terminal and the GPRS traffic will be consumed heavily.)

Data Flow Diagram



#### iv. Data Packet Format

The communication is transferred asynchronously in bytes.

The total length of packets is (10+N) Bytes.

Format	Length(Byte)
Start Bit	2
Packet Length	1
Protocol Number	1
Information Content	N
Information Serial Number	2
Error Check	2
Stop Bit	2

##### 4.1. Start Bit

Fixed value in HEX 0x78 0x78.

##### 4.2. Packet Length

Length = Protocol Number + Information Content + Information Serial Number + Error Check, totally (5+N)Bytes, because the Information Content is a variable length field.

##### 4.3. Protocol Number

Type	Value
Login Message	0x01
Location Data	0x12
Status information	0x13
String information	0x15
Alarm data	0x16
GPS, query address information by phone number	0x1A
Command information sent by the server to the terminal	0x80

##### 4.4. Information Contents

The specific contents are determined by the protocol numbers corresponding to different applications.

##### 4.5. Information Serial Number

The serial number of the first GPRS data (including status packet and data packet such as GPS, LBS) sent after booting is '1', and the serial number of data sent later at each time will be automatically added '1'.

##### 4.6. Error Check

A check code may be used by the terminal or the server to distinguish whether the received information is error or not. To prevent errors occur during data transmission, error check is added to against data misoperation, so as to increase the security and efficiency of the system. The check code is generated by the CRC-ITU checking method.

The check codes of data in the structure of the protocol, from the Packet Length to the Information Serial Number (including "Packet Length" and "Information Serial Number") , are values of

---

CRC-ITU.

CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet.

#### 4.7. Stop Bit

Fixed value in HEX 0x0D 0x0A.

## V.Details about Data Packet sent by Server to Terminal

The commonly used information packages sent by the terminal and those sent by the server will be interpreted separately.

### 5.1. Login Message Packet

#### 5.1.1. Terminal Sending Data Packet to Server

The login message packet is used to be sent to the server with the terminal ID so as to confirm the established connection is normal or not.

	Description	Bits	Example
Login Message Packet(18 Byte)	Start Bit	2	<u>0x78 0x78</u>
	Packet Length	1	<u>0x0D</u>
	Protocol Number	1	<u>0x01</u>
	Terminal ID	8	<u>0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45</u>
	Information Serial Number	2	<u>0x00 0x01</u>
	Error Check	2	<u>0x8C 0xDD</u>
	Stop Bit	2	<u>0x0D 0x0</u>

##### 5.1.1.1. Start Bit

For details see Data Packet Format section 4. 1.

##### 5.1.1.2. Packet Length

For details see Data Packet Format section 4.2.

##### 5.1.1.3. Protocol Number

For details see Data Packet Format section 4.3.

##### 5.1.1.4. Terminal ID

The terminal ID applies IMEI number of 15 bits.

Example: if the IMEI is 123456789012345,

the terminal ID is 0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45.

##### 5.1.1.5. Information Serial Number

For details see Data Packet Format section 4.5.

##### 5.1.1.6. Error Check

For details see Data Packet Format section 4.6.

**5.1.1.7. Stop Bit**

For details see Data Packet Format section 4.7.

**5.1.2. Server Responds the Data Packet**

	Description	Bits	Example
Login Message Packet (18 Byte)	Start Bit	2	<u>0x78 0x78</u>
	Packet Length	1	<u>0x05</u>
	Protocol Number	1	<u>0x01</u>
	Information Serial Number	2	<u>0x00 0x01</u>
	Error Check	2	<u>0xD9 0xDC</u>
	Stop Bit	2	<u>0x0D 0x0A</u>

The response packet from the server to the terminal: the protocol number in the response packet is identical to the protocol number in the data packet sent by the terminal.

**5.1.2.1. Start Bit**

For details see Data Packet Format section 4. 1.

**5.1.2.2. Packet Length**

For details see Data Packet Format section 4.2.

**5.1.2.3. Protocol Number**

For details see Data Packet Format section 4.3.

**5.1.2.4. Information Serial Number**

For details see Data Packet Format section 4.5.

**5.1.2.5. Error Check**

For details see Data Packet Format section 4.6.

**5.1.2.6. Stop Bit**

For details see Data Packet Format section 4.7.

**5.1.3. Examples**

Examples of the login message packet sent by the terminal to the server and the response packet sent by the server to the terminal are as follows: (in the examples the terminal ID is 123456789012345).

**Example of data packet sent by the terminal** 78 78 0D 01 01 23 45 67 89 01 23 45 00 01 8C DD 0D 0A

**Explain**

<u>0x78 0x78</u>	<u>0x0D</u>	<u>0x01</u>	<u>0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45</u>	<u>0x00 0x01</u>	<u>0x8C</u> <u>0xDD</u>	<u>0x0D 0x0A</u>
Start Bit	Length	Protocol No.	Terminal ID	Serial No.	Error Check	Stop Bit

**Example of response packet returned by the server**  
78 78 05 01 00 01 D9 DC 0D 0A

**Explain**

<u>0x78 0x78</u>	<u>0x05</u>	<u>0x01</u>	<u>0x00 0x01</u>	<u>0xD9 0xDC</u>	<u>0x0D 0x0A</u>
Start Bit	Length	Protocol No.	Serial No.	Error Check	Stop Bit

## 5.2. Location Data Packet (combined information package of GPS and LBS)

### 5.2.1. Terminal Sending Location Data Packet to Server

Format of location data packet sent Server by default (mileage turned off).

Format		Length(Byte)	Example	
Information Content	Start Bit	2	0x78 0x78	
	Packet Length	1	0x1F	
	Protocol Number	1	0x12	
	GPS Information	Date Time	6	0x0B 0x08 0x1D 0x11 0x2E 0x10
		Quantity of GPS information satellites	1	0xCF
		Latitude	4	0x02 0x7A 0xC7 0xEB
		Longitude	4	0x0C 0x46 0x58 0x49
		Speed	1	0x00
		Course, Status	2	0x14 0x8F
		LBS Information	MCC	2
	MNC		1	0x00
	LAC		2	0x28 0x7D
	Cell ID		3	0x00 0x1F 0xB8
	Serial Number	2	0x00 0x03	
Error Check	2	0x80 0x81		
Stop Bit	2	0x0D 0x0A		

Format of location data packet sent Server by default (mileage turned on).

Format		Length(Byte)	Example	
Information Content	Start Bit	2	0x78 0x78	
	Packet Length	1	0x23	
	Protocol Number	1	0x12	
	GPS Information	Date Time	6	0x0B 0x08 0x1D 0x11 0x2E 0x10
		Quantity of GPS information satellites	1	0xCF
		Latitude	4	0x02 0x7A 0xC7 0xEB
		Longitude	4	0x0C 0x46 0x58 0x49
		Speed	1	0x00
		Course,	2	0x14 0x8F

		Status		
	LBS Information	MCC	2	0x01 0xCC
		MNC	1	0x00
		LAC	2	0x28 0x7D
		Cell ID	3	0x00 0x1F 0xB8
		Mileage	4	0x00 0x00 0x00 0x00
	Serial Number		2	0x00 0x03
	Error Check		2	0x61 0x90
	Stop Bit		2	0x0D 0x0A

#### 5.2.1.1. Start Bit

For details see Data Packet Format section 4. 1.

#### 5.2.1.2. Packet Length

For details see Data Packet Format section 4.2.

#### 5.2.1.3. Protocol Number

For details see Data Packet Format section 4.3.

#### 5.2.1.4. Date Time

Format	Length(Byte)	Example
Year	1	0x0A
Month	1	0x03
Day	1	0x17
Hour	1	0x0F
Minute	1	0x32
Second	1	0x17

Example: 2010-03-23 15:30:23

Calculated as follows:

10 (Decimal)=0A (Hexadecimal)

3 (Decimal)=03 (Hexadecimal)

23 (Decimal)=17 (Hexadecimal)

15 (Decimal)=0F (Hexadecimal)

50 (Decimal)=32 (Hexadecimal)

23 (Decimal)=17 (Hexadecimal)

Then the value is: 0x0A 0x03 0x17 0x0F 0x32 0x17

#### 5.2.1.5. Length of GPS information, quantity of positioning satellites

The field is 1 Byte displayed by two hex digits, wherein the first one is for the length of GPS information and the second one for the number of the satellites join in positioning.

Example: if the value is 0xCB, it means the length of GPS information is 12 and the number of the positioning satellites is 11.

(C = 12Bit Length , B = 11 satellites)

#### 5.2.1.6. Latitude

Four bytes are consumed, defining the latitude value of location data. The range of the value is 0-162000000, indicating a range of 0°-90°. The conversion method thereof is as follow:

Converting the value of latitude and longitude output by GPS module into a decimal based on minute;

multiplying the converted decimal by 30000; and converting the multiplied result into hexadecimal

Example:  $22^{\circ}32.7658' = (22 \times 60 + 32.7658) \times 30000 = 40582974$ , then converted into a hexadecimal number

$40582974(\text{Decimal}) = 26B3F3E(\text{Hexadecimal})$

at last the value is 0x02 0x6B 0x3F 0x3E.

**5.2.1.7. Longitude**

Four bytes are consumed, defining the longitude value of location data. The range of the value is 0-324000000, indicating a range of 0°- 180°.

The conversion method herein is same to the method mentioned in Latitude (see section 5.2. 1.6).

**5.2.1.8. Speed**

One byte is consumed, defining the running Speed of GPS. The value ranges from 0x00 to 0xFF indicating a range from 0 to 225km/h.

e.g. 0x00 represents 0 km/h.

0x10 represents 16km/h.

0xFF represents 255 km/h.

**5.2.1.9. Course & Status**

Two bytes are consumed, defining the running direction of GPS. The value ranges from 0° to 360° measured clockwise from north of 0°.

BYTE_1	Bit7	0	0: ACC OFF 1: ACC ON
	Bit6	0	1
	Bit5	GPS real-time/differential positioning	
	Bit4	GPS having been positioning or not	
	Bit3	East Longitude, West Longitude	
	Bit2	South Latitude, North Latitude	
	Bit1 Bit0	Course	
Bit7			
Bit6			
Bit5			
Bit4			
Bit3			
Bit2			
Bit1 Bit0			
BYTE_2	Bit7		
	Bit6		
	Bit5		
	Bit4		
	Bit3		
	Bit2		
	Bit1		
	Bit0		

CONFIDENTIAL

Note:

1. If the Bit6 in BYTE\_1 is 1, then the Bit7 is valid. In this case, if Bit7 is 1, means ACC ON; if it is 0, means ACC OFF.
2. The status information in the data packet is the status corresponding to the time bit recorded in the data packet.

For example: the value is 0x15 0x4C, the corresponding binary is 00010101 01001100,

BYTE_1 Bit7	0		
BYTE_1 Bit6	0		
BYTE_1 Bit5	0	(real time GPS)	
BYTE_1 Bit4	1	(GPS has been positioned)	
BYTE_1 Bit3	0	(East Longitude)	
BYTE_1 Bit2	1	(North Latitude)	
BYTE_1 Bit1	0	}	
BYTE_1 Bit0	1		
BYTE_2 Bit7	0		
BYTE_2 Bit6	1		
BYTE_2 Bit5	0		→ Course 332° (0101001100 in Binary, or 332 in decimal)
BYTE_2 Bit4	0		
BYTE_2 Bit3	1		
BYTE_2 Bit2	1		
BYTE_2 Bit1	0		
BYTE_2 Bit0	0		

which means GPS tracking is on, real time GPS, location at north latitude, east longitude and the course is 332°.

#### 5.2.1.10. MCC

The country code to which a mobile user belongs, i.e., Mobile Country Code(MCC).

Example: Chinese MCC is 460 in decimal, or 0x01 0xCC in Hex (that is, a decimal value of 460 converting into a hexadecimal value, and 0 is added at the left side because the converted hexadecimal value is less than four digits).

Herein the range is 0x0000 ~ 0x03E7.

#### 5.2.1.11. MNC

Mobile Network Code(MNC)

Example: Chinese MNC is 0x00.

#### 5.2.1.12. LAC

Location Area Code (LAC) included in LAI consists of two bytes and is encoded in hexadecimal. The available range is 0x0001-0xFFFFE, and the code group 0x0000 and 0xFFFF cannot be used. (See GSM specification 03.03, 04.08 and 11.11).

#### 5.2.1.13. Cell ID

Cell Tower ID (Cell ID), which values ranges from 0x000000 to 0xFFFFF.

#### 5.2.1.14. Mileage Statistics (after turned on)

Mileage statistics do mileage calculation and showed by hex.

CONFIDENTIAL

**5.2.1.15. Information Serial Number**

For details see Data Packet Format section 4.5.

**5.2.1.16. Error Check**

For details see Data Packet Format section 4.6.

**5.2.1.17. Stop Bit**

For details see Data Packet Format section 4.7.

**5.2.2. Examples of Packet Sent from Terminal to Server**

Example of sending by the terminal										
78 78 1F 12 0B 08 1D 11 2E 10 CC 02 7A C7 EB 0C 46 58 49 00 14 8F 01 CC 00 28 7D 00 1F B8 00 03 80 81 0D 0A										
Explain										
<u>0x78 0x78</u>	<u>0x1F</u>	<u>0x12</u>	<u>0x0B 0x08 0x1D 0x11 0x2E 0x10</u>				<u>0xCC</u>	<u>0x02 0x7A 0xC7 0xEB</u>		
Start Bit	Packet Length	Protocol No.	Date Time			Quantity of GPS information satellites	Latitude			
<u>0x0C 0x46 0x58 0x49</u>	<u>0x00</u>	<u>0x14 0x8F</u>	<u>0x01 0xCC</u>	<u>0x00</u>	<u>0x28 0x7D</u>	<u>0x00 0x1F 0xB8</u>	<u>0x00 0x03</u>			
Longitude		Speed	Course Status	MCC	MNC	LAC	Cell ID	Serial No.		
<u>0x80 0x81</u>	<u>0x0D 0x0A</u>									
Error Check	Stop Bit									

### 5.3. Alarm Packet (Combined information packet of GPS, LBS and Status)

#### 5.3.1. Server Sending Alarm Data Packet to Server

Format		Length (Byte)	
Information Content	Start Bit	2	
	Packet Length	1	
	Protocol Number	1	
	Date Time	6	
	GPS Information	Quantity of GPS information satellites	1
		Latitude	4
		Longitude	4
		Speed	1
	LBS Information	Course, Status	2
		LBS Length	1
		MCC	2
		MNC	1
		LAC	2
	status Information	Cell ID	3
		Terminal Information Content	1
		Voltage Level	1
		GSM Signal Strength	1
	Alarm/Language	2	
Serial Number	2		
Error Check	2		
Stop Bit	2		

Alarm packet is consisted by adding status information to location packet, so does the encoding format of the protocol.

##### 5.3.1.1. Start Bit

For details see Data Packet Format section 4. 1.

##### 5.3.1.2. Packet Length

For details see Data Packet Format section 4.2.

##### 5.3.1.3. Protocol Number

For details see Data Packet Format section 4.3.

##### 5.3.1.4. Date Time

For details see Location Data Packet Format section 5.2.1.4.

##### 5.3.1.5. Length of GPS information, quantity of positioning satellites

For details see Location Data Packet Format section 5.2.1.5.

##### 5.3.1.6. Latitude

For details see Location Data Packet Format section 5.2.1.6.

##### 5.3.1.7. Longitude

For details see Location Data Packet Format section 5.2.1.7.

##### 5.3.1.8. Speed

For details see Location Data Packet Format section 5.2.1.8.

**5.3.1.9. Status and Course**

For details see Location Data Packet Format section 5.2.1.9.

**5.3.1.10. MCC**

For details see Location Data Packet Format section 5.2.1.10.

**5.3.1.11. MNC**

For details see Location Data Packet Format section 5.2.1.11.

**5.3.1.12. LAC**

For details see Location Data Packet Format section 5.2.1.12.

**5.3.1.13. Cell ID**

For details see Location Data Packet Format section 5.2.1.13.

**5.3.1.14. Terminal Information**

One byte is consumed, defining various status information of the mobile phone.

Bit		Code Meaning
BYTE	Bit7	1: oil and electricity disconnected
		0: gas oil and electricity connected
	Bit6	1: GPS tracking is on
		0: GPS tracking is off
	Bit3~ Bit5	100: SOS
		011: Low Battery Alarm
		010: Power Cut Alarm
		001: Shock Alarm
	Bit2	000: Normal
		1: Charge On
	Bit1	0: Charge Off
		1: ACC high
	Bit0	0: ACC Low
		1: Defense Activated
	0: Defense Deactivated	

Example: 0x44, corresponding binary value is 01000100, indicates that the status of the terminal is: oil and electricity connected, GPS tracking is on, normal without any alarm, charge on, ACC is low, and defense deactivated.

**5.3.1.15. Voltage Level**

The range is 0~6 defining the voltage is from low to high.

- 0: No Power (shutdown)
- 1: Extremely Low Battery (not enough for calling or sending text messages, etc.)
- 2: Very Low Battery (Low Battery Alarm)
- 3: Low Battery (can be used normally)
- 4: Medium
- 5: High
- 6: Very High

Example: 0x02 indicates very low battery and a Low Battery Alarm is sending.

**5.3.1.16. GSM Signal Strength Levels**

0x00: no signal;

---

0x01: extremely weak signal;

0x02: very weak signal;

0x03: good signal;

0x04: strong signal.

Example: 0x03 indicates the GSM signal is good.

### 5.3.1.17. Alarm/Language

0x00 (former bit) 0x01 (latter bit)

former bit: terminal alarm status (suitable for alarm packet and electronic fence project)

latter bit: the current language used in the terminal

former bit	0x00: normal
	0x01: SOS
	0x02: Power Cut Alarm
	0x03: Shock Alarm
	0x04: Fence In Alarm
	0x05: Fence Out Alarm
	0x06 Over Speed Alarm
	0x29 Rapid acceleration
	0x30 Sudden brake
latter bit	0x01: Chinese
	0x02: English

Examples:

No Alarm and Language is Chinese: 0x00 0x01

No Alarm and Language is English: 0x00 0x02

**To increase the reliability of alarm information, labeling the alarm information repeatedly; in most cases, the alarm information keeps consistent with information of former terminal, while the inconsistencies are as follows:**

- A. Low Battery Alarm occurred in the information of the terminal**
- B. Fence in and out Alarm in the Alarm/Language information**

### 5.3.1.18. Information Serial Number

For details see Data Packet Format section 4.5.

### 5.3.1.19. Error Check

For details see Data Packet Format section 4.6.

### 5.3.1.20. Stop Bit

For details see Data Packet Format section 4.7.

### 5.3.1.21. Examples

**Examples of terminal transmission**

78 78 25 16 0B 0B 0F 0E 24 1D CF 02 7A C8 87 0C 46 57 E6 00 14 02 09 01 CC 00 28 7D 00 1F 72 65 06 04 01 01 00 36 56 A4 0D 0A

**Explain**

<u>0x78 0x78</u>	<u>0x25</u>	<u>0x16</u>	<u>0x0B 0x0B 0x0F 0x0E 0x24 x01D</u>	<u>0xCF</u>	<u>0x02 0x7A 0xC8 0x87</u>			
Start Bit	Length	Protocol No.	Date Time	Quantity of GPS information satellites	Latitude			
<u>0x0C 0x46 0x57 0xE6</u>	<u>0x00</u>	<u>0x14 0x02</u>	<u>0x09</u>	<u>0x01 0xCC</u>	<u>0x00</u>	<u>0x28 0x7D</u>	<u>0x00 0x1F 0x72</u>	
Longitude	Speed	Course Status	LBS Length	MCC	MNC	LAC	Cell ID	
<u>0x65</u>	<u>0x06</u>	<u>0x04</u>	<u>0x01 0x01</u>	<u>0x00 0x36</u>	<u>0x56 0xA4</u>		<u>0x0D 0x0A</u>	
Terminal Information Content	Voltage Level	GSM Signal Strength	Alarm/Language	Serial No.	Error Check	Stop Bit		

Note: The status information in the data packet is the status corresponding to the time bit recorded in the data packet.

**5.3.2. Server responding alarm data packet to terminal (terminal do not check enforcedly)**

Format		Length(Byte)
Information Content	Start Bit	2
	Packet Length	1
	Protocol Number	1
	Serial Number	2
	Error Check	2
	Stop Bit	2

Alarm packet is consisted by adding status information to location packet, so does the encoding format of the protocol.

**5.3.2.1. Start Bit**

For details see Data Packet Format section 4.1

**5.3.2.2. Packet Length**

For details see Data Packet Format section 4.2

**5.3.2.3. Protocol Number**

For details see Data Packet Format section 4.3

**5.3.2.4. Serial Number**

For details see Data Packet Format section 4.5

**5.3.2.5. Error Check**

For details see Data Packet Format section 4.6

**5.3.2.6. Stop Bit**

For details see Data Packet Format section 4.7

**5.3.2.7. Examples**

**Example of data packet responded by the server**

78 78 05 16 00 36 95 70 0D 0A

**5.3.3. Server responding alarm data address packet to Terminal**

**5.3.3.1. Response package in Chinese**

The response data packet in Chinese is as follow:

Command packet sent from the server to the terminal (15+M+N Byte)	Start Bit		2	
	Length of data bit		1	
	Protocol Number		1	
	Information Content	Length of Command		1
		Server Flag Bit		4
		Command Content	ALARMSMS	8
			&&	2
			Address Content	M
			&&	2
			Phone Number	21
			##	2
	Information Serial Number		2	
	Check Bit		2	
	Stop Bit		2	

The Protocol Number of request Chinese address response is 0X17.

Command Content: ADDRESS&&Address Content&&Phone Number(All is 0)## (ADDRESS, &&, ## are fixed strings)

Chinese address content is sent in UNICODE.

**Example of Chinese address response information:**

```

7878 // Start Bit
85 // Data Length
17 // Response Protocol Number
7E // Length of Command, i.e., length of the information of the transmitted content
0000001 // Server Flag Bit
414C41524D534D53 //ALARMSMS
2626 //&& Separator
624059044F4D7F6E0028 // Chinese address is sent in UNICODE
004C004200530029003A
5E7F4E1C77015E7F5DDE
5E0282B190FD533AFF17
FF15FF144E6190530028
004E00320033002E0033
00390035002C00450031
    
```

```

00310032002E00390038
0038002996448FD1
2626| //&& Separator
000000000000000000000000000000000000 // Phone Number
2323| //## terminator of content
0106| // Serial No.
3825| // Check Bit
0D0A // Stop Bit

```

### 5.3.3.2. Response package in English

Considering the address or other foreign address in English is generally longer than that in Chinese, one data bit is not enough, so the data bit is occupied in 2 bytes.

Note: only the length of data bit corresponding to the protocol number of response address information is changed into two bytes.

Command packet sent from the server to the terminal (15+M+N Byte)	Start Bit		2	
	Length of data bit		2	
	Protocol Number		1	
	Information Content	Length of Command		2
		Server Flag Bit		4
		Command Content	ALARMSMS	8
			&&	2
			Address Content	M
			&&	2
			Phone Number	21
			##	2
	Information Serial Number		2	
Check Bit		2		
Stop Bit		2		

The Protocol Number of request English address response is 0X97.

Command Content: ADDRESS&&Address Content&&Phone Number(All is 0)##(ADDRESS, &&, ## are fixed strings)

#### Example of English address response information:

```

7878 // Start Bit
00D2 | // Data Length
97 // Response Protocol Number
00CA | // Length of Command, i.e., length of the information of the transmitted content
00000001| // Server Flag Bit

```

CONFIDENTIAL

414C41524D534D53 //ALARMSMS  
2626| //&& Separator  
0053004F00530028004C | // English address is sent in UNICODE  
0029003A005300680069  
006D0069006E00200046  
0061006900720079006C  
0061006E006400200057  
00650073007400200052  
0064002C004800750069  
006300680065006E0067  
002C004800750069007A  
0068006F0075002C0047  
00750061006E00670064  
006F006E00670028004E  
00320033002E00310031  
0031002C004500310031  
0034002E003400310031  
0029004E006500610072  
00620079  
2626| //&& Separator  
00 // Phone Number  
2323| //## terminator of content  
0007| //Serial No.  
72b5| // Check Bit  
0D0A // Stop Bit

**5.4. Heartbeat Packet (status information packet)**

Heartbeat packet is a data packet to maintain the connection between the terminal and the server.

**5.4.1. Terminal Sending Heartbeat Packet to Server**

Format		Length (Byte)	
Information Content	Start Bit	2	
	Packet Length	1	
	Protocol Number	1	
	Status Information	Terminal Information Content	1
		Voltage Level	1
		GSM Signal Strength	1
		Alarm/Language	2
	Serial Number	2	
	Error Check	2	
	Stop Bit	2	

**5.4.1.1. Start Bit**

For details see Data Packet Format section 4. 1.

**5.4.1.2. Packet Length**

For details see Data Packet Format section 4.2.

**5.4.1.3. Protocol Number**

For details see Data Packet Format section 4.3.

**5.4.1.4. Terminal Information**

One byte is consumed defining for various status information of the mobile phone.

Bit	Code Meaning
Bit7	1: oil and electricity disconnected
	0: gas oil and electricity
Bit6	1: GPS tracking is on
	0: GPS tracking is off
Bit3~ Bit5	100: SOS
	011: Low Battery Alarm
	010: Power Cut Alarm
	001: Shock Alarm
Bit2	000: Normal
	1: Charge On
Bit1	0: Charge Off
	1: ACC high
Bit0	0: ACC Low
	1: Defense Activated
	0: Defense Deactivated

Example: 0x44, corresponding binary value is 01000100, indicates that the status of the terminal is: oil and electricity connected, GPS tracking is on, normal without any alarm, charge on, ACC is low,

and defense deactivated.

**5.4.1.5. Voltage Level**

The range is 0~6 defining the voltage is from low to high.

0: No Power (shutdown)

1: Extremely Low Battery (not enough for calling or sending text messages, etc.)

2: Very Low Battery (Low Battery Alarm)

3: Low Battery (can be used normally)

4: Medium

5: High

6: Very High

Example: 0x02 indicates very low battery and a Low Battery Alarm is sending.

**5.4.1.6. GSM Signal Strength Levels**

0x00: no signal;

0x01: extremely weak signal;

0x02: very weak signal;

0x03: good signal;

0x04: strong signal.

Example: 0x03 indicates the GSM signal is good.

**5.4.1.7. Alarm/Language**

0x00 (former bit) 0x01 (latter bit)

former bit: terminal alarm status (suitable for alarm packet and electronic fence project)

latter bit: the current language of the terminal

former bit	
latter bit	0x01: Chinese
	0x02: English

Examples:

No Alarm and Language is Chinese: 0x00 0x01

No Alarm and Language is English: 0x00 0x02

**5.4.1.8. Information Serial Number**

For details see Data Packet Format section 4.5.

**5.4.1.9. Error Check**

For details see Data Packet Format section 4.6.

**5.4.1.10. Stop Bit**

For details see Data Packet Format section 4.7.

**5.4.2. Server Responds the Data Packet**

	Description	Bits	Example
Login Message Packet (18 Byte)	Start Bit	2	<u>0x78 0x78</u>
	Packet Length	1	<u>0x05</u>
	Protocol Number	1	<u>0x01</u>
	Information Serial Number	2	<u>0x00 0x01</u>
	Error Check	2	<u>0xD9 0xDC</u>
	Stop Bit	2	<u>0x0D 0x0A</u>

The response packet from the server to the terminal: the protocol number in the response packet is identical to the protocol number in the data packet sent by the terminal.

**5.4.2.1. Start Bit**

For details see Data Packet Format section 4. 1.

**5.4.2.2. Packet Length**

For details see Data Packet Format section 4.2.

**5.4.2.3. Protocol Number**

For details see Data Packet Format section 4.3.

**5.4.2.4. Information Serial Number**

For details see Data Packet Format section 4.5.

**5.4.2.5. Error Check**

For details see Data Packet Format section 4.6.

**5.4.2.6. Stop Bit**

For details see Data Packet Format section 4.7.

**5.4.3. Examples**

Example of data packet sent by the terminal

78 78 08 13 4B 04 03 00 01 00 11 06 1F 0D 0A

Explain

<u>0x78 0x78</u>	<u>0x08</u>	<u>0x13</u>	<u>0x4B 0x04 0x03</u>	<u>0x00 0x01</u>	0x00 0x11	0x06 0x1F	0x0D 0x0A
Start Bit	Length	Protocol No.	Information Content	Reserved bit (Language)	Serial No.	Error Check	Stop Bit

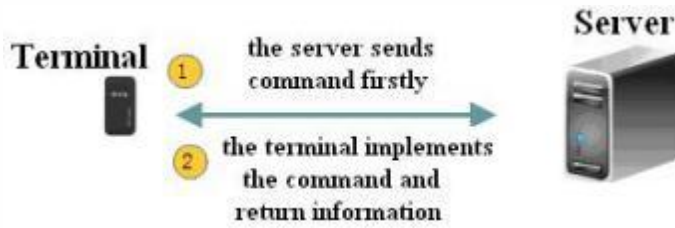
Example of response packet returned by the server

78 78 05 13 00 11 F9 70 0D 0A

Explain

<u>0x78 0x78</u>	<u>0x05</u>	<u>0x13</u>	<u>0x00 0x11</u>	<u>0xF9 0x70</u>	<u>0x0D 0x0A</u>
Start Bit	Length	Protocol No.	Serial No.	Error Check	Stop Bit

## VI. Data Packet Sent From Server to Terminal



### 6.1. Packet Sent by Server

Format		Length (Byte)
Start Bit		2
Packet length		1
Protocol Number		1
Information Content	Length of Command	1
	Server Flag Bit	4
	Command Content	M
Information Serial Number		2
Error Check		2
Stop Bit		2

#### 6.1.1. Start Bit

For details see Data Packet Format section 4. 1.

#### 6.1.2. Packet Length

For details see Data Packet Format section 4.2.

#### 6.1.3. Protocol Number

The Protocol Number of terminal transmission is 0x80.

#### 6.1.4. Length of Command

Server Flag Bit + Length of Command Content

Example: measured in bytes, 0x0A means the content of command occupied ten bytes.

#### 6.1.5. Server Flag Bit

It is reserved to the identification of the server. The binary data received by the terminal is returned without change.

#### 6.1.6. Command Content

It is represented in ASC II of string, and the command content is compatible with text message command.

#### 6.1.7. Information Serial Number

For details see Data Packet Format section 4.5.

#### 6.1.8. Error Check

For details see Data Packet Format section 4.6.

#### 6.1.9. Stop Bit

For details see Data Packet Format section 4.7.

### 6.2. Packet Replied by Terminal

Format		Length (Byte)
Start Bit		2
Packet Length		1
Protocol Number		1
Information Content	Length of Command	1
	Server Flag Bit	4
	Command Content	M
	Language	2
Information Serial Number		2
Error Check		2
Stop Bit		2

**6.2.1. Start Bit**

For details see Data Packet Format section 4. 1.

**6.2.2. Packet Length**

For details see Data Packet Format section 4.2.

**6.2.3. Protocol Number**

The terminal responds to the command sent by the server. The format of data packet is consistent with “the command sent by the server to the terminal”, but the Protocol Number herein is different and is 0x15.

**6.2.4. Length of Command**

Server Flag Bit + Length of Command Content

Example: measured in bytes, 0x0A means the content of command occupied ten bytes.

**6.2.5. Server Flag Bit**

It is reserved to the identification of the server. The binary data received by the terminal is returned without change.

**6.2.6. Command Content**

It is represented in ASC II of string, and the command content is compatible with text message command.

**6.2.7. Language**

A bit indicates the current language used in the terminal.

Chinese: 0x00 0x01

English: 0x00 0x02

**6.2.8. Information Serial Number**

For details see Data Packet Format section 4.5.

**6.2.9. Error Check**

For details see Data Packet Format section 4.6.

**6.2.10. Stop Bit**

For details see Data Packet Format section 4.7.

**6.3. Looking Up Location Information**

**Function Description:** the command to obtain the positioning information. A mobile phone user or a

short message server may obtain the positioning information by this command.

In an example, the transmitting and returning strings are converted into ASCII to generate command contents.

**Sending by the server**

DWXX#

**Returned by the terminal**

if successful, return

DWXX=Lat:<North/South Latitude>,Lon:<East/West Longitude>,Course:<angle>,Speed:<speed>,DateTime:<time>

if failed, return

DWXX=Command Error!

if tracking unsuccessful, return

DWXX=Lat:,Lon:, Course:,Speed:,DateTime:-:

Example:

DWXX=Lat:N23d5.1708m,Lon: E114d23.6212m,Course:120,Speed:53.02;DateTime:08-09-12 14:52:36

Explain: which means: N23d5.1708m, E114d23.6212m, Course: 120, Speed: 53.02km/h, Date Time: 08-09-12 14:52:36.

#### 6.4. Cutting Oil and Electricity

**Function Description:** cutting off the vehicle oil-electric control circuit

In an example, the transmitting and returning strings are converted into ASCII to generate command contents.

**Sending by the server**

RELAY,1 #

**Returned by the terminal**

if successful, return

reply: Cut off the fule supply:Success!

if failed, return

reply: Already in the state of fuel supply cut off, the command is not running!

Explain: the oil and electricity are not allowed to be disconnect when the GPS tracking is off or the running speed is higher than 20KM/H.

#### 6.5. Connecting Oil and Electricity

**Function Description:** connecting the vehicle oil-electric control circuit

In an example, the transmitting and returning strings are converted into ASCII to generate command contents.

**Sending by the server**

RELAY,0#

**Returned by the terminal**

if successful, return

reply: Restore fule supply: Success!

if failed, return

reply: Already in the state of fuel supply to resume, the command is not running!

#### 6.6. Address Querying Information Sent by the Server

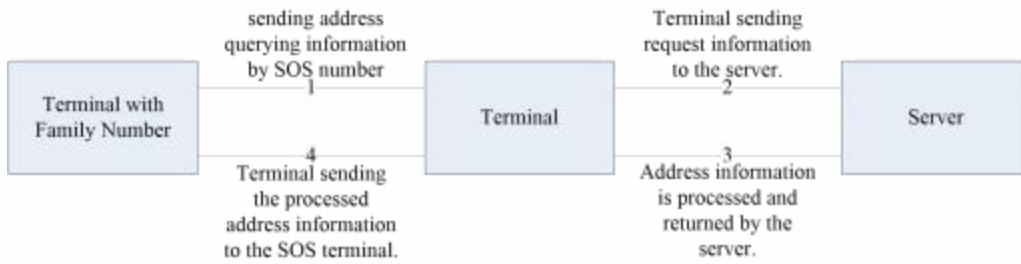
In an example, the transmitting and returning strings are converted into ASCII to generate command contents.

**Sending by the server**

ADDRESS, Address Content, Phone Number

Note: The address content in Chinese is sent in UNICODE.

## 6.7. GPS, Phone Number Querying Address Information Package (0X1A)



### 6.7.1. Information from Terminal to Server

The information is received by the terminal.

The format is basically same to the format mentioned as GPS information content, and the difference is that phone number for querying address is added here.

Format		Length (Byte)		
Start Bit		2		
Packet Length		1		
Protocol Number		1		
Information Content	Date Time		6	
	GPS Information	Length of GPS information, quantity of positioning satellites		1
		Latitude		4
		Longitude		4
		Speed		1
		Course, Status		2
	Phone Number		21	
	Language		2	
Information Serial Number		2		
Error Check		2		
Stop Bit		2		

#### 6.7.1.1. Start Bit

For details see Data Packet Format section 4.1.

#### 6.7.1.2. Packet Length

For details see Data Packet Format section 4.2.

Example: measured in bytes, 0x2E means the content of command occupied 46 bytes.

#### 6.7.1.3. Protocol Number

0x1A is utilized.

#### 6.7.1.4. Date Time

For details see Location Data Packet Format section 5.2.1.4.

#### 6.7.1.5. Length of GPS information, quantity of positioning satellites

For details see Location Data Packet Format section 5.2.1.5.

#### 6.7.1.6. Latitude

For details see Location Data Packet Format section 5.2.1.6.

#### 6.7.1.7. Longitude

For details see Location Data Packet Format section 5.2.1.7.

---

### 6.7.1.8. Speed

For details see Location Data Packet Format section 5.2.1.8.

### 6.7.1.9. Course

For details see Location Data Packet Format section 5.2.1.9.

### 6.7.1.10. Phone Number

The SOS phone number used for requesting address query, which is converted by ASCII and 0 is added at the right side if less than 21 bits.

### 6.7.1.11. Language

A bit indicates the current language used in the terminal.

Chinese: 0x00 0x01

English: 0x00 0x02

### 6.7.1.12. Information Serial Number

For details see Data Packet Format section 4.5.

### 6.7.1.13. Error Check

For details see Data Packet Format section 4.6.

### 6.7.1.14. Stop Bit

For details see Data Packet Format section 4.7.

## 6.7.2. Response of Server

The server replies Chinese address or English address based on the extended command, and the response data packet is inconsistent

### 6.7.2.1. Response package in Chinese

The response data packet in Chinese is as follow:

Command packet sent from the server to the terminal (15+M+N Byte)	Start Bit		2	
	Length of data bit		1	
	Protocol Number		1	
	Information Content	Command Content	Length of Command	1
			Server Flag Bit	4
			ADDRESS	7
			&&	2
			Address Content	M
			&&	2
			Phone Number	21
			##	2
	Information Serial Number		2	
	Check Bit		2	
Stop Bit		2		

The Protocol Number of request Chinese address response is 0X17.

Command Content: ADDRESS&&Address Content&&Phone Number## (ADDRESS, &&, ## are

fixed strings)

Chinese address content is sent in UNICODE.

**Example of Chinese address response information:**

```

7878|          //Start Bit
84          //Data Length
17          //Response Protocol Number
7E          //Length of Command, i.e., length of the information of the transmitted
content
00000001|          //Server Flag Bit
41444452455353 |          //ADDRESS
2626|          //&& Separator
624059044F4D7F6E0028 //Chinese address is sent in UNICODE
004C004200530029003A
5E7F4E1C77015E7F5DDE
5E0282B190FD533AFF17
FF15FF144E6190530028
004E00320033002E0033
00390035002C00450031
00310032002E00390038
0038002996448FD1
2626|          //&& Separator
313337313038313931333500000000000000000000 | //Phone Number
2323|          //## terminator of content
0106          //Serial No.
3825|          //Check Bit
0D0A          //Stop Bit
    
```

**6.7.2.2. Response package in English**

Considering the address or other foreign address in English is generally longer than that in Chinese, one data bit is not enough, so the data bit is occupied in 2 bytes.

Note: only the length of data bit corresponding to the protocol number of response address information is changed into two bytes.

Command packet sent from the server to the terminal (15+M+N Byte)	Start Bit		2	
	Length of data bit		2	
	Protocol Number		1	
	Information Content	Length of Command		2
		Server Flag Bit		4
		Command Content	ADDRESS	7
			&&	2
Address		M		

		Content	
		&&	2
		Phone Number	21
		##	2
	Information Serial Number		2
	Check Bit		2
	Stop Bit		2

The Protocol Number of request English address response is 0X97.

Command Content: ADDRESS&& Address Content&&Phone Number##( ADDRESS, &&, ## are fixed strings)

**Example of English address response information:**

```

7878| //Start Bit
00D1 | //Data Length
97 //Response Protocol Number
00CA | //Length of Command, i.e., length of the information of the transmitted content
00000001| //Server Flag Bit
41444452455353 //ADDRESS
2626| //&& Separator
0053004F00530028004C | //English address is sent in UNICODE
0029003A005300680069
006D0069006E00200046
0061006900720079006C
0061006E006400200057
00650073007400200052
0064002C004800750069
006300680065006E0067
002C004800750069007A
0068006F0075002C0047
00750061006E00670064
006F006E00670028004E
00320033002E00310031
0031002C004500310031
0034002E003400310031
0029004E006500610072
00620079
2626| //&& Separator
313235323031333739303737343035310000000000 | //Phone Number
2323| //## terminator of content
0007| // Serial No.
72b5| //Check Bit
0D0A //Stop Bit

```

## VII: Information Transfer Packet

### Description:

It is used to transmit all kinds of non-location data.

#### a) Information transfer packet (sent by terminal)

		Length	Details
Start Bit		2	0x79 0x79
Packet Length		2	Length = Protocol number + Information content + Information SN + CRC
Protocol Number		1	0x94
Information Content	Information type (sub-protocol No.)	1	00: 00: External battery voltage 01–03: Customized 04: Terminal status synchronization 05: Door status 08: Self-check parameters 09: Information of visible satellites 0A: ICCID information 1BRFID .....To be added
	Data content	N	Different content will be transmitted according to different information types. For details, see the table below.
Information SN		2	The SN will be automatically added by "1" for each data sending after power-on.
CRC		2	It is the CRC-ITU value from "Packet Length" to "Information SN". If the receiver receives a packet that contains a CRC error, it ignores the error and discards the packet (See Attachment 1 for algorithm details).
Stop Bit		2	It is fixed at 0x0D 0x0A.

#### Example data:

```
7979007F9404414C4D313D43343B414C4D323D43433B414C4D333D34433B535441313D
43303B4
459443D30313B534F533D2C2C3B43454E5445523D3B46454E43453D46656E63652C4F4
E2C302
C32332E3131313830392C3131342E3430393236342C3430302C494E206F72204F55542C3
03B4D4 946493D4D4946492C4F4646000A061E0D0A
```

#### Transferred information content

When the information type is "00", it carries the voltage of the external battery, which is a 2-bit hex. The hex is then converted into a decimal and further divided by 100.

Take "0x04,0x9F" for example, it is 1183 in decimal and is 11.83 after being divided by 100, which means the voltage of the external battery is 11.83V.

When the information type is "04", it carries the terminal status synchronization information and is of variable-length in ASCII coding.

#### Content IDs

Definition	ID
Alarm byte 1	ALM1
Alarm byte 2	ALM2
Alarm byte 3	ALM3
Alarm byte 4	ALM4
Status byte 1	STA1
SOS number	SOS
Center number	CENTER
Geofence	FENCE
Fuel/power cutoff status	DYD
Mode	MODE

◇ **ALM1 (status)**

Bit	Definition	Remarks
bit7	Vibrating alert	1: ON; 0: OFF
bit6	Alert via GPRS	1: ON; 0: OFF
bit5	Alert via call	1: ON; 0: OFF
bit4	Alert via SMS	1: ON; 0: OFF
bit3	Tow/theft alert	1: ON; 0: OFF
bit2	Alert via GPRS	1: ON; 0: OFF
bit1	Alert via call	1: ON; 0: OFF
bit0	Alert via SMS	1: ON; 0: OFF

◇ **ALM2 (status)**

Bit	Definition	Remarks
bit7	Low internal battery alert	1: ON; 0: OFF
bit6	Alert via GPRS	1: ON; 0: OFF
bit5	Alert via call	1: ON; 0: OFF
bit4	Alert via SMS	1: ON; 0: OFF
bit3	Low external battery alert	1: ON; 0: OFF
bit2	Alert via GPRS	1: ON; 0: OFF
bit1	Alert via call	1: ON; 0: OFF
bit0	Alert via SMS	1: ON; 0: OFF

◇ **ALM3 (status)**

Bit	Definition	Remarks
bit7	Speed alert	1: ON; 0: OFF
bit6	Alert via GPRS	1: ON; 0: OFF
bit5	Alert via call	1: ON; 0: OFF
bit4	Alert via SMS	1: ON; 0: OFF
bit3	Power cut alert	1: ON; 0: OFF
bit2	Alert via GPRS	1: ON; 0: OFF
bit1	Alert via call	1: ON; 0: OFF

bit0	Alert via SMS	1: ON; 0: OFF
------	---------------	---------------

◇ **ALM4 (status)**

Bit	Definition	Remarks
bit7	SOS alert	1: ON; 0: OFF
bit6	Alert via GPRS	1: ON; 0: OFF
bit5	Alert via call	1: ON; 0: OFF
bit4	Alert via SMS	1: ON; 0: OFF
bit3	Voice control alert	1: ON; 0: OFF
bit2	Alert via GPRS	1: ON; 0: OFF
bit1	Alert via call	1: ON; 0: OFF
bit0	Alert via SMS	1: ON; 0: OFF

◇ **STA1 (status)**

Bit	Definition	Remarks
bit7	Defense status	1: Defense on; 0: Defense off
bit6	Auto defense	1: ON; 0: OFF
bit5	Manual defense	1: ON; 0: OFF
bit4	Remote cancellation of defense	1: ON; 0: OFF
bit3	To be defined	
bit2	To be defined	
bit1	Tamper switch	1: Close; 0: Open
bit0	Tamper alert	1: ON; 0: OFF

◇ **Fuel/power cutoff status**

Bit	Definition	Remarks
bit7	Undefined	
bit6	Undefined	
bit5	Undefined	
bit4	Undefined	
bit3	Delay execution because the speed is too high	1: Valid; 0: Invalid
bit2	Delay execution because the terminal is not positioned	1: Valid; 0: Invalid
bit1	Cut fuel/power	1: Valid; 0: Invalid
bit0	Connect fuel/power	1: Valid; 0: Invalid

◇ **SOS: It transmits in ASCII coding (multiple SOS numbers are separated by commas [,]).**

- ✧ **Center number:** It transmits in ASCII coding.
- ✧ **Geofence:** It transmits in ASCII coding.
- ✧ **Mode:** It transmits in ASCII coding (parameters are separated by commas [,]).

**Example:**

**ALM1=FF;ALM2=FF;ALM3=FF;STA1=CO;DYD=01;SOS=12345,2345,5678;CENTER=987654; FENCE=FENCE,ON,0,-22.277120,-113.516763,5,IN,1; MODE=MODE,1,20,500**

**Note: Not all of the content will be transmitted. The platform can parse according to bits. The content uploaded varies with products.**

**When the information type is "05", it carries the detection (door detection) status of the external I/O in hex.**

Bit	Definition	Remarks
bit7	TBD	
bit6	TBD	
bit5	TBD	
bit4	TBD	
bit3	TBD	
bit2	I/O port status	1: High; 0: Low
bit1	Trigger status	1: Level high; 0: Level low
bit0	Door status	1: ON; 0: OFF

**When the information type is "09", it carries the GPS status of the terminal in hex.**

GPS module status	1	0x00: No such feature; 0x01: Satellite searching; 0x02: 2D positioning; 0x03: 3D positioning; 0x04: Sleeping
Number of satellites engaged in position fix	1	Based on this the number of transmission strength is determined.
GPS1 strength	1	Strength of GPS location satellite 1
GPS2 strength	1	Strength of visible satellite 2
.....		
Number of GPS satellites that are visible but not engaged in position fix	1	Based on this the number of transmission strength is determined.
Visible GPS1 Strength	1	Strength of visible satellite 1
Visible GPS2 strength	1	Strength of visible satellite 2
.....		
BDS module status	1	0x00: No such feature; 0x01: Satellite searching; 0x02: 2D positioning; 0x03: 3D positioning; 0x04: Sleeping
Number of BDS satellites engaged in position fix	1	This is the basis for determining the volume of satellite signal strength.
BDS1 strength	1	Strength of BDS location satellite 1
BDS2 strength	1	Strength of BDS location satellite 2
.....		



---

When the information type is "12", it carries the STRELA Sensor(BLE) information in hex.

<b>STRELA Sensor(BLE)</b>	4	Example: 0x008f061d 0x8f means percentage (bit0-bit6 is percentage) 0x06 means temperature and the value is 6°C 0x1d means battery and the value is 2.9V (0x1d=29 battery=29/10=2.9V)
---------------------------	---	--

When the information type is "13", it carries the STRELA Sensor(RS485) information in hex.

<b>STRELA Sensor(RS485)</b>	5	Example: 0x0102d51e00 0x02d5 means N and the value is 725 0x1e means temperature and the value is 30°C
-----------------------------	---	--

b) Return packet (from server)

No response is required from the server.

CONFIDENTIAL

**VIII . Appendix A: code fragment of the CRC-ITU lookup table algorithm implemented based on C language**

Code fragment of the CRC-ITU lookup table algorithm implemented based on C language is as follow:

```
static const U16 crctab16[] =
{
    0X0000, 0X1189, 0X2312, 0X329B, 0X4624, 0X57AD, 0X6536, 0X74BF,
    0X8C48, 0X9DC1, 0XAF5A, 0XBED3, 0XCA6C, 0XD8E5, 0XE97E, 0XF8F7,
    0X1081, 0X0108, 0X3393, 0X221A, 0X56A5, 0X472C, 0X75B7, 0X643E,
    0X9CC9, 0X8D40, 0XBFDB, 0XAE52, 0XDAED, 0XCB64, 0XF9FF, 0XE876,
    0X2102, 0X308B, 0X0210, 0X1399, 0X6726, 0X76AF, 0X4434, 0X55BD,
    0XAD4A, 0XBCC3, 0X8E58, 0X9FD1, 0XEB6E, 0XFAE7, 0XC87C, 0XD9F5,
    0X3183, 0X200A, 0X1291, 0X0318, 0X77A7, 0X662E, 0X54B5, 0X453C,
    0XBDCB, 0XAC42, 0X9ED9, 0X8F50, 0XFBEF, 0XEA66, 0XD8FD, 0XC974,
    0X4204, 0X538D, 0X6116, 0X709F, 0X0420, 0X15A9, 0X2732, 0X36BB,
    0XCE4C, 0XD5C5, 0XED5E, 0XFC77, 0X8868, 0X99E1, 0XAB7A, 0XBAF3,
    0X5285, 0X430C, 0X7197, 0X601E, 0X14A1, 0X0528, 0X37B3, 0X263A,
    0XD6CD, 0XCF44, 0XFDDF, 0XEC56, 0X98E9, 0X8960, 0XBBFB, 0XAA72,
    0X6306, 0X728F, 0X4014, 0X519D, 0X2522, 0X34AB, 0X0630, 0X17B9,
    0XEF4E, 0XFEC7, 0XCC5C, 0XDDD5, 0XA96A, 0XB8E3, 0X8A78, 0X9BF1,
    0X7387, 0X620E, 0X5095, 0X411C, 0X35A3, 0X242A, 0X16B1, 0X0738,
    0XFFCF, 0XEE46, 0XDCDD, 0XCD54, 0XB9EB, 0XA862, 0X9AF9, 0X8B70,
    0X8408, 0X9581, 0XA71A, 0XB693, 0XC22C, 0XD3A5, 0XE13E, 0XF0B7,
    0X0840, 0X19C9, 0X2B52, 0X3ADB, 0X4E64, 0X5FED, 0X6D76, 0X7CFF,
    0X9489, 0X8500, 0XB79B, 0XA612, 0XD2AD, 0XC324, 0XF1BF, 0XE036,
    0X18C1, 0X0948, 0X3BD3, 0X2A5A, 0X5EE5, 0X4F6C, 0X7DF7, 0X6C7E,
    0XA50A, 0XB483, 0X8618, 0X9791, 0XE32E, 0XF2A7, 0XC03C, 0XD1B5,
    0X2942, 0X38CB, 0X0A50, 0X1BD9, 0X6F66, 0X7EEF, 0X4C74, 0X5DFD,
    0XB58B, 0XA402, 0X9699, 0X8710, 0XF3AF, 0XE226, 0XD0BD, 0XC134,
    0X39C3, 0X284A, 0X1AD1, 0X0B58, 0X7FE7, 0X6E6E, 0X5CF5, 0X4D7C,
    0XC60C, 0XD785, 0XE51E, 0XF497, 0X8028, 0X91A1, 0XA33A, 0XB2B3,
    0X4A44, 0X5BCD, 0X6956, 0X78DF, 0X0C60, 0X1DE9, 0X2F72, 0X3EFB,
    0XD68D, 0XC704, 0XF59F, 0XE416, 0X90A9, 0X8120, 0XB3BB, 0XA232,
    0X5AC5, 0X4B4C, 0X79D7, 0X685E, 0X1CE1, 0X0D68, 0X3FF3, 0X2E7A,
    0XE70E, 0XF687, 0XC41C, 0XD595, 0XA12A, 0XB0A3, 0X8238, 0X93B1,
    0X6B46, 0X7ACF, 0X4854, 0X59DD, 0X2D62, 0X3CEB, 0X0E70, 0X1FF9,
    0XF78F, 0XE606, 0XD49D, 0XC514, 0XB1AB, 0XA022, 0X92B9, 0X8330,
    0X7BC7, 0X6A4E, 0X58D5, 0X495C, 0X3DE3, 0X2C6A, 0X1EF1, 0X0F78,
};

// calculate the 16-bit CRC of data with predetermined length.
U16 GetCrc16(const U8* pData, int nLength)
{
    U16 fcs = 0xffff;           // initialization
    while(nLength>0){
        fcs = (fcs >> 8) ^ crctab16[(fcs ^ *pData) & 0xff];
        nLength--;
        pData++;
    }
    return ~fcs;               // negated
}
```

---

## **IX. Appendix B: a fragment of example of data packet of communication protocol**

The following data displayed in hexadecimal are intercepted from the communication between a terminal and a server, wherein transmission means sending by the terminal and reception means returned from the server:

Login packet:

transmission: 78 78 0D 01 03 53 41 35 32 15 03 62 00 02 2D 06 0D 0A

reception: 78 78 05 01 00 02 EB 47 0D 0A

GPS data packet (06 adopts combined information package of GPS and LBS):

transmission: 78 78 1F 12 0B 08 1D 11 2E 10 CF 02 7A C7 EB 0C 46 58 49 00 14 8F 01 CC 00 28  
7D 00 1F B8 00 03 80 81 0D 0A

**Status packet:**

transmission: 78 78 0A 13 44 01 04 00 01 00 05 08 45 0D 0A

reception: 78 78 05 13 00 05 AF D5 0D 0A

**disconnect oil and electricity online:**

reception: 78 78 12 80 0C 00 11 42 78 52 45 4C 41 59 2C 31 23 00 00 D2 02 0D 0A

transmission: 78 78 2D 15 25 00 11 42 78 43 75 74 20 6F 66 66 20 74 68 65 20 66 75 65 6C 20 73 75 70  
70 6C 79 3A 20 53 75 63 63 65 73 73 21 00 02 00 15 90 3B 0D 0A

the server sending: RELAY,1#

reply: Cut off the fuel supply:Success!

Command sent during disconnection of oil and electricity:

reception: 78 78 12 80 0C 00 11 42 79 52 45 4C 41 59 2C 31 23 00 00 87 93 0D 0A

transmission: 78 78 54 15 4C 00 11 42 79 41 6C 72 65 61 64 79 20 69 6E 20 74 68 65 20 73 74 61 74 65  
20 6F 66 20 66 75 65 6C 20 73 75 70 70 6C 79 20 63 75 74 20 6F 66 66 2C 20 74 68 65 20 63 6F 6D 6D  
61 6E 64 20 69 73 20 6E 6F 74 20 72 75 6E 6E 69 6E 67 21 00 02 00 1A 05 54 0D 0A

the server sending :RELAY,1#

reply: Already in the state of fuel supply cut off, the command is not running!

**Connect oil and electricity online:**

reception: 78 78 12 80 0C 00 11 42 80 52 45 4C 41 59 2C 30 23 00 00 BE C2 0D 0A

transmission: 78 78 29 15 21 00 11 42 80 52 65 73 74 6F 72 65 20 66 75 65 6C 20 73 75 70 70 6C 79 3A  
20 53 75 63 63 65 73 73 21 00 02 00 1C 26 D2 0D 0A

the server sending: RELAY,0#

reply: Restore fuel supply: Success!

Command sent during connection of oil and electricity:

reception: 78 78 12 80 0C 00 11 42 81 52 45 4C 41 59 2C 30 23 00 00 EB 53 0D 0A

transmission: 78 78 56 15 4E 00 11 42 81 41 6C 72 65 61 64 79 20 69 6E 20 74 68 65 20 73 74 61 74 65  
20 6F 66 20 66 75 65 6C 20 73 75 70 70 6C 79 20 74 6F 20 72 65 73 75 6D 65 2C 20 74 68 65 20 63 6F  
6D 6D 61 6E 64 20 69 73 20 6E 6F 74 20 72 75 6E 6E 69 6E 67 21 00 02 00 20 06 74 0D 0A

the server sending: RELAY,0#

reply: Already in the state of fuel supply to resume, the command is not running!

**Querying address information online:**

reception: 78 78 16 80 10 00 01 A9 67 44 57 58 58 2C 30 30 30 30 30 23 00 A0 06 2D 0D 0A

transmission: 78 78 64 15 5C 00 01 A9 67 44 57 58 58 3D 4C 61 74 3A 4E 32 33 2E 31 31 31 36 38 32  
2C 4C 6F 6E 3A 45 31 31 34 2E 34 30 39 32 31 37 2C 43 6F 75 72 73 65 3A 30 2E 30 30 2C 53 70 65 65  
64 3A 30 2E 33 35 31 38 2C 44 61 74 65 54 69 6D 65 3A 31 31 2D 31 31 2D 31 35 20 20 31 31 3A 35 33



away from ATM machine of Bank of China, about 31 meters away from Jiangbei branch of of Bank of China, 11-11-15 14:36:29.

The specific meanings of the above commands can be looked up in the protocol document.

**CONFIDENTIAL**

**. Appendix C: Complete Format of the Information Package A.**

data packet sent by the terminal to the server

Login Message Packet (18 Byte)							
Start Bit	Packet length	Protocol Number	Terminal ID	Information	Serial Number	Check Bit	Stop Bit
2	1	1	8		2	2	2

GPS Information Package (26+N Byte)													
Start Bit	Packet length	Protocol Number	Information Content								Information serial number	check bit	stop bit
			GPS Information							Reserved extended bit			
			Date Time	Length of GPS information, quantity of positioning satellites	Latitude	Longitude	Speed	Course, Status					
2	1	1	6	1	4	4	1	2	N	2	2	2	

LBS information package (23+N Byte)													
Start Bit	Packet length	Protocol Number	Information Content							Reserved extended bit	Information serial number	check bit	stop bit
			LBS Information				Reserved extended bit						
			Date Time	MCC	MNC	LAC		Cell ID					
2	1	1	6	2	1	2	3	N	2	2	2		

LBS complete information package (42+N Byte)																						
Start Bit	Packet length	Protocol Number	Information Content															Reserved extended bit	Information serial number	check bit	stop bit	
			LBS Information																			
			Date Time	MCC	MNC	LAC	MCI	MCISS	NIC1	NIC2	NIC3	NIC4	NIC5	NIC6	NIC7	NIC8						
2	1	1	6	2	1	2	2	1	2	1	2	1	2	1	2	1	2	1	N	2	2	2

GPS、LBS information package (34+M+N Byte)																		
Start Bit	Packet length	Protocol Number	Information Content												Reserved and extended	Information serial number	check bit	stop bit
			GPS Information							LBS Information								
			Date Time	Length of GPS information, quantity of positioning satellites	Latitude	Longitude	Speed	Course, Status	Reserved extended bit	MCC	MNC	LAC	Cell ID					
2	1	1	6	1	4	4	1	2	M	2	1	2	3	M	2	2	2	

Status Packet(13+N Byte)									
Start Bit	Packet Length	Protocol Number	Information Content				Information Serial Number	Check Bit	Stop Bit
			Terminal Information Content	Voltage Level	GSM Signal Strength Level	Reserved and Extended			

t B i t						Bit (language)			
2	1	1	1	1	1	2	2	2	2

SNR information of satellite (11+M+N Byte)											
Start Bit	Packet Length	Protocol Number	Information Content						Information Serial Number	Check Bit	Stop Bit
			Quantity of positioning satellites	SNR of Satellite				Reserved and Extended Bit			
				1	2	3	.....				
2	1	1	1	M				N	2	2	2

terminal responds to the command sent by server (15+M+N Byte)										
Start Bit	Packet Length	Protocol Number	String Content				Reserved and Extended Bit (language)	Information Serial Number	Check Bit	Stop Bit
			Length of Command	Server Flag Bit	Command Content					
2	1	1	1	4	M	2	2	2	2	

GPS, LBS, Status Information Package (40+M+N+L Byte)																						
Start Bit	Packet Length	Protocol Number	Date Time	Information Content														Reserved and Extended Bit (language)	Information Serial Number	Check Bit	Stop Bit	
				GPS Information						LBS Information					Status Information							
				Length of GPS information, quantity of positioning satellites	Latitude	Longitude	Speed	Course, Status	Reserved and Extended Bit	LBS Length	MCC	MNC	LAC	Cell ID	Reserved and Extended Bit	Terminal Information Content	Voltage Level					GSM Signal Strength Level
2	1	1	6	1	4	4	1	2	M	1	2	1	2	3	N	1	1	1	2	2	2	2

### B. Data Packet Sent by Server to Terminal

Response of Server after receiving Status Packet from Terminal (10 Bytes)					
Start Bit	Packet Length	Protocol Number	Information Serial Number	Check Bit	Stop Bit
2	1	1	2	2	2

Command Packet Sent by Server to Terminal (15+M+N Byte)									
Start Bit	Packet Length	Protocol Number	Information Content				Information Serial Number	Check Bit	Stop Bit
			Length of Command	Server Flag Bit	Command Content	Reserved extended bit			
2	1	1	1	4	M	N	2	2	2