Abstract

This document defines the manner in which to calculate the checksum for the protocol DIASER. DIASER is a protocol for communication with traffic lights controllers used in France. DIASER is specified at AFNOR. The specification misses an instruction on how to compute the ‘BCC’ checksum (‘Byte Character Control’).
1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. DIASER Protocol and IETF Protocols

The DIASER protocol does this and that with a Traffic Lights controller - it is an Application Layer protocol. DIASER can be transported over UDP and over IP. The DIASER specification is available at a cost from AFNOR, on the World Wide Web. The DIASER specification does not describe the mechanism to compute the checksum 'BCC' (Byte Control Character). There exist several verbal (oral) versions of this mechanism: to cover or not to cover the STX (Start of Text), or the ETX (End of Text). Studying some implementations of a particular controller (Aximum) and packet dumps from independent sources, lead to a possibility to reverse engineer the specification of the checksum calculation of DIASER.

The DIASER protocol is an application layer protocol. Initially it was designed to run on serial lines like RS-232. Later on it was put on UDP (User Datagram Protocol). The UDP protocol is an IETF protocol. Running DIASER over UDP over IP is a great fact; contrary to RS-232, it allows to query a Traffic Lights Controller from a remote 'Poste de Commande et Control', and further from any other point in the Internet; second, it allows to query the controller over the future generation of Internet Protocol namely IPv6; thirdly, it allows to query the controller from nearby like an autonomous shuttle, with lower latency communications, thus supporting higher autonomous shuttle speeds; fourthly, it is easy to secure - rely on numerous security tools for software (IPsec, VPN) widely available and enjoy trust developed by Certificate Authorities and Let’s Encrypt.
IETF has its own way to specify a checksum. UDP, ICMP and other IETF protocols use a unique kind of checksum, which is specified in a particular RFC. It is clear that the RFC checksum is different from the DIASER checksum, at least because it involves also a notion of complement (not just XOR).

3. Checksum

The DIASER checksum is independent of the checksum field in the UDP header preceding the DIASER payload. In a DIASER/UDP packet there are two checksums: the DIASER checksum and the UDP checksum.

The DIASER checksum is an exclusive or operation (XOR) performed sequentially on the DIASER command; the bytes are read from left to right; the STX character is not read; the ETX character is read.

In French, the description of the checksum can be found in a proposal of updating the DIASER standard dated September 2018. It is written like this: 'Le caractère de contrôle BCC [checksum] est le résultat du “ou exclusif” de tous les caractères du message après STX non inclus, et peut prendre n’importe quelle valeur ASCII.'

A python implementation of the DIASER checksum is the following. Note the use of ‘^’ operator for XOR and the ‘for’ iteration on each byte. Note that only ETX is covered by the checksum, not the STX.

```python
#!/usr/bin/env python
# Mariama for CEA

packet="\x43\x6B\x30\x33\x47\x30\x30\x47\x30\x31\x47\x30\x32\x47\x30\x33\x47\x30\x34\x47\x30\x35\x47\x30\x36\x47\x30\x37\x47\x30\x38\x2A\x2A\x2A\x2A\x2A\x2A\x2A\x2A\x03"
# packet is 'Ck03G00G01G02G03G04G05G06G07G08*********|ETX'
checksum = 0
for el in packet:
    checksum ^= ord(el)
print hex(checksum)
```

Figure 1: Code snippet for DIASER Checksum

4. Security Considerations

Wrongly calculating a checksum may lead to security risks.

Petrescu & Sarr Expires November 21, 2019 [Page 3]
5.  IANA Considerations

    no request.

6.  Contributors

    Listed.

7.  Acknowledgements

    StA(C)phane GOEURIOT suggested an initial approximative oral
description of the checksum calculation.  Christophe DAMAS detailed
the description of the checksum calculation with more precision, as
an improvement to the DIASER standard.  Marco PEROTTI faced necessity
of proper checksum calculation.

8.  Normative References

    [RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
    Requirement Levels", BCP 14, RFC 2119,
    DOI 10.17487/RFC2119, March 1997,

Appendix A.  ChangeLog

    The changes are listed in reverse chronological order, most recent
    changes appearing at the top of the list.

    -01: added the description of checksum calculation as reported in
      French.

Authors’ Addresses

    Alexandre Petrescu
    CEA, LIST
    CEA Saclay
    Gif-sur-Yvette, Ile-de-France 91190
    France

    Phone: +33169089223
    Email: Alexandre.Petrescu@cea.fr
Mariama Sarr
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
France

Phone: +phone
Email: Mariama.Sarr@cea.fr