



Providing Control Parameters for STANAG 5066 over UDP/IP through IP Crypto (S5066-APP9)

11th December 2019

Version: 1.0

Status: Experimental

1 Purpose

This specification defines a control mechanism to communicate key parameters to a black side STANAG 5066 server in conjunction with use of IP Crypto and “Providing STANAG 5066 services over UDP” (S5066-APP7).

Two mechanisms are defined:

1. To use the DSCP header, which is a simple mechanism that is expected to be available as an option in many IP Crypto systems.
2. To use an IP addressing mechanism that can be used with any IP Crypto.

2 Requirements

When IP Crypto is used, all of the end to end data specified in S5066-APP7 is encrypted and so not available for control.

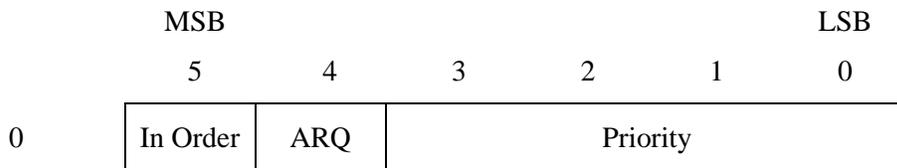
IP Cryptos will provide black side IP addressing that can be used to select destination and map to source and destination STANAG 5066 Addresses.

Each black side IP packet contains a single encrypted STANAG 5066 Unidata request. In order for an S5066-APP7 SIS Server provide the full SIS service for this Unidata, the following information needs to be communicated to the black side STANAG 5066 server:

1. Priority of the Unidata.
2. ARQ or Non-ARQ.
3. “In Order”.

3 Encoding and Mechanisms

The following 6 bit encoding of an integer is defined:



This is defined as follows:

1. In Order bit set to 1 if “in order” service required.
2. ARQ bit set to 1 if ARQ service required and 0 for non-ARQ.
3. STANAG 5066 priority encoded in bits 0-3, with MSB in bit 3.

This is a simple encoding. Use of standard DSCP values needs to be considered, and an encoding that will better co-exist with other DSCP uses may be considered.

3.1 Use with DSCP

Where the DSCP field can be used for red to black transfer, the integer is used in the 6 bit IPv4 or IPv6 DSCP field. If DSCP can be used, it is generally preferred.

However, use of DSCP may not pass through IP Crypto or may get modified on path to IP Crypto.

3.2 Use with IP Addressing

A second approach is to signal on sending side, the parameters by use of IP addressing.

On Red sending side, use a range 64 IP addresses, with the choice of addresses communicating the parameter. There can be a base IP address, and by adding the integer to the base address, an IP address for each service combination can be allocated, and the correct black side STANAG 5066 parameters chosen.

For example consider use of a private IP subnet 192.168.0.0/64, which has IP addresses in the range 192.168.0.0 to 192.168.0.63. 192.168.0.0 is “not in order”, “non-ARQ”, priority 0; 192.168.0.1 is “not in order”, “non-ARQ”, priority 1; and so on.

This approach gives a simple signaling mechanism from the red side SIS server to IP Crypto.

It will generally be inconvenient to configure large numbers of IP addresses black side. In practice only a few combinations will be needed, noting:

- In Order is only used by a few legacy applications, with ARQ and fixed priority.
- The only current application that varies priority is military messaging, and only four values are used. Note that priority is also used to distinguish between applications.
- Black side addresses could represent a range of priorities.

Black side IP addresses will generally be chosen in context of target traffic, and mappings with red side addresses configured for IP Crypto.

A possible approach is to map IP addresses with the DSCP value extractable by Icon-IP using a bit-mask.