

ProgrammerSought



Siemens PLC protocol-S7COMM-extended

tags: [plc](#) [S7](#) [java](#) [Internet of Things](#) [The internet](#)

Siemens PLC protocol-S7COMM-extended

Article Directory

[Siemens PLC protocol-S7COMM-extended](#)

[S7 Communication structure](#)

[TPKT protocol](#)

[structure](#)

[For example](#)

[COTP protocol](#)

[Introduction](#)

COTP connection package

For example

COTP function package

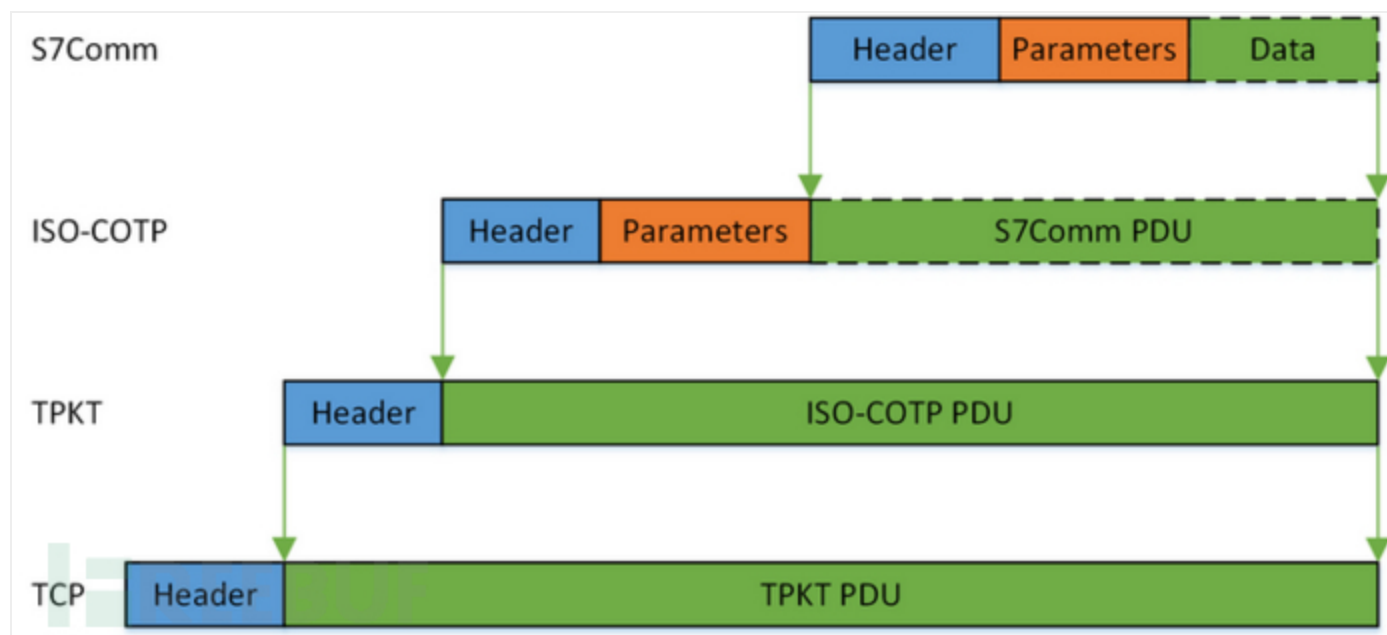
For example

At last

I wrote the PDU in S7 in detail before, but S7 Communication is encapsulated in the TPKT and SO-COTP protocols, then S7 Communication needs at least the following components:

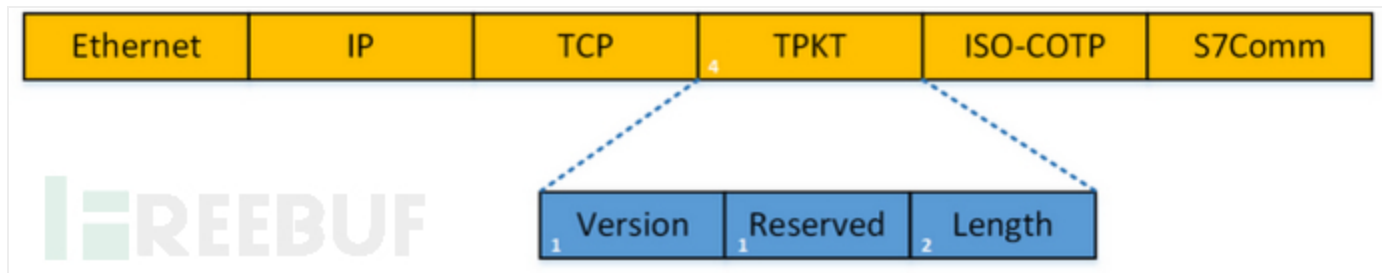
- COTP: ISO 8073 COTP connection-oriented transmission protocol.
- TPKT: Application layer data transmission protocol, between TCP and COTP protocol. The transport layer protocol is mainly used to build a bridge between COTP and TCP.
- TCP: Protocol data unit, TCP payload sends content.

S7 Communication structure



TPKT protocol

structure



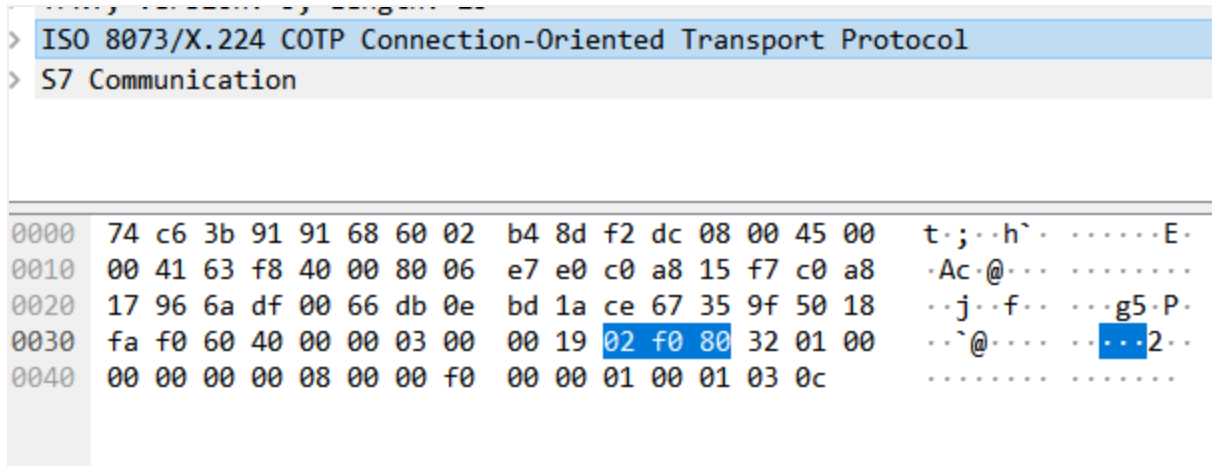
- Version: 1byte, version number
- Reserved: 1byte, reserved word
- Length: 2byte, length, the total length of the PDU of TPKT, COTP, and S7, which can also be said to be the length of the TCP payload

For example

>	TPKT, Version: 3, Length: 25																
>	ISO 8073/X.224 COTP Connection-Oriented Transport Protocol																
>	S7 Communication																
0000	74	c6	3b	91	91	68	60	02	b4	8d	f2	dc	08	00	45	00	t ; . h ` E .
0010	00	41	63	f8	40	00	80	06	e7	e0	c0	a8	15	f7	c0	a8	. Ac . @
0020	17	96	6a	df	00	66	db	0e	bd	1a	ce	67	35	9f	50	18	. . j . . f g5 . P .
0030	fa	f0	60	40	00	00	03	00	00	19	02	f0	80	32	01	00	. . ` @ 2 . .
0040	00	00	00	00	08	00	00	f0	00	00	01	00	01	03	0c	

TPKT protocol with version bit 3 and length bit 25 (0x0019)

COTP protocol



Introduction

COTP (ISO 8073/X.224 COTP Connection-Oriented Transport Protocol) is a protocol on top of TCP defined by the OSI 7-layer protocol. COTP uses "Packet" as the basic unit to transmit data, so that the receiver will get data with the same boundary as the sender. **(Extract online definition)**

structure

COTP protocol has two forms

- COTP Connection Packet: COTP connection packet
- COTP Function Packet: COTP function packet

COTP connection package

- Length: (1byte) length, COTP protocol length, excluding COTP subsequent data length, nor Length length, generally 17 bytes.
- Type: (1byte) type

code	description	description
0x01	ED Expedited Data	Urgent data
0x02	EA Expedited Data Acknowledgement	Urgent data confirmation
0x04	UD	User data
0x05	RJ Reject	Refuse

code	description	description
0x06	AK Data Acknowledgement	Data confirmation
0x07	ER TPDU Error	TPDU error
0x08	DR Disconnect Request	Disconnect request
0xC0	DC Disconnect Confirm	Disconnect confirmation
0xD0	CC Connect Confirm	Connection confirmation
0xE0	CR Connect Request	Connection request
0xF0	DT Data	data transmission

- DST Ref: (2bytes) target associated value
- SRC Ref: (2bytes) source associated value
- Opt: (1byte)
- Parameters: parameter value
 - code: number
 - length: length
 - Data: Data content

For example

```

1 | 11
2 | E0
3 | 00 00
4 | 00 01
5 | 00
6 | C1 02 01 00
7 | C2 02 01 02
8 | C0 01 09

```

What are opt and parameters? I won't go into further details here.

COTP function package

The function package is relatively simple, only the length type and

For example

1	02
2	F0
3	80

At last

No matter if it is TPKT, except for the change of data length, the other contents are unchanged, and the COTP protocol is basically unchanged, and it can be hard-coded when writing code.

Therefore, the problem of why the S7 protocol cannot be directly initiated directly using Netty is solved, and only the TPKT protocol and the COTP protocol need to be encapsulated.

[Copyright Complaint](#) [Spam Report](#)



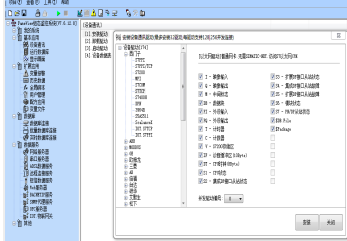
Powered By **VDO.AI**

Zabbix disk performance monitoring

Intelligent Recommendation

Python communicates with Siemens PLC

Install Python-snap7 Open "Run" with win+R, enter cmd, after confirming, enter the DOS command line terminal, enter the following command: pip install python-snap7 areas = ADict({ 'PE&...

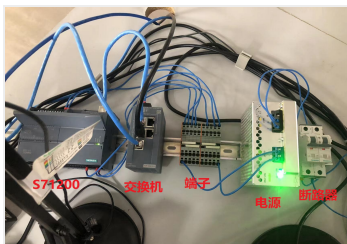


JieKong configuration Siemens PLC

JieKong configuration Siemens PLC experience summary 1. Install the driver To create a new project, select Device Communication -> Install Driver, and select Siemens S7TCP. 2. Add the switch data b...

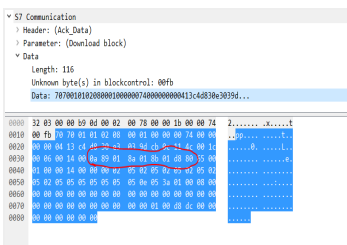
C # Communication Siemens PLC

First, the environment c#: .net core、s7netplus Siemens PLC: S7200Smart Second, the code...



c# connect to Siemens plc


1. Basic configuration: 2. Set the local IPv4 code segment to be the same. 3.c# interface design: (the IP format has been defined and can be seen in the program) 4. Reference xktcomm in the c# manager...



S7comm protocol analysis of the data fields (1)

Experimental environment: Siemens S7-300, CUP 315-2DP, step7 5.6, wireshark Objective: fetch packet reduction codes PLC Using

wireshark fetch PC and PLC data transmission, which contains code for the ...




IC Markets

Trade Now

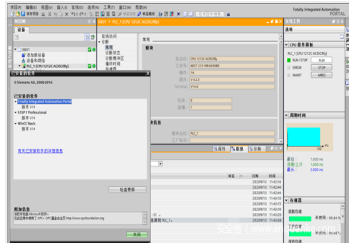
Trading CFDs involves high risk

Go Long or Short
with Leverage





More Recommendation



S7Comm Plus protocol research dynamic debugging two

1 Overview Previous articleDescribes the dynamic debugging of OMSp_core_managed.dll to understand the specific communication handshake and encryption authentication process.

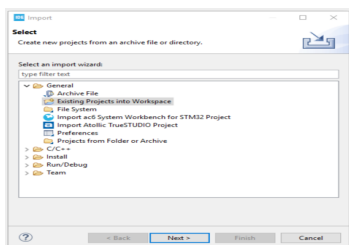
Through calculation, the v...



Dynamic debugging of S7Comm Plus protocol research

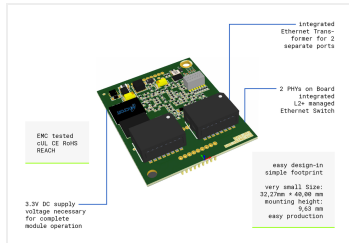
1 Overview Previous articlePreliminary research on the S7comm-Plus protocol is considered as a theoretical research. This article takes the core communication DLL (OMSp_core_managed.dll) as

the target...



SoM IoT multi-protocol module and Siemens PLC S7-1200 communication test guide (below)

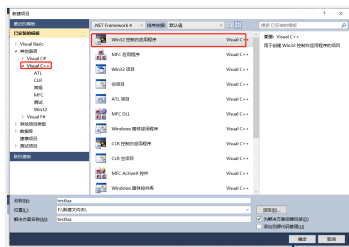
2.2 Import project Use the import dialog of STM Cube IDE to import the projects in the previously unzipped folder into the IDE. When prompted to enter the import type, select "Existing projects i...



SoM IoT multi-protocol module and Siemens PLC S7-1200 communication test guide (on)


1. SoM Introduction to IoT multi-protocol module The SoM IoT multi-protocol solution is a real-time, pre-certified (including sample applications) dual-port Ethernet module solution.

Currently, th...



Lua language with Siemens PLC interacts with S7 communication (II, homemade Lua protocol library, LUA and C language interaction)


Connect the upper article, this article is divided into several contents: 1. Use VS to create a dynamic link library. 2. Transplant the Lua Agreement Library. 3. Write the ADD (addition function) in t...




Trade Now

Trading CFDs involves high risk

Go Long or Short
with Leverage





Related Posts

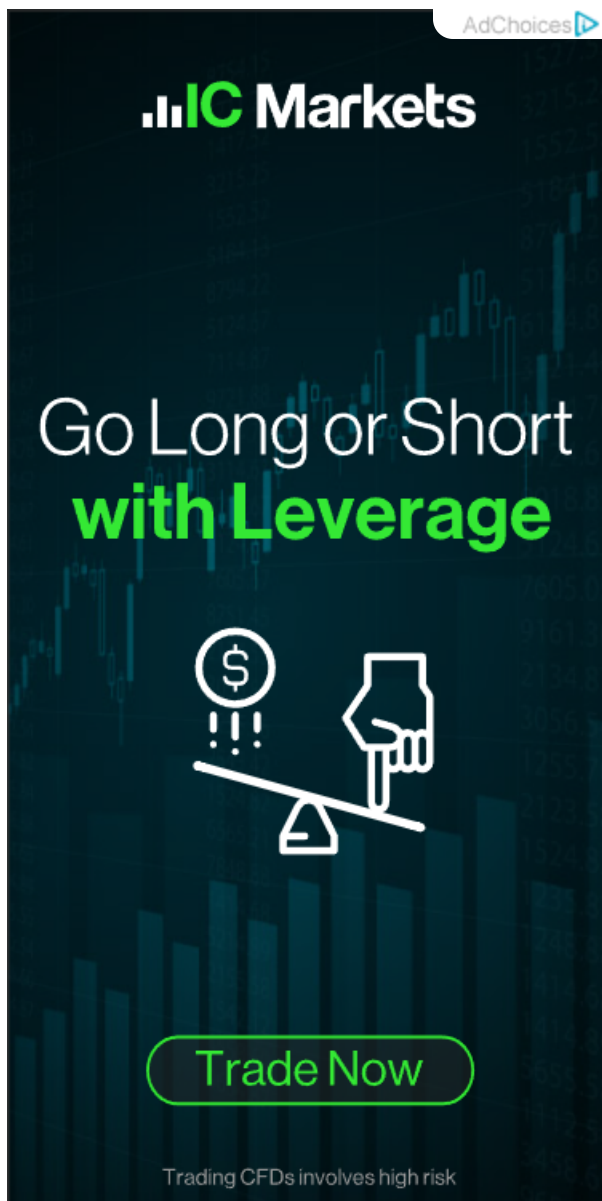
- Siemens PLC protocol-S7COMM
- Use QT to give Siemens PLC to Siemens PLC through the Modbusrtu protocol
- Siemens PLC various communication protocol parsing, analysis
- S7Comm Plus protocol research
- (2) Analysis of S7COMM protocol
- Analysis of data fields in the S7comm protocol
- Each brand PLC protocol reads and writes (Siemens AB Mitsubishi)
- [Industrial control old horse] Detailed explanation of Siemens PLC TCP protocol
- Analysis of Siemens S7comm-plus communication process and replay attack
- Siemens Soft PLC



Popular Posts

- Keywords: packet
- idea integrates tomcat and solves the console garbled problem

- [SOJ 639] trees
- Xiaobaixue front-end -----CSS basic grammar
- MYSQL date and time type format (detailed introduction)
- Network stream (template transfer)
- Layui jq finds the elements of the first element
- Python Algorithm Learning: Competitive Code Programming-Lanqiao Cup School Trial (Preliminary) Replay
- Freeswitch startup service script
- RISCv's cache



AdChoices

IC Markets

Go Long or Short
with Leverage

Illustration of a hand holding a lever with a dollar sign and three exclamation marks, symbolizing high leverage and risk.

Trade Now

Trading CFDs involves high risk

Recommended Posts

- Data Structures and Algorithms basis

- Front End Knowledge Sharing - SHEETJS Usage Experience
- Solve Endnote's reference to the problem without GBT7714 format
- Day04 (array)
- Mac installation git
- Image and large array types
- Convert grayscale image to pseudo-color image-pseudo-color processing
- GHOST blog build
- Android application component - Service
- Krpano tutorial - view tag Chinese description

**Khu Pho Luong Binh: Click Here To
See The Price Of Solar Panels**

housing-ink

Sponsored Links by Taboola

Related Tags

plc

S7

socket

java

Qt

automated industry

The internet

Industrial Control Protocol Series

Safety

Industrial control

Copyright **DMCA** 2018-2023 - All Rights Reserved -
www.programmersought.com **User Notice**