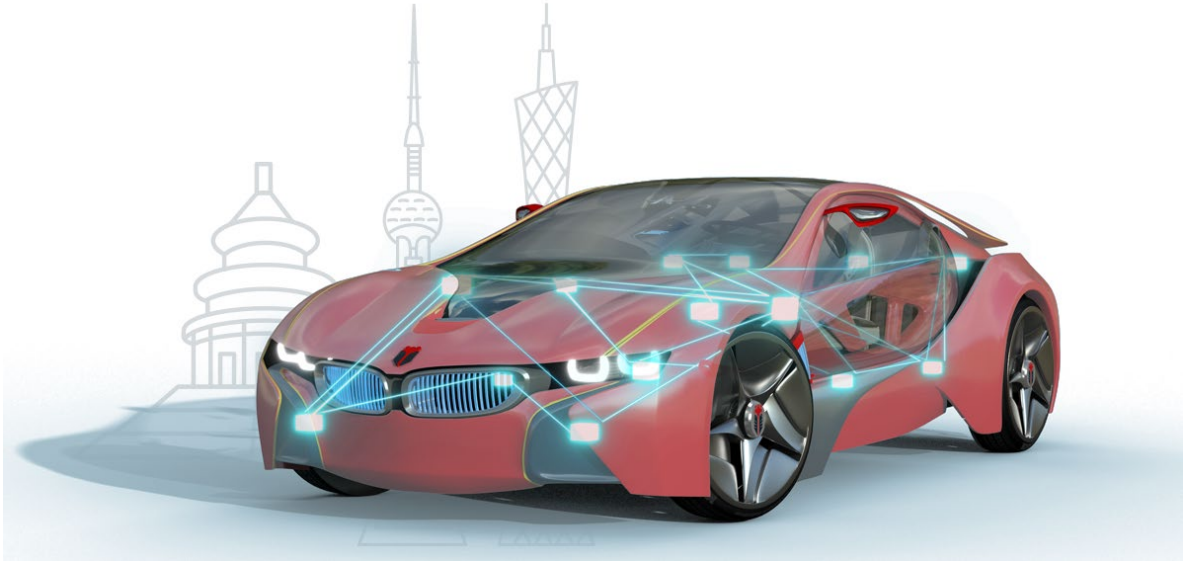
知从青龙瑞萨 RH850U2A 以太网刷写介绍

INTRODUCTION TO ZC.QINGLONG ETHERNET FLASHING BASED ON RH850U2A



知从青龙瑞萨 RH850U2A 以太网刷写介绍

INTRODUCTION TO ZC.QINGLONG ETHERNET FLASHING BASED ON RH850U2A

1 概述 OVERVIEW

瑞萨 RH850U2A MCU 是瑞萨电子跨域 MCU 产品系列的首款产品，其架构设计支持 EVITA Full 级别的信息安全功能，满足安全、快速的完全无等待 OTA 软件更新的安全需求。该汽车控制微控制器采用双核锁步架构，最高可配置四组主频达 400MHz 的 CPU 核心。每个核心均集成硬件虚拟化辅助功能，支持多个不同 ISO 26262 功能安全等级的软件系统在高性能运行状态下实现互不干扰的独立运作，同时有效降低虚拟化带来的性能损耗，确保实时计算效能。RH850/U2A MCU 集成多制式网络接口阵列，可高效处理 ADAS 及自动驾驶系统中多类型传感器生成的海量异构数据流。该设计为系统架构提供前瞻性支持，满足新一代高速率网络传输标准及严苛的通信带宽需求。

The RH850/U2A MCU is the first member of Renesas' cross-domain MCUs, with featuring architectural design that supports EVITA Full-level cybersecurity functions, enabling the device to support safe and rapid Full No-Wait Over-the-Air (OTA) software updates as security requirements evolve. This automotive control microcontroller adopts a dual-core lockstep architecture and can be configured with up to four groups of CPU cores with a main frequency of up to 400 MHz. Each core integrates hardware virtualization assistance functions, supporting multiple software systems with different ISO 26262 functional safety levels to operate independently without interference in a high - performance running state. At the same time, it effectively reduces the performance loss caused by virtualization and ensures real - time computing efficiency. The RH850/U2A MCU integrates a multi-protocol network interface array, enabling efficient processing of massive heterogeneous data streams generated by diverse sensors in ADAS and autonomous driving systems. This architecture provides forward-looking support for system design, meeting next-generation high-speed network transmission standards and rigorous communication bandwidth requirements.

2 ETHERNET OTA 概述 ETHERNET OTA OVERVIEW

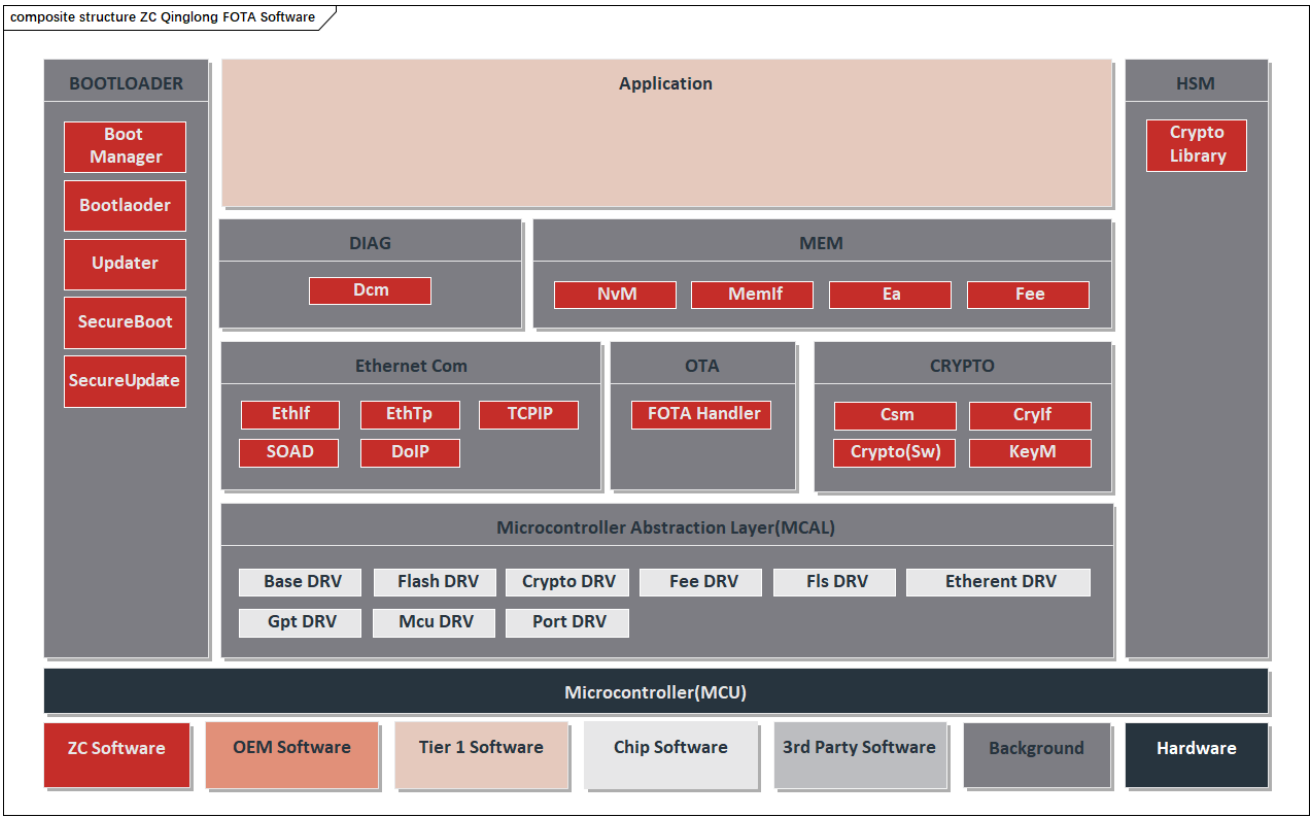
Ethernet OTA 的演进直接响应了汽车产业向"软件定义汽车"的转型需求。采用以太网的 OTA 方案，可将整车级软件刷新时间从 CAN 时代的 7.2 小时压缩至 18 分钟，同时支持 A/B 分区验证、数字签名校验等安全机制，符合 UNECE R156 法规对软件更新管理系统的强制认证要求。

The evolution of Ethernet OTA directly responds to the transformation needs of the automotive industry towards "software-defined vehicles". With the Ethernet-based OTA solution, the vehicle-level software refresh time can be reduced from 7.2 hours in the CAN era to 18 minutes. Meanwhile, it supports security mechanisms such as A/B partition verification and digital signature verification, meeting the mandatory certification requirements of the UNECE R156 regulation for software update management systems.

Ethernet OTA 技术作为智能汽车电子架构演进的核心支撑，其必要性主要体现在三个方面：首先，面对车载软件复杂度指数级增长，传统线下刷写方式已无法满足高频次的 ECU 固件更新需求；其次，ISO 21434 网络安全标准强制要求车辆具备安全漏洞的 72 小时热修复能力；再者，自动驾驶算法迭代需 50-100GB 级数据包的可靠传输，这远超传统 CAN/LIN 总线的承载极限。

As the core support for the evolution of the intelligent vehicle electronic architecture, the necessity of Ethernet OTA technology is mainly reflected in three aspects: First, in the face of the exponential growth of the complexity of in-vehicle software, the traditional offline flashing method can no longer meet the requirements of high-frequency ECU firmware updates. Second, the ISO 21434 network security standard mandates that vehicles should have the ability to perform hot-fixes for security vulnerabilities within 72 hours. Third, the iteration of autonomous driving algorithms requires reliable transmission of 50 - 100GB-level data packets, far exceeding the carrying capacity of traditional CAN/LIN buses.

3 OTA 架构概述 OTA ARCHITECTURE OVERVIEW



FOTA 系统架构
FOTA SYSTEM ARCHITECTURE

知从青龙 Ethernet FOTA 系统架构支持以太网通信场景下的 FOTA 功能，通过 TCP/IP、DoIP、SoAd、Dcm 模块实现 Ethernet 通信 UDS 诊断刷写，并通过适配 Crypto Library 实现各 OEM 规范的信息安全需求。以下为各模块的功能描述：

- Bootloader

  BootManager 模块提供 FOTA 启动管理功能，支持适配软硬件 SecureBoot 功能，通过烧录和刷写存储 Bootloader 和 Application 的期望 MAC 值，启动阶段 SecureBoot 通过计算比较 Bootloader 和 Application 的 MAC 执行软件完整性校验，保证软件安全需求。
- Ethernet Com

  DoIP 模块基于 TCP/IP 协议实现 Ethernet 通信收发功能，满足 ISO 13400 标准定义。通过车辆识别、路由激活、诊断消息功能实现 UDS 刷写流程，实现 Ethernet OTA 功能。
- Crypto、HSM

  Ethernet OTA 支持适配木牛加密库功能，支持非对称加密算法和加密算法结合实现安全刷写功能，适配证书认证功能满足安全诊断功能，适配 HSM 提高信息安全功能的稳定性和校验速度。

The Qinglong Ethernet FOTA system architecture supports the FOTA function in Ethernet communication scenarios. It realizes the UDS diagnostic flashing for Ethernet communication through the TCP/IP, DoIP, SoAd, and Dcm modules, and meets the Cybersecurity requirements of various OEM specifications by adapting to the Crypto Library. The following are the function descriptions of each module:

- Bootloader

  The BootManager module provides FOTA startup management functions and supports the adaptation of hardware and software SecureBoot functions. It stores the expected MAC values of the Bootloader and Application through programming and flashing. During the startup phase, SecureBoot performs software integrity verification by calculating and comparing the MACs of the Bootloader and Application to ensure software security requirements.

- Ethernet Com

  The DoIP module realizes the Ethernet communication sending and receiving functions based on the TCP/IP protocol, meeting the definition of the ISO 13400 standard. It implements the UDS flashing process through vehicle identification, routing activation, and diagnostic message functions, thereby achieving the Ethernet OTA function.

- Crypto, HSM

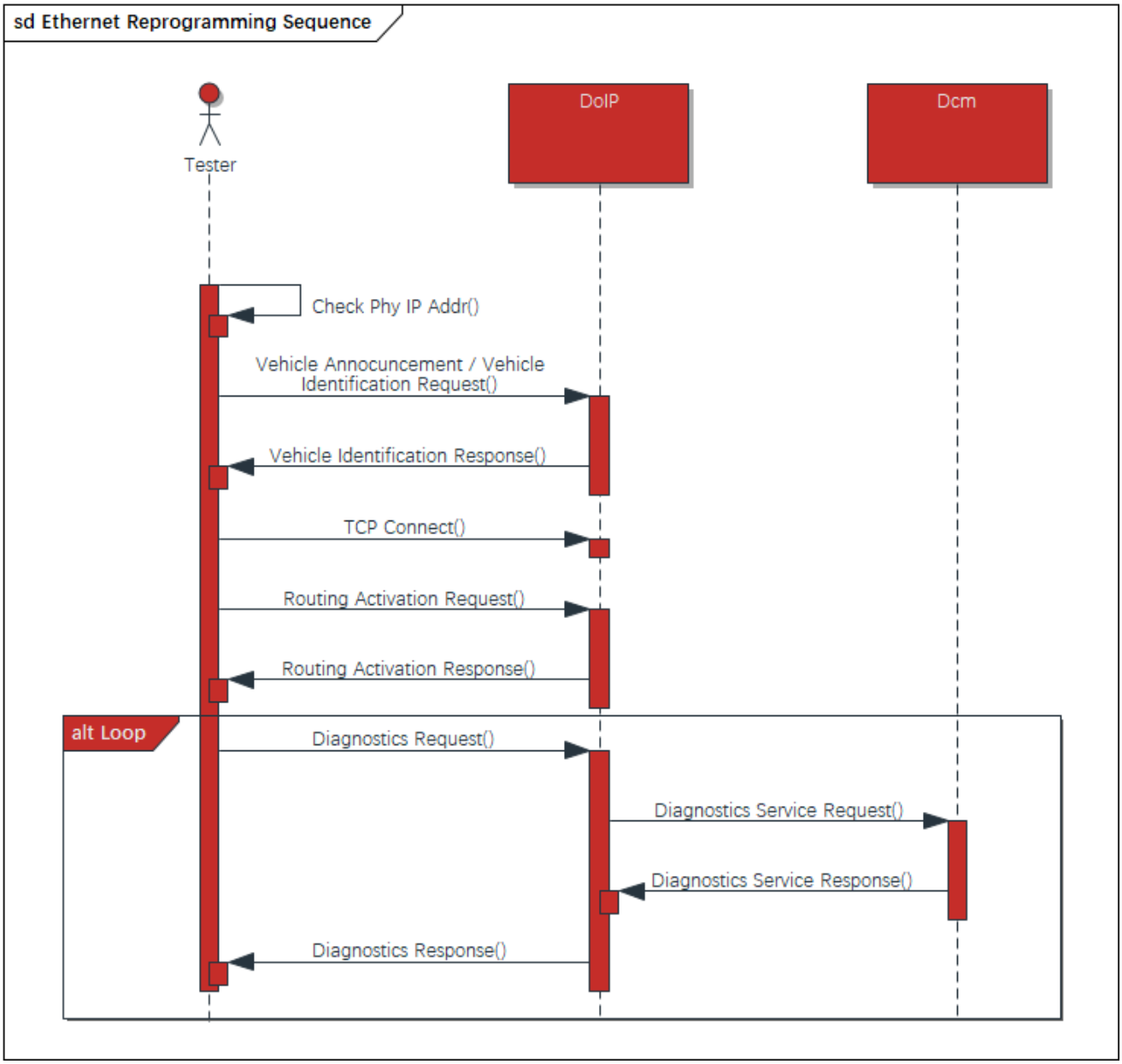
  The Ethernet OTA supports the adaptation of the Muniu encryption library functions. It combines asymmetric encryption algorithms with other encryption algorithms to achieve the secure flashing function. It adapts to the certificate authentication function to meet the security diagnostic requirements and adapts to the HSM to improve the stability and verification speed of the Cybersecurity function.

4 ETHERNET 刷写流程介绍 ETHERNET REPROGRAMMING PROCESS INTRODUCTION

外部诊断设备与车内 DoIP 实体通过车辆识别、建立连接、路由激活完成通信连接，并通过发送诊断服务执行 Ethernet OTA 的诊断刷写功能。外部诊断设备与车内 DoIP 实体建立通信的流程如下图所示。

The external diagnostic device and the in-vehicle DoIP entity complete the communication connection through vehicle identification, connection establishment, and routing activation, and execute the diagnostic flashing function of Ethernet OTA by sending diagnostic services. The

process of establishing communication between the external diagnostic device and the in-vehicle DoIP entity is shown in the following figure.



ETHERNET 刷写流程
ETHERNET FLASHING PROCESS

车辆发现流程的目的是将节点的 DoIP 属性告诉给当前局域网内其它 DoIP 节点。其它 DoIP 节点可根据当前节点的通信需求，决定是否与其建立通信连接：

The purpose of the vehicle discovery process is to inform other DoIP nodes in the current local area network of the DoIP attributes of a node. Other DoIP nodes can decide whether to establish a communication connection with it based on the communication requirements of the current node:

a) 上电后，Client 以广播方式主动发送 Vehicle Announcement Message / Vehicle Identification Request，在消息中携带逻辑地址、VIN、EID 等信息；

After power - on, the Client actively sends a Vehicle Announcement Message / Vehicle Identification Request in a broadcast manner, carrying information such as logical address, VIN, and EID in the message.

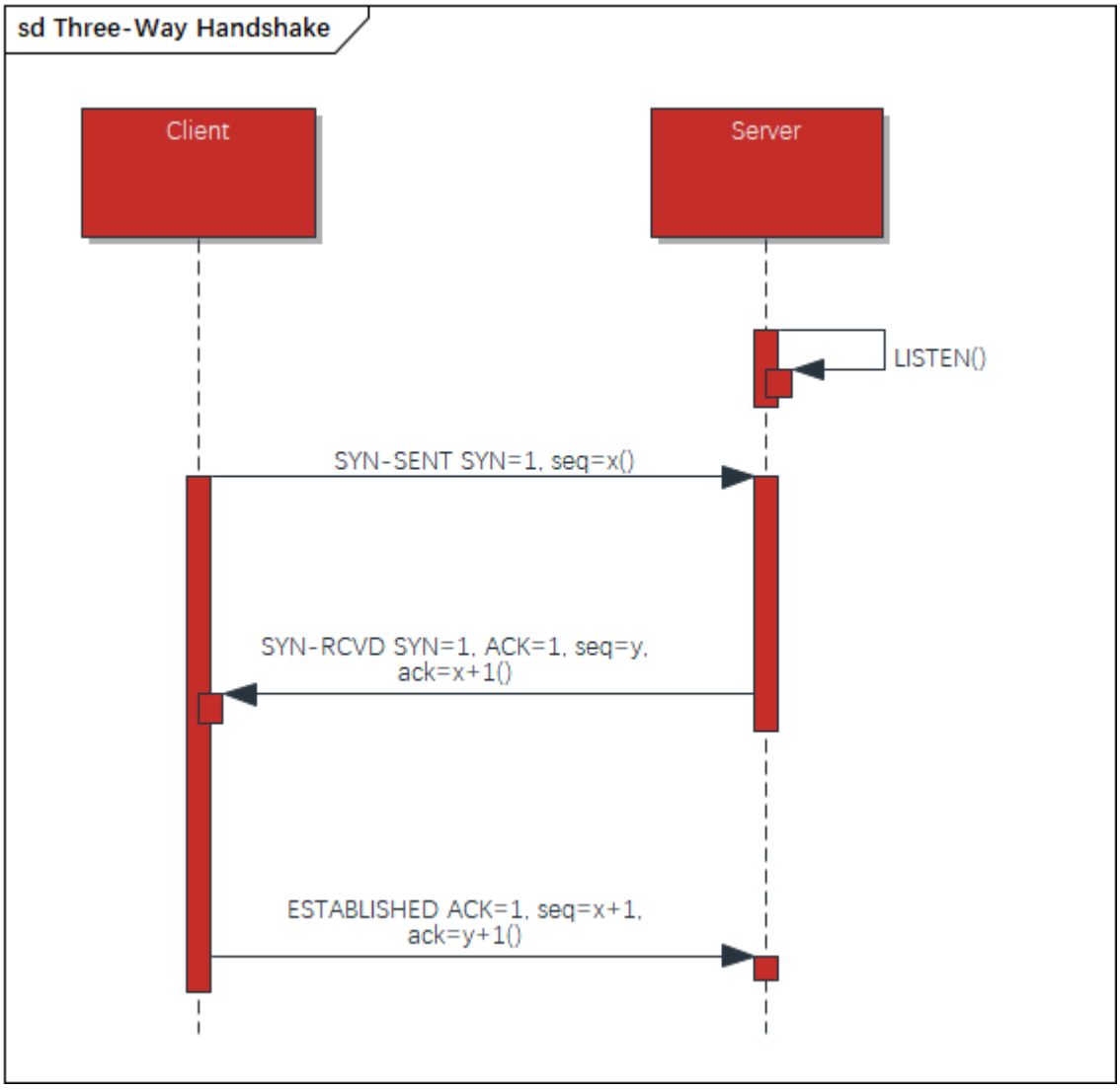
b) 收到该消息的 Server 以单播的形式回复 Vehicle Identification Response 消息，其中携带逻辑地址、VIN、EID 等信息。
The Server that receives this message replies with a Vehicle Identification Response message in a unicast form, which also carries information such as logical address, VIN, and EID.

Client 与 Server 在完成车辆识别后，通过建立 TCP 连接进行 UDS 通信：
After the Client and the Server complete vehicle identification, they conduct UDS communication by establishing a TCP connection:

a) Client 通过三次握手主动与 Server 建立 TCP 连接：
The Client actively establishes a TCP connection with the Server through a three - way handshake:

- 第一次握手：客户端向服务器发送一个带有 SYN（同步）标志的数据包，该数据包中包含客户端选择的初始序列号（Sequence Number），表示客户端希望与服务器建立连接。
First handshake: The client sends a data packet with the SYN (Synchronize) flag to the server. This packet contains the initial sequence number selected by the client, indicating that the client wishes to establish a connection with the server.
- 第二次握手：服务器接收到客户端的 SYN 数据包后，会向客户端发送一个带有 SYN 和 ACK（确认）标志的数据包。这个数据包中的序列号是服务器自己选择的初始序列号，而确认号则是客户端的序列号加 1，表示服务器已经收到了客户端的连接请求，并准备好与客户端建立连接。
Second handshake: After receiving the client's SYN packet, the server sends a data packet with both SYN and ACK (Acknowledgment) flags to the client. The sequence number in this packet is the initial sequence number selected by the server, and the acknowledgment number is the client's sequence number plus 1. This indicates that the server has received the client's connection request and is ready to establish a connection with the client.
- 第三次握手：客户端接收到服务器的 SYN+ACK 数据包后，会向服务器发送一个带有 ACK 标志的数据包，确认号为服务器的序列号加 1，表示客户端已经收到了服务器的响应，并且连接建立成功。此时，TCP 连接正式建立，客户端和服务器可以开始进行数据传输
Third handshake: After receiving the server's SYN + ACK packet, the client sends a data packet with the ACK flag to the server. The acknowledgment number is the server's sequence number plus 1, indicating that the client has received the server's response

and the connection is successfully established. At this point, the TCP connection is officially established, and the client and the server can start data transmission.



三次握手流程
THREE-WAY HANDSHAKE PROCESS

b) Client 发送 Routing Activation Request 消息请求激活路由，Server 根据实际情况同意或者拒绝激活请求，激活结果通过发送 Routing Activation Response 消息告知 Client。
The Client sends a Routing Activation Request message to request route activation. The Server either approves or rejects the activation request based on the actual situation and informs the Client of the activation result by sending a Routing Activation Response message.

完成路由激活后，上位机通过 DoIP 协议发送诊断刷写请求，使用诊断消息（0x8001）、诊断确认消息（0x8002）、诊断否定确认消息（0x8003）等载荷类型进行交互，并按照刷写流程发送指定的诊断报文数据，诊断刷写流程与 CAN 刷写无较大差异。

After the routing activation is completed, the upper computer sends a diagnostic flashing request via the DoIP protocol. It interacts using payload types such as diagnostic messages

(0x8001), diagnostic confirmation messages (0x8002), and negative diagnostic confirmation messages (0x8003), and sends the specified diagnostic message data according to the flashing process. There is no significant difference between the diagnostic flashing process and the CAN flashing process.

Payload type value	Payload type name	Specified in subclause	Support (DoIP gateways)	Support (DoIP nodes)	Port and protocol
0x0000	Generic DoIP header negative acknowledge	7.1.2	mandatory	mandatory	UDP_DISCOVERY UDP_TEST_EQUIPMENT_REQUEST TCP_DATA
0x0001	Vehicle identification request message	7.1.4	mandatory	mandatory	UDP_DISCOVERY
0x0002	Vehicle identification request message with EID	7.1.4	optional	optional	UDP_DISCOVERY
0x0003	Vehicle identification request message with VIN	7.1.4	mandatory	mandatory	UDP_DISCOVERY
0x0004	Vehicle announcement message/vehicle identification response message	7.1.4	mandatory	mandatory	UDP_DISCOVERY UDP_TEST_EQUIPMENT_REQUEST
0x0005	Routing activation request	7.1.5	mandatory	mandatory	TCP_DATA
0x0006	Routing activation response	7.1.5	mandatory	mandatory	TCP_DATA
0x0007	Alive check request	7.1.7	mandatory	mandatory	TCP_DATA
0x0008	Alive check response	7.1.7	mandatory	mandatory	TCP_DATA
0x0009 to 0x4000	Reserved by this part of ISO 13400				
0x4001	DoIP entity status request	7.1.9	optional	optional	UDP_DISCOVERY
0x4002	DoIP entity status response	7.1.9	optional	optional	UDP_TEST_EQUIPMENT_REQUEST
0x4003	Diagnostic power mode information request	7.1.8	mandatory	mandatory	UDP_DISCOVERY
0x4004	Diagnostic power mode information response	7.1.8	mandatory	mandatory	UDP_TEST_EQUIPMENT_REQUEST
0x4005 to 0x8000	Reserved by this part of ISO 13400				

DOIP PAYLOAD TYPES

Ethernet 刷写相比较于 CAN 刷写，主要在于以太网的通信速率则高很多，常见的有 100Mbps、1000Mbps 甚至更高，能够以更快的速度传输数据，大大缩短了刷写时间。同时由于 Ethernet 通信采用星型拓扑结构，通过交换机等设备将各个节点连接起来。诊断设备与目标 ECU 通过以太网接口和网线进行连接，利用以太网交换机实现数据的交换和转发，可支持更多设备连接，网络扩展性更好，能更好地支持多节点并发刷写。

Compared with CAN flashing, Ethernet flashing mainly features much higher communication rates of Ethernet. Common rates are 100Mbps, 1000Mbps or even higher, which enables data to be transmitted at a much faster speed and greatly shortens the flashing time. At

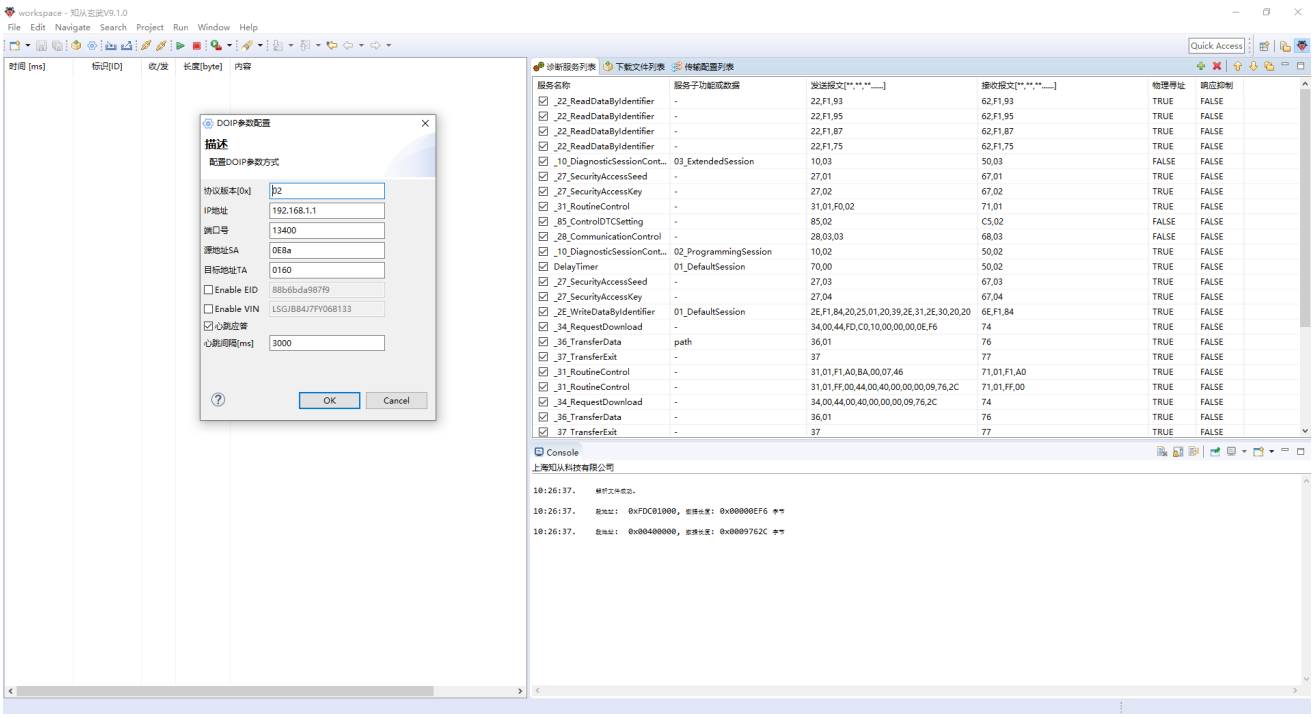
the same time, since Ethernet communication adopts a star topology, all nodes are connected through devices such as switches. The diagnostic device is connected to the target ECU via an Ethernet interface and network cable, and the Ethernet switch is used to realize data exchange and forwarding. It can support the connection of more devices, has better network scalability, and can better support concurrent flashing of multiple nodes.

以太网的网络管理功能较为强大，可通过交换机实现 VLAN 划分、流量控制、端口绑定等功能。安全性方面，可采用 IP 地址过滤、MAC 地址绑定、SSL/TLS 加密等多种安全机制，能更好地保护刷写过程中的数据安全和网络安全。

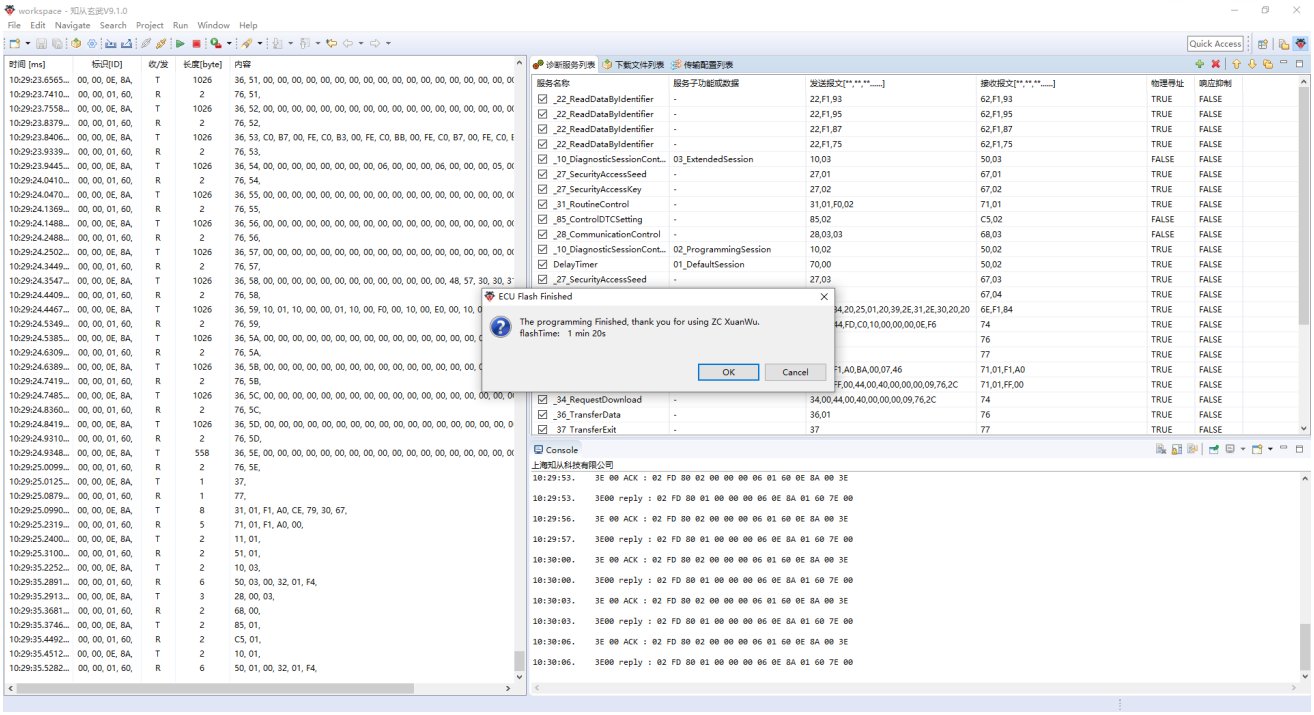
The network management function of Ethernet is quite powerful. Functions such as VLAN division, traffic control, and port binding can be achieved through switches. In terms of security, multiple security mechanisms such as IP address filtering, MAC address binding, and SSL/TLS encryption can be adopted to better protect data security and network security during the flashing process.

知从玄武上位机刷写工具支持 Boot 自动化测试：诊断服务测试、DID 测试、鲁棒性测试、压力测试，能够针对刷写场景自由配置逻辑地址、VIN、EID 等 DoIP 通信配置和诊断刷写流程，以下为知从玄武上位机刷写工具配置界面和刷写测试记录：

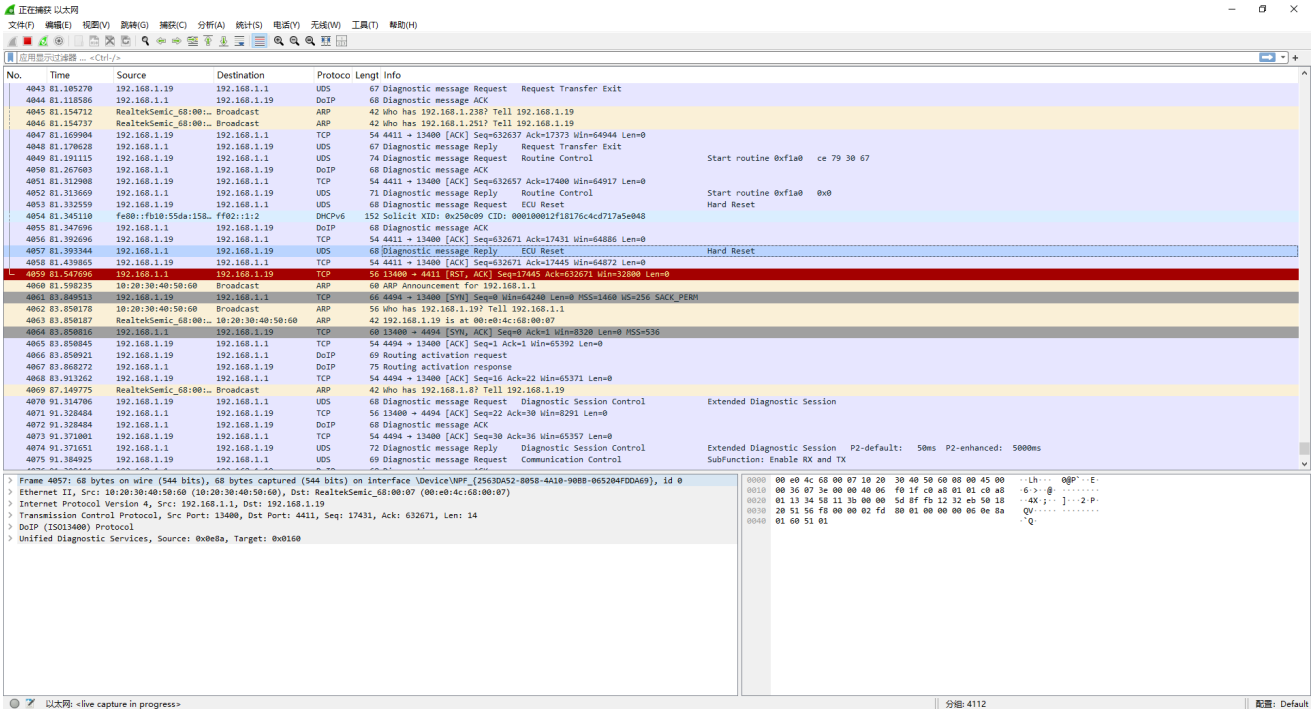
ZC Xuanwu Reprogramming Tool supports automated Boot testing, including diagnostic service testing, DID testing, robustness testing, and stress testing. It can freely configure DoIP communication settings such as logical addresses, VINs, and EIDs, as well as the diagnostic flashing process for different flashing scenarios. The following is the configuration interface of the ZC Xuanwu Reprogramming Tool:



知从玄武刷写工具配置界面
ZC XUANWU FLASHING TOOL CONFIGURATION INTERFACE



知从玄武刷写工具刷写记录
ZC XUANWU FLASHING TOOL FLASHING RECORDS



WIRESHARK 刷写记录
WIRESHARK FLASHING RECORDS