XEP-0365: Server to Server communication over STANAG 5066 ARQ

Steve Kille

mailto:steve.kille@isode.com

xmpp:steve.kille@isode.com

2022-03-28
Version 0.3

Status	Type	Short Name
Experimental	Standards Track	S5066

This specification defines operation over XMPP over the NATO STANAG 5066 data link service for point to point links (ARQ). This enables optimized XMPP performance over HF Radio (which STANAG 5066 was designed for) and over other data links using STANAG 5066.

Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 – 2024 by the XMPP Standards Foundation (XSF).

Permissions

Permission is hereby granted, free of charge, to any person obtaining a copy of this specification (the "Specification"), to make use of the Specification without restriction, including without limitation the rights to implement the Specification in a software program, deploy the Specification in a network service, and copy, modify, merge, publish, translate, distribute, sublicense, or sell copies of the Specification, and to permit persons to whom the Specification is furnished to do so, subject to the condition that the foregoing copyright notice and this permission notice shall be included in all copies or substantial portions of the Specification. Unless separate permission is granted, modified works that are redistributed shall not contain misleading information regarding the authors, title, number, or publisher of the Specification, and shall not claim endorsement of the modified works by the authors, any organization or project to which the authors belong, or the XMPP Standards Foundation.

Warranty

NOTE WELL: This Specification is provided on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE.

Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall the XMPP Standards Foundation or any author of this Specification be liable for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising from, out of, or in connection with the Specification or the implementation, deployment, or other use of the Specification (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if the XMPP Standards Foundation or such author has been advised of the possibility of such damages.

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF's Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy> or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

Contents

1 Introduction

This specification arose from requirements to operate over HF Radio, which has exceedingly high latency (sometimes minutes) low data rates (down to 75 bits/second) and poor reliablity. STANAG 5066 [1] is a widely used HF link level protocol. Direct use of **STANAG 5066** enables elimination of all extraneous end to end handshaking, which is important to optimize performance. It also enables use of **STANAG 5066** flow control, which is important for resilience.

The solution uses the streaming service specified by SLEP [2] - SIS Layer Extension Protocol. **SLEP** specifies three layer services that operate over STANAG 5066, including a streaming service which provides an equivalent service to TCP. **SLEP** also provides compression, which is mandated for use by this specification.

The solution is based on Zero Handshake Server to Server Protocol (XEP-0361) [3] and requires peer configuration to be established according to **XEP-0361**. The data exchanged between the XMPP servers follows exactly what is specified in **XEP-0361**. The data is transferred using **SLEP** rather than using TCP.

2 Requirements

This specification can be considered as a profile for server to server XMPP communication, to enable XMPP deployment over HF Radio using **STANAG 5066**. This profile MUST only be used where its use has been pre-agreed and configured for both participating servers.

3 Use Cases

An example scenario where this protocol is important is where two ships connected by HF Surface Wave communication only need to exchange XMPP messages. A reliable link (Soft Link) can be established using **STANAG 5066** and XMPP communicated efficiently and reliably over **SLEP**.

4 Business Rules

4.1 General Operation

Because of potentially very low bandwidth sending server MAY perform traffic optimisation, such as selective removal of stanzas that are not adding sufficient value, like CSNs, or strip selected elements such as xhtml-im.

---

[1]STANAG 5066 C3B (EDITION 3): PROFILE FOR HF RADIO DATA COMMUNICATIONS <https://www.isode.com/documentation/S5066Edition4ratification.pdf>.

[2]SIS Layer Extension Protocol (SLEP) (S5066-APP3) <https://www.isode.com/whitepapers/S5066-APP3.html>.

[3]XEP-0361: Zero Handshake Server to Server Protocol <https://xmpp.org/extensions/xep-0361.html>.

Applications sending data over **STANAG 5066** need to be aware of increased delays and any application level timers (e.g., IQ response timers) need to be set accordingly.

Stream Management (XEP-0198) [4] MAY be used over **SLEP**. Although reliability of stanza transfer is provided by use of **STANAG 5066** and **SLEP**, use of Stream Management (XEP-0198) [5] is RECOMMENDED to monitor link latency.

Application-layer keepalives such as white-space pings are NOT RECOMMENDED.

4.2 Mapping onto SLEP

The stanza stream is transferred using **SLEP**. **SLEP** compression is mandatory.

4.3 Addressing

The peer addressing of the **STANAG 5066** end points will be configured as part of the **XEP-0361** peer agreement.

The **STANAG 5066** SAP MAY be set to any mutually agreed value. It is RECOMMENDED that 6 is used which is the value specified in **STANAG 5066** for use by this XEP.

5 Security Considerations

Security Considerations of **XEP-0361** apply. **STANAG 5066** will frequently be employed in conjunction with link level crypto devices, which SHOULD be done when appropriate to provide data confidentiality.

6 STANAG 5066 Standard

This specification uses STANAG 5066 Edition 4 "TECHNICAL STANDARDS FOR HF RADIO LINK LAYER AND APPLICATION SUPPORT PROTOCOLS FOR SINGLE CHANNEL WAVEFORMS" (November 2021).

STANAG 5066 is a NATO UNCLASSIFED (Releasable to the Public) document that may circulated freely. It is available on `https://www.isode.com/documentation/S5066Edition4rat ification.pdf`.

---

[4]XEP-0198: Stream Management <`https://xmpp.org/extensions/xep-0198.html`>.

[5]XEP-0198: Stream Management <`https://xmpp.org/extensions/xep-0198.html`>.

7 SLEP

This specification uses the streaming service specified by SIS Layer Extension Protocol (SLEP) (S5066-APP3).
SLEP is an openly available protocol specification with no license restrictions. It is available on https://www.isode.com/whitepapers/S5066-APP3.html.

8 Acknowledgements

Curtis King designed and validated the original approach documented in this XEP.
Kevin Smith provided useful comments on this specification.
Dave Cridland asked NATO about STANAG 5066 publication, leading to its availability on the Web.
Edwin Mons implemented and validated the SLEP mapping.