PAX Unified Transport Protocol

V 1.00.03

www.pax.com.cn

Copyright © 2000-2021 PAX Computer Technology (Shenzhen) Co., Ltd.

The information contained in this document is subject to change without notice. Although PAX Computer Technology (Shenzhen) Co., Ltd. has attempted to ensure the accuracy of the contents of this document, this document may include errors or omissions. The examples and sample programs are for illustration only and may not be suited for your purpose. You should verify the applicability of any example or sample program before placing the software into productive use.

Revision History

Date	Version	Note	Author
20/05/2015	1.00.00	First edition	Tu qinkui
30/05/2018	1.00.01	1、add charpter 2.1.5 2、add charpter 2.1.6 3、add charpter 3.1	Huang wuping
16/01/2020	1.00.02	1、rearrange the document 2、add charpter 4.2 3、add charpter 4.3 4、add charpter 5	Huang wuping
29/10/2020	1.00.03	Perfect description	Zhang yuan

Contents

1 Overview

1.1 Purpose

This document is used to unify the transport protocol format, transfer headers, validation, and transfer end flag. The purpose is to ensure that the application layer can receive and receive data stably.

1.2 Applicable platform

The protocol format described in this document is platform independent and communication mode independent. Applicable to all platforms and any communication mode

1.3 Readers

All programmers and customer groups who need to use protocols to secure data transfer.

1.4 Document conventions

NOTE

Used for labeling common notes.

CAUTION

Used for reminding the audience some place may have to pay attention to, which may lead to exceptions or errors.

WARNING

Used for reminding the audience some place may have to pay attention to, which may lead to exceptions or errors.

2 Message format description

2.1 Frame Message format

The basic functions of the system are used to control the POS master system. Such as clock, buzzer, product version management and other general control functions.

2.1.1 Confirmation frame

2.1.1.1 ACK frame

Send an ACK frame when the LRC check is correct.

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
0x02	0x01	0x00,0x00				0x00,0x01		0X06	LRC	0x03

2.1.1.2 NAK frame

Send an NAK frame when the LRC check is incorrect.

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
0x02	0x01	0x00,0x00				0x00,0x01		0X15	LRC	0x03

2.1.2 Sync/Handshake frame

The sender		The receiver
Synchronize request frame	→→	
	→→	Synchronize response frame

2.1.2.1 Request frame

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
0x02	0x01	0x00,0x01		0x00，0x01		0x00,0x00		null	LRC	0x03

2.1.2.2 Request frame

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
0x02	0x01	0x00,0x01		0x00，0x01		0x00,0x08		PaSize+ FrSize	LRC	0x03

PaSize: The maximum length of packet supported by client device, 4 bytes, large end.

FrSize: The maximum length of frame supported by client device, 4 bytes, large end.

2.1.3 Out-of-step frame

The out-of-step frame can be used to synchronize again to achieve the requirement of complete communication synchronization. The specific process is as follows: when client device detects the out-of-step signal, drop the request message and respond to the out-of-step frame directly.

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
0x02	0x01	0x00,0x02		0x00，0x01		0x00,0x00		null	LRC	0x03

2.1.4 Data frame

Package number greater than or equal to 1000 indicates that the transmission is data. Application layer use packet number and frame number flexibly, which can be applied to synchronization and multi-task scenarios, and different strategies can be achieved. This document provides a fully synchronized policy (optional). Please refer to charpter 4.1.

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
The starting character is fixed to 0x02	Packet version number currently fixed at 0x01	PaNoH=PaNo/258 PaNoL=PaNo%256 Start from 1000.		Start from 1, PaNoH=PaNo/258 PaNoL=PaNo%256					LRC check value of all data from STX	End character: 0x03 endS frame 0x17 has subsequent frames

The packet serial number is fixed at 1000 when the version number is 0x01.

For following different version numbers, the packet number may need to be increased automatically.

2.1.5 Report frame

To escalate the current states during the process of the request, client device can use the escalation frame to escalate or use the data frame to design the corresponding report state (instruction).

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
0x02	0x01	0x00,0x03		0x00，0x01					LRC	0x03

2.1.6 Cancel frame

Master device can initiate a cancel frame when master device initiates a time-

consuming request and client device has already carried out the cycle waiting operation, cancel frame does not need to go back to ACK. Client device monitors whether the cancel frame is received in the cycle, so as to exit the cycle waiting state (such as the cycle detection card can be cancelled by ECR operator), and the operator decides whether to cancel, and finally returns to the final state.

STX	Ver.	Packet series number （PaNo）		Frame series number （FrNo）		Data field length Len		Data field	LRC	ETX
		PaNoH	PaNoL	FrNoH	FrNoL	LenH	LenL			
0x02	0x01	0x00,0x4		0x00，0x01		0x00,0x00		null	LRC	0x03

3 Communication mode description

3.1 Applicable scenario description

1. It is suitable for master device and client device to adopt the communication mode of one receiving and one sending. Master device sends the request message, client device receives and processes the command, and then sends the response message.
2. It is suitable for master device to initiate a request, and client device can report various processing states (send a report frame) in the process of processing, and then send the send response message after processing.
3. Time consuming request, after receiving the cancel frame sent by master device, client device cancels the current request and responds to the corresponding time consuming request.
4. When client device executes time-consuming operations, master device can actively inquire the status.

When a request message and a response message are transmitting, the receiver sends back a confirmation frame which includes a receive frame (ACK) or a reject frame (NAK) after the sender sends a command data frame. The ACK frame indicates that the receiver confirms receipt of the message while the NAK frame indicates an error. The sender needs to resend after receiving a reject frame (NAK)

Multiple frames can be transferred when the length of the transmitted data exceeds the maximum limit of one frame. The protocol end of the frame indicats there are subsequent frames when it's set to 0x17.

The receiver replies a response message and returns the execution result after processing the command.

3.2 Communication mode

3.2.1 Single frame mode

The sender(upper computer)		The receiver(client device)
Request message	→→→	
	←←←	ACK
	←←←	Response message
ACK	→→→	

3.2.2 Multi-frame mode

The sender(upper computer)		The receiver(client device)
Request message 1st frame	→→→	
	←←←	ACK
Request message 2nd frame	→→→	
	←←←	ACK
Request message nth frame	→→→	
	←←←	ACK
	←←←	Response message 1st frame
ACK	→→→	
	←←←	Response message 2nd frame
ACK	→→→	
	←←←	Response message nth frame
ACK	→→→	

4 Policy description

4.1 Policy (optional)

In addition to a unified message format, this protocol also defines a set of related policies (optional), including retransmission mechanism, synchronous sending and receiving policy, and subcontracting rules. Based on the message format above, the application layer can also customize policies.

The policies in this protocol can be divided into: retransmission, out-of-step processing convention and subcontracting rules.

4.1.1 Retransmission

1. Retransmission includes timeout retransmission and NAK retransmission. The sender will retransmit the frame if the confirmation frame (ACK) is not received within the timeout specified by both sides. (Timeout time can be flexibly adjusted by the application layer according to machine performance and communication mode.)

2. The sender will retransmit the frame if NAK frame is received.

The receiver will drop the data packet if a retransmission frame, a data packet whose FrNo is 1 less than currently expected, is received. If the retransmission still fails, an error is returned to the calling layer. The chance of retransmissions specified in this protocol is 3.

4.1.2 Out-of-step processing convention

Out-of-step includes the following two scenarios:

1. For an upper computer, if the packet serial number of the reponse packet is different from the request's. (Note: The packet serial number is fixed at 1000 when the version number is 0x01.)

2. For client device, if the request packet serial number is not equal to the current expected (note: The packet serial number is fixed at 1000 when the version number is 0x01) or the frame number is neither equal to nor 1 less than the current expected value.

Taking master device as the main body to control the out-of-step processing
Master device processing is below:
1）Master device will send synchronization request packet to client device when detects out-of-step, and then client device will reset (synchronous) the packet serial number and respond to the frame size and packet size
2）Master device resends the whole packet;

Client device processing is below:
1）Client device responds to the out-of-step frame directly when detects the out-of-step.

4.1.3 Package size and subcontracting rules

Factors affecting subpackage and framing:

1. Machine hardware limitations, such as memory;
2. Communication modes, the buffer size of different communication modes is different.

The packet size and subcontractingn rules (the frame size) pass the synchronization frame, and client device informs master device.
The subpacket size is subject to the maximum frame value of client device. The PAX POS USB buffer is 8K, so the frame size cannot be larger than 8K. The PAX Bluetooth buffer size is 1000 bytes, so when using bluetooth, the frame size cannot exceed 1000 bytes.
The packet size is related to the available memory, depending on the situation. A pre negotiated definition needs to be applied.

4.2 Analysis of advantages and disadvantages of this policy

Advantages:
1. It is suitable for scenarios requiring complete synchronization of sending and receiving;

2. With a retransmission policy, the application layer does not need to relate to too many plicies.
3. Two control frames (report frame and cancel frame) are defined under the one receiving one sending policy, which can be used for uploading state and canceling time-consuming operations without losing step. If the data frame is used as the carrier to define the reporting and canceling instruction set, it will lead to out-of-step.

Disadvantages:
1. With some limitations, ti's not flexible enough;
2. The policy is too complex and overall performance is average;
3. Only one instruction request of application layer can be supported. Only when the instruction returns, the next instruction could be initiated. That is to say, client device does not support master device to send query instructions again when processing time-consuming requests

4.3 Application layer custom policies

Since the policies formulated in this protocol may not suit the using scenario, users can customize the strategy or not which is simpler and more efficient based on consideration of flexibility and efficiency. It should be noted that the upper and client devices need to use the same policy. Add a description, if the policy is defined.

5 Security

The goal of this document is to unify the message format and does not involve security. Refer to the following hierarchy if encryption is required for secure transmission.