Isode

XML Control Messages for STANAG 5066 over UDP/IP through a Data Diode (S5066-APP7)

20th December 2021

Version: 1.3

Status: Experimental

1 Purpose

This specification defines data formats to communicate control information from a black side STANAG 5066 server in conjunction with use of IP Crypto and "Providing STANAG 5066 services over UDP/IP" (S5066-APP4).

The model is that a data diode is used on the security boundary between the SIS server and black side STANAG 5066 server. This specification is for use where the data diode is an XML guard. It defines XML format messages.

The specification also defines an optional red to black side protocol, to enable reliable communication.

This version of the specification provides example XML messages. A future version of this specification will include an XML schema.

2 Requirements

The (red side) SIS server needs to flow control its clients in line with the black side STANAG 5066 server. So, flow control needs to be communicated black to red side.

When messages are sent using UDP over S5066-APP7, any rejections and node confirmation of delivery needs to be communicated from the black side STANAG 5066 server. This needs a mechanism to associate rejections and confirmations to the original message. This is done by the black side assigning an ID to each inbound message and communicating this with a message to red side.

When messages are delivered, a data diode message is provided to enable red side to determine if there is message loss.

3 Transfer

This format can be transferred over a choice of data diode mechanisms including:

1. UDP used in conjunction with a physical data diode. This is an unreliable mechanism. The protocols specified here are designed so that messages can be repeated in order to increase reliability.
2. Interface to XML Guard acting as an application data diode. This mechanism will provide reliable transfer.

4 XML Messages (Black to Red)

This section shows by example a set of XML messages to be sent from black to red.

4.1 Flow Control

Two XML packets are defined, representing Flow On and Flow Off messages

```
<Flow xmlns='http://isode.com/s5066-app7/0/'>
      <on/>
</Flow>
```

And

```
<Flow xmlns='http://isode.com/s5066-app7/0/'>
      <off/>
</Flow>
```

4.2 IP Packet Correlation

There is a need to correlate IP packets. The core approach is the black side will assign an ID to each packet sent, with an integer ID one greater than the previous one. It will report the ID and information about the IP packet to red side using the following message:

```
<IPSent xmlns='http://isode.com/s5066-app7/0/'>
      <IP-ID>123456</IP-ID>
      <Source>
            <IPv4>192.168.0.0</IPv4>
      </Source>
      <Dest>
            <IPv4>192.168.0.0</IPv4>
      </Dest>
      <IPProtocol>51</IPProtocol>
      <Size>392</Size>
      <DSCP>55</DSCP>
      <ECN>2</ECN>
      <ARQ/>
      <Priority>7</Priority>
      <NotInOrder/>
</IPSent>
```

4.3 Black Side Operation

The black side IP Client needs to distinguish between IP packets containing encrypted data which correspond to red side requests and information being exchanged by the crypto devices over IP, typically for initialization and key update. This can usually be done by IP protocol number, where the red traffic uses one IP protocol and other data uses different protocol numbers. Some crypto devices might need other heuristics.

Communication from the crypto devices should be sent ARQ and with priority 15.

The black side model for red side packets is that it will mechanically report on each IP packet arriving.

1. Source and Destination IP addresses are taken from the packet.
2. IP Protocol is the IP protocol being used
3. Size is the IP packet size
4. DSCP value (6 bits)
5. ECN value (2 bits)

6. STANAG 5066 values for ARQ and Priority used by black side, which may be derived from DSCP or address map.

4.4 Red Side Operation

Basic operation is that red side will send a packet and then wait for the matching IP packet to be sent. It can then correlate the IP ID to the STANAG 5066 message sent. This enables status messages to be sent back correctly. It is envisaged that IP packets will be sent lock step, where a packet is sent by red side and it waits for an ack.

The most likely reason for delay in acknowledgement is that an HF link has not been established and this is preventing crypto initialization and so the packet is not sent. Rather than resending the unacknowledged packet, and empty packet is sent. This will allow the red side to detect when the link is up.

There is a very small risk that packets will be lost and this needs to be allowed for. Red side needs to correlate based in information in this message and to resend when it is clear that a message has been lost. There are a number of heuristics that can be applied:

1. ARQ setting and priority are echoed back. This can give clear correlation in the event that these values change between PDUs.
2. Message size. This will be correlated to the size of data sent noting that the reported sizes will be larger. This may be useful when PDU sizes vary.
3. ECN provides two bits that can be sent. Most crypto devices will pass these through and so the values will be echoed back. By incrementing the value, occasional loss can be detected.

4.5 Node Confirm and Reject

If an IP packet sent over STANAG 5066 gets a reject, the following message is sent:

```
<Reject xmlns='http://isode.com/s5066-app7/0/'>
      <IP-ID>123456</IP-ID>
      <Reason>2</Reason>
</Reject>
```

If an IP packet confirms node delivery, then the following message is sent. Note that Node Delivery is always requested for ARQ black side. Red side will return to client if the client requested it.

```
<NodeConfirm xmlns='http://isode.com/s5066-app7/0/'>
      <IP-ID>123456</IP-ID>
</NodeConfirm>
```

4.6 Inbound Data

IP traffic also flows from Black to Red. This traffic is reported over the data diode using a similar mechanism:

```
<IPReceived xmlns='http://isode.com/s5066-app7/0/'>
      <IP-RCV-ID>123456</IP-ID>
      <Source>
            <IPv4>192.168.0.0</IPv4>
      </Source>
      <Source>
            <IPv4>192.168.0.0</IPv4>
      </Source>
      <IPProtocol>51</IPProtocol>
      <Size>392</Size>
      <DSCP>55</DSCP>
      <ECN>2</ECN>
      <ARQ/>
      <Priority>7</Priority>
      <NotInOrder/>
</IPReceived>
```

IP-RCV-ID is assigned one greater than previous. This allows red side to detect loss, but not to address it.

There is possibility of loss of either this datagram (which may be repeated to increase reliability) or of the IP packet on which it is reporting. Loss of this datagram can be inferred by IP-RCV-ID sequence number gaps. Risk of loss is low. Red side needs to correlate the datagrams, to handle loss on startup. The additional information enables this.

1. If DSCP and ECN can be set and are passed by the IP crypto, these can be set with increasing values to provide robust correlation,
2. The other three parameters can be determined from SIS. These will match values inside the encrypted IP packet, and so can also provide correlation.

5 Red to Black Protocol

There is a similar protocol for diode going red to black side, which addresses the risk of loss of IP packets going black to red. It is a simple resend request for a packet of a given ID.

5.1 IP Packet Correlation

There is a need to correlate IP packets. The core approach is the black side will assign an ID to each packet sent (IP-RCV-ID), with an integer ID one greater than the previous one as described in Section 4.6. This message is used by red side to request resend of a specific message:

```
<ResendRequest xmlns='http://isode.com/s5066-app7/0/'>
      <IP-RCV-ID>123456</IP-RCV-ID>
</ResendRequest>
```