Interface Control Document
For the
Internet Protocol Suite (IPS) Gateway

Draft version 3

June 15, 2018

Prepared by:

Rockwell Collins IMS

Revision History

Revision	Date	Action / Preparer
v1	2/1/2018	Initial Release / R. Dlouhy, J. Graefe, M. Stevenson
v2	4/12/2018	Updated to incorporate feedback and results from prototype testing / J. Graefe, R. Dlouhy, M. Niraula
v3	6/15/18	Updated in response to industry and internal comments. R. Dlouhy, J. Graefe, M. Niraula

Table of Contents

List of Figures

List of Figures

1 Scope

This ICD defines the air and ground interfaces for the IPS Gateway and the associated required processing.

1.1 System Overview

With the existing ACARS network and Aeronautical Telecommunication Network (ATN) infrastructure being aviation-unique and becoming dated, a need has been identified for a modern, off-the-shelf, efficient, and robust network infrastructure for both air traffic services (ATS) and aeronautical operational communications (AOC) safety service applications, as well as for other applications like Aeronautical Administrative Communications (AAC), System Wide Information Management (SWIM), Unmanned Airborne System (UAS) Command and Control (C2), Airport Operations, Voice over IP (VoIP), and ground/ground services. The new aviation network infrastructure for these safety services is based on the modern Internet Protocol Suite (IPS). Internet Protocol (IP) simplifies routing in an increasingly internetworked aviation industry. IP provides a sustainable path away from ARINC 620 (A620) ground messaging. IP is the universal norm for application to application communication. IP version 6 (IPv6) address space allows for fixed aircraft address, greatly simplifying message delivery across the globe. This new IPS network must accommodate legacy and new production aircraft, and must support existing A620 hosts for AOC and FANS 1/A applications, and ATN/OSI for B1/B2 applications. To provide this level of flexibility ground gateways are required to be a part of this network.

The IPS Gateway (G/W) provides this interoperability between IPS Aircraft, legacy aircraft, IPS Ground Systems, ATN/OSI end systems, and legacy A620 hosts. This is done by the IPS Gateway by accommodating multiple protocol types of aircraft and providing the protocol conversion and routing between the aircraft and the peer ground system. The architecture incorporating the IPS Gateway is shown in Figure 1-1. The lines in red highlight the new infrastructure.

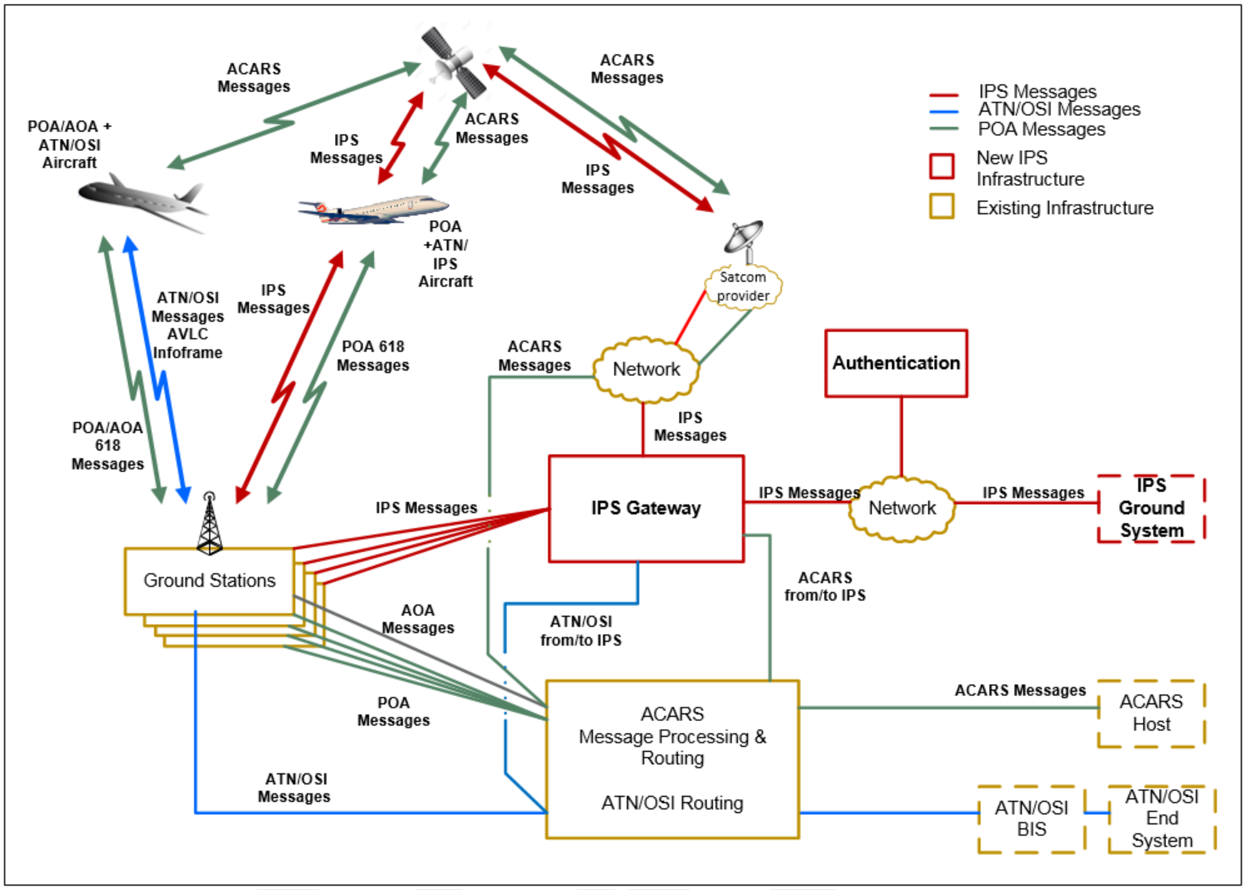


Figure 1-1 - Air-Ground Communications w/IPS Architecture

Since the introduction of ATN/IPS avionics and ATN/IPS ground end systems will happen over an extended time period, the ground-based IPS Gateways will become a key part of the ATN/IPS ground infra-structure. Air/Ground Communications Service Providers (ACSPs) will have to facilitate interoperability by providing ATN/IPS ground gateways.

The IPS gateway will be compatible with the multi-link concept, supporting the use of all available IPS media with the routing based on user (airline or ANSP) defined routing policy (either pre-defined or based on Quality of Service criteria).

The context driving the ground architecture is illustrated in Figure 1-2.

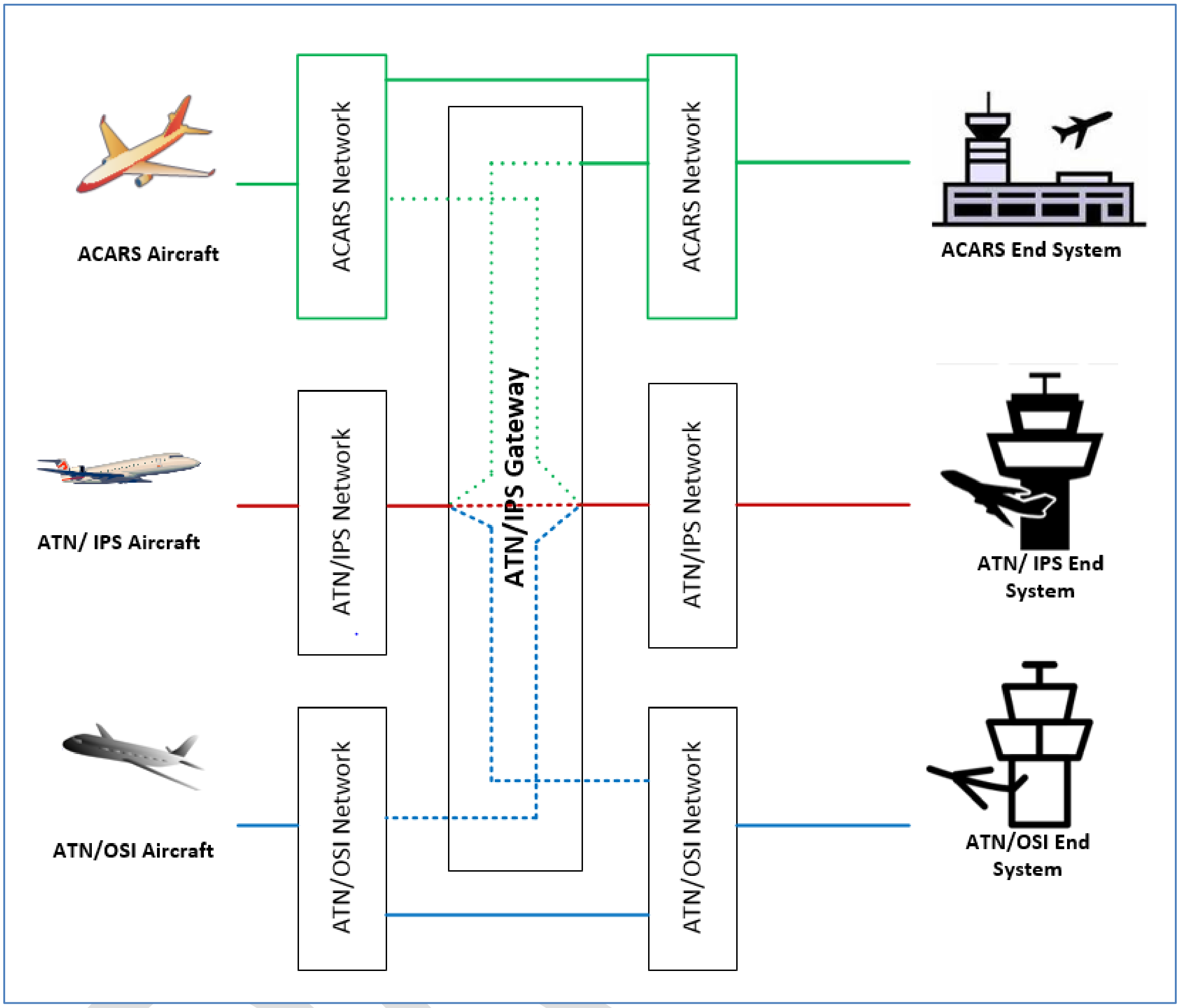


Figure 1-2 – ATN/IPS Gateway Interfaces

The key point of the figure above is that protocol conversion will be done by the IPS Gateway only if one side (either the aircraft or End System) is IPS enabled. In these cases, the IPS Gateway is effectively an IP End System.

The key areas the IPS Gateway addresses include:

- Accommodation of multiple protocols, providing conversion and routing functionality:
    - Routing of IP downlink messages, both ATS and AOC, including internetworking via other CSP network(s)
    - Creating copies of ATS IP messages per airline customer request (normal request on FAA Datacomm)
    - Converting AOC IP downlink messages to ARINC 620 per airline customer request (legacy back-office support)
    - Converting ATS IP downlink message to ATN/OSI per ANSP request (legacy ANSP support)

  - Converting legacy ARINC 620 AOC input messages to IP uplinks (legacy airline back-office support)
  - Converting ATS ATN/OSI uplink messages to IP uplinks (legacy ASNP support)
  - Converting IP AOC input messages to ARINC 620 for uplink via legacy ACARS in non-IPS regions for non-SATCOM aircraft
- Accommodation of existing and future air ground data links. These air/ground links include:
  - Future SatCom (SBB , Certus)
  - VDL Mode 2
  - AeroMACS
  - LDACS
- Implementation of cyber security measures.
- Authentication of aircraft for IPS communications.
- Provision of data compression.
- IP name lookup service.
- Message encapsulation

1.2 Document Overview

This document is organized as follows:

- **Section 1, Scope,** Contains the project identification, system and document overviews, a list of the terms, and acronyms used in this document.
- **Section 2, Applicable Documents,** Provides a list of the documents referenced in this standard. References contain the document number, exact title, revision level and issue date.
- **Section 3, General Requirements,** Provides the top level requirements for the gateway.
- **Section 4, Media Specific Details,** Provides the details of IPS over different media.
- **Section 5, Interface Characteristics,** Provides an overview of the IPS interface.
- **Section 6, Interface Details,** Provides the details of the IPS interface.
- **Section 7, Appendix A – Ground Station Requirements,** Provides the details of the ground station requirements for IPS.

1.3 Acronyms

ACARS	Aircraft Communications Addressing and Reporting System
AOA	ACARS Over AVLC
AOC	Airline Operational Control
ARLM	Air/Ground Router Link Manager
ATN	Aeronautical Telecommunication Network
ATNPKT	Aeronautical Telecommunication Network Packet
ATS	Air Traffic Service
AVLC	Aviation VHF Link Control
A620	ARINC 620
CA	Certificate Authority
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DH	Diffie Hellman

DHE	Diffie Hellman Ephemeral
DL	Downlink
DS	Dialogue Service
DSA	Digital Signature Algorithm
DSP	Datalink Service Provider
DTE	Data Terminal Equipment
DTLS	Datagram Transport Layer Security
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
FCS	Frame Check Sequence
GS	Ground Station
GSIF	Ground Station information Frame
G/W	Gateway
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPI	Initial Protocol Identifier
IPS	Internet Protocol Suite
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MIC	Message Integrity Check
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
RFC	Request for Comments
SDP	Satellite Data Packet
TLS	Transport Layer Security
UDP	User Datagram Protocol
UL	Uplink
VDL	VHF Data Link
VDLM2	VDL Mode 2

1.4 Terminology

ACARS – Aircraft Communications Addressing and Reporting System
A protocol designed by ARINC for transmission of short messages between aircraft and ground stations via airband radio or satellite. The basic ACARS protocol and air/ground message structure used to transfer information between customer aircraft and the datalink service provider are defined by the industry specification ARINC 618 (Air-Ground Character-Oriented Protocol Specification).

AOA – ACARS Over AVLC (where AVLC stands for Aviation VHF Link Control)
The protocol used to carry ACARS messages between the aircraft and VDLM2 ground stations.

IPS Aircraft – Aircraft that has the collection of airborne components and functions that provide ATN/IPS services. IPS aircraft are anticipated to be dual-stacked with ATN/IPS and ACARS capability.

IPS Ground System – Ground system that has the collection of ground components and functions that provide ATN/IPS services.

IPS Gateway – Ground functionality that provides for interoperability between IPS aircraft and non-IPS (ATN/OSI, ACARS) ground systems, and non-IPS aircraft and IPS ground systems.

Primary Service Provider – The communications service provider that is contracted to provide communications service for a given aircraft. The Primary Service Provider is the home mobility point and provider for keys and key management functions.

Trusted companion service provider – A communications service provider that an airline has an agreement with for secondary communications services (when out of primary service providers area of coverage) and with which the primary service provider has an established trust relationship.

Untrusted companion service provider – A communications service provider that does not have an established trust relationship with the primary service provider.

2 Applicable Documents

[1] **ICAO Document 9896, 2nd Edition:** Manual on the ATN using IPS Standards and Protocols

[2] **ICAO Document 9776:** Manual on VHF Digital Link (VDL) Mode 2

[3] **ARINC Specification 618:** Air-Ground Character-Oriented Protocol

[4] **ARINC Specification 620:** Data Link Ground System Standard and Interface Specification (DGSS/IS)

[5] **ARINC Specification 622:** ATS Data Link Applications over ACARS Air-Ground Network

[6] **ARINC Specification 623:** Character-Oriented Air Traffic Service (ATS) Applications

[7] **ARINC Report 842-**1: Guidance for Usage of Digital Certificates

[8] **ARINC Project Paper 658:** Internet Protocol Suite (IPS) for Aeronautical Safety Services Roadmap

[9] **CPS-IAGS Interface Control Document,** ARINC Document Number 16069

[10] **RFC 2373,** IP Version 6 Addressing Architecture

[11] **RFC 8200**, Internet Protocol, Version 6 (IPv6) Specification

[12] **RFC 6347**, Datagram Transport Layer Security Version 1.2

[13] **RFC 4492**, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security

[14] **RFC 5077**, Transport Layer Security (TLS) Session Resumption without Server-Side State

[15] **RFC 5289**, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

[16] **RFC 5246**, The Transport Layer Security (TLS) Protocol Version 1.2

[17] **RFC 7627**, Transport Layer Security (TLS) Session Hash and Extended Master Secret

[18] **IANA Transport Layer Security (TLS) Extensions**, https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml

3 General Requirements

The IPS Gateway is designed to facilitate communications with IPS equipped aircraft using existing air-ground network infrastructure and to accommodate future air-ground links. The IPS Gateway will initially interface with IPS Aircraft using VDL Mode 2 and Satcom, with IPS Ground Systems, with legacy A620 airline hosts, and with ATN/OSI End Systems. Figure 3-1 identifies the interfaces and data flow that the IPS Gateway supports for IPS.

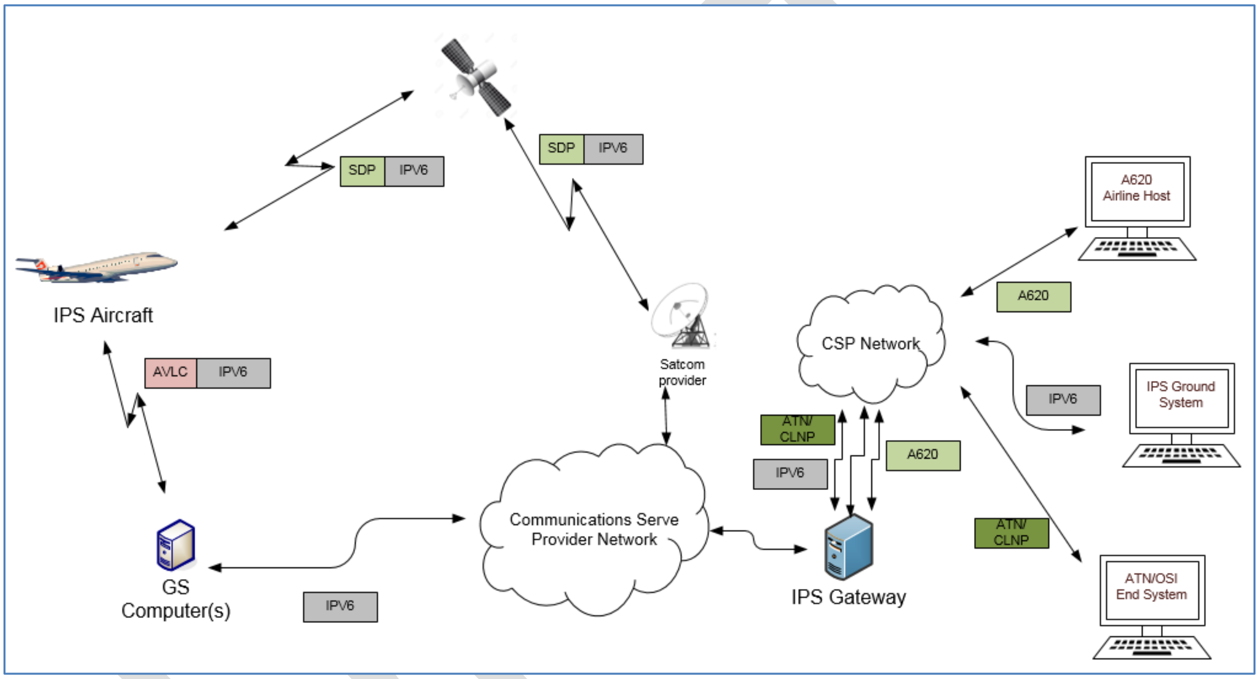


Figure 3-1 - Data Flow to/from IPS Aircraft

The IPS Gateway will also support communication of non-IPS aircraft (ATN/OSI and ACARS) with IPS Ground Systems. Figure 3-2 shows the data flow for between an ACARS aircraft and an IPS ground system.

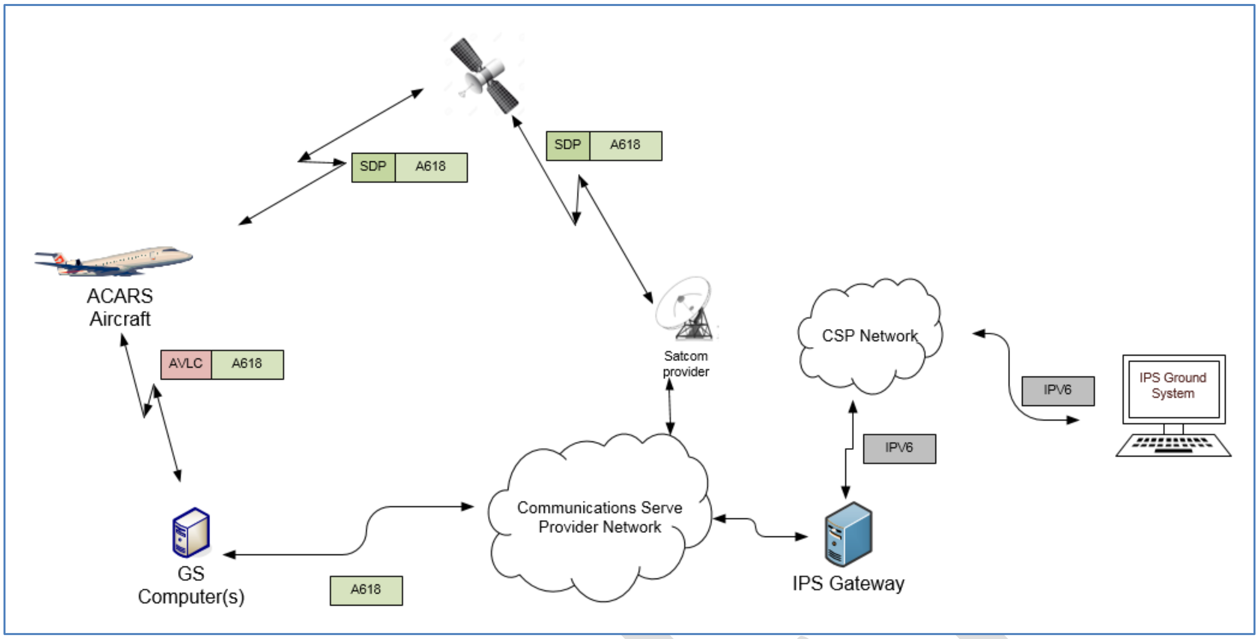


Figure 3-2 -Data Flow between IPS Ground System and non-IPS aircraft

It should be noted that there can be any number of IPS Gateways as a part of the ATN/IPS network. A Gateway could be associated with landing of data for a specific air / ground link or with a specific ANSP or a specific airline. The following diagram illustrates this concept.

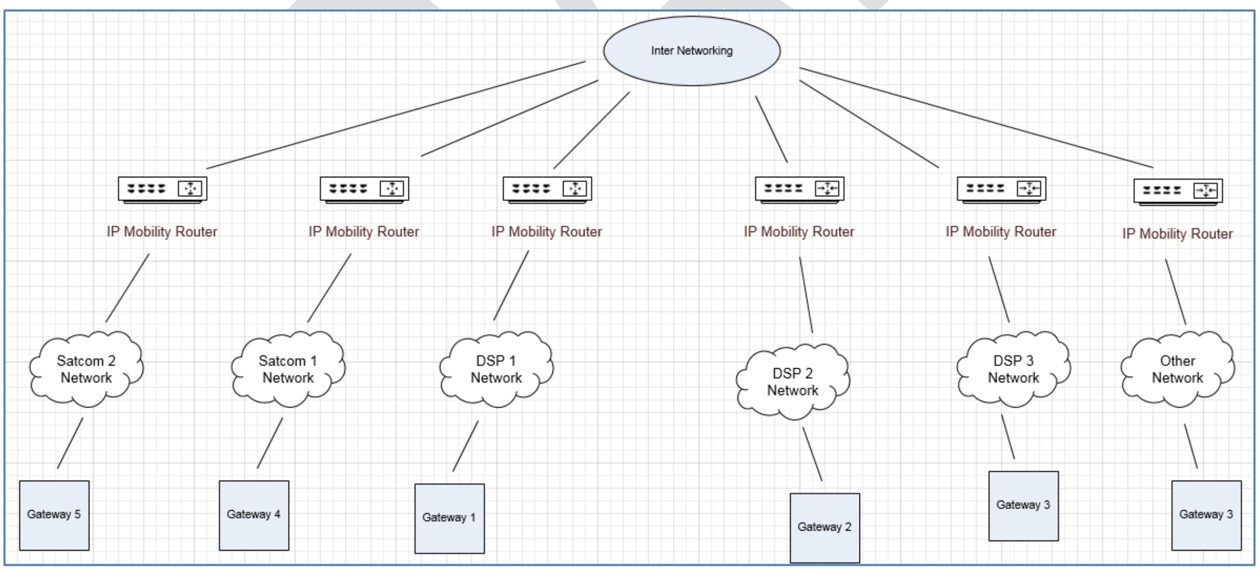


Figure 3-3 – Inter Networking Concept

Since triple stack (ATN/OSI, ATN/IPS and ACARS) aircraft are not envisaged, accommodation needs to be provided on the ground. The IPS Gateway is the key part of the transition path to ATN/IPS by providing protocol conversions, supporting the following communications modes:

- ATN/IPS aircraft < -- > ATN/IPS end system
- ATN/IPS aircraft < -- > Legacy facility (ATN/OSI, ACARS)
- Legacy aircraft (ATN/OSI, ACARS) < -- > ATN/IPS end system

3.1 IPS Aircraft – IPS Ground System

For IPS Aircraft to IPS Ground System Messaging, illustrated in Figure 3-4, the IPS Gateway is used to manage the message flow without interpreting or reformatting the message data. The general requirements for the IPS Gateway are:

- Aircraft authentication
- Maintaining key aircraft information for each authentication event
- Maintain session information
- Managing sequence numbers
- Supporting IP name lookup
- Providing Compression, Segmentation and Reassembly functionality
- Providing message integrity checking
- Supporting multilink and mobility

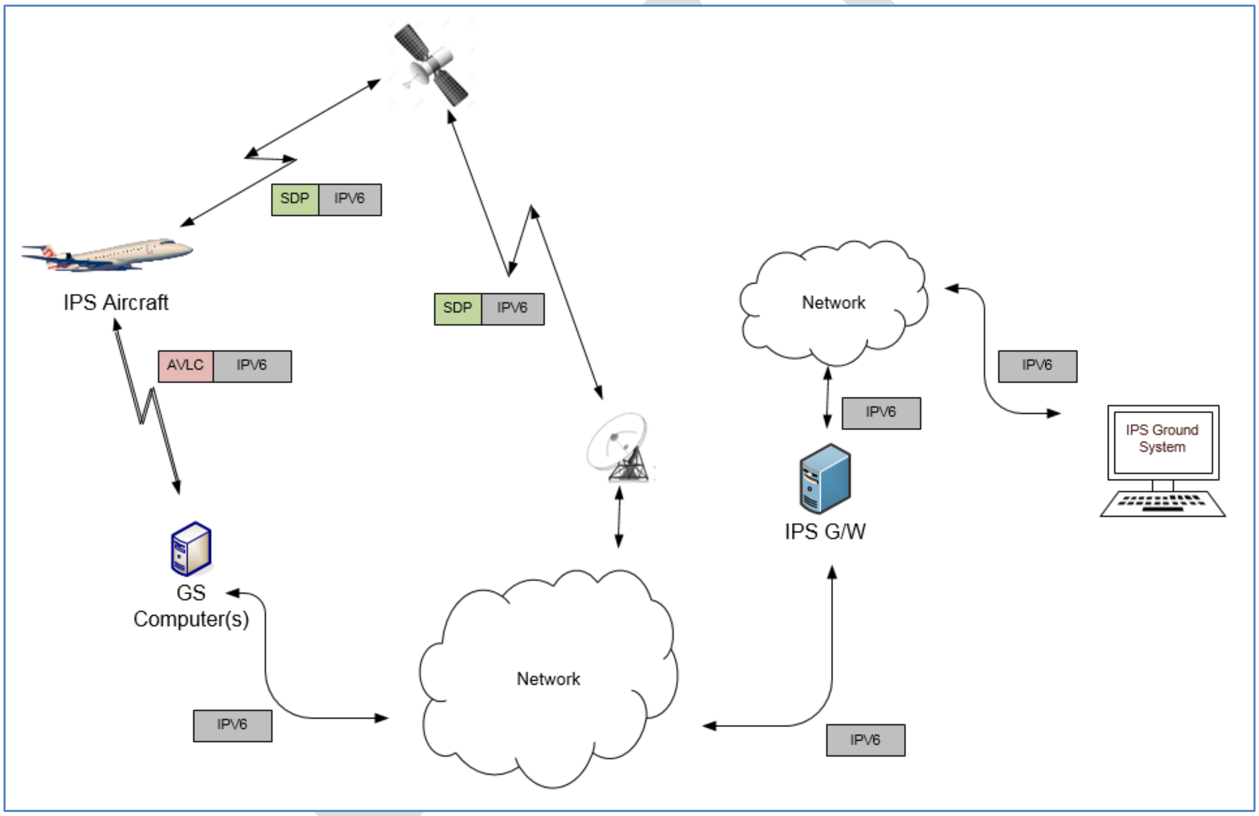


Figure 3-4 - DL Flow to/from IPS Ground System

3.2 IPS Aircraft – A620 Host

Figure 3-5 shows the communications path between the IPS Aircraft and an ARINC 620 (A620) Host. The DS peers are the IPS Aircraft (avionics) and the IPS Gateway. For IPS Aircraft to A620 Host data exchange the IPS Gateway provides an IP termination point and supports the IP - A620 conversion for messages to/from the A620 Host System.

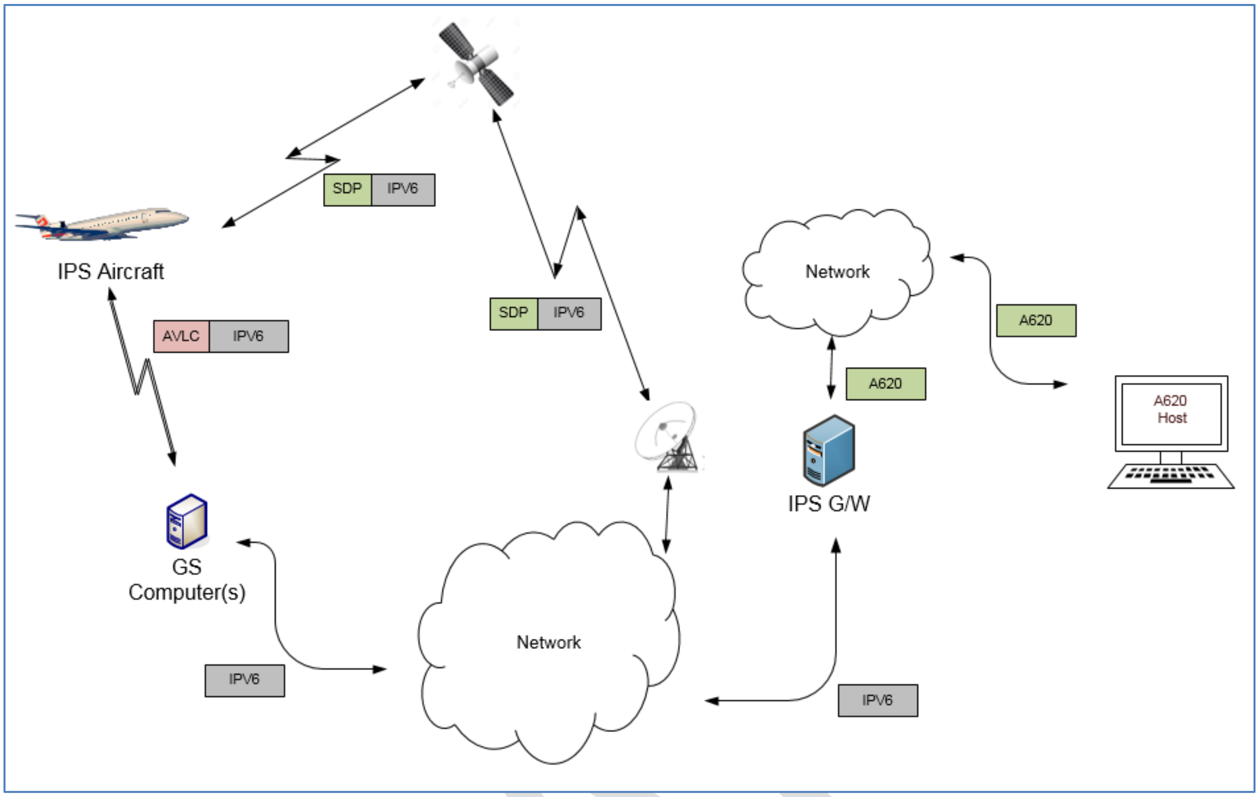


Figure 3-5 - DL Flow to/from A620 Host

The following are the general requirements for the IPS Gateway for IPS Aircraft to A620 Host communications which are similar to the general requirements for IPS Aircraft to IPS Ground System:

- Aircraft authentication
- Maintaining key aircraft information for each authentication event
- Maintain session information
- Managing sequence numbers
- Providing Compression, Segmentation and Reassembly functionality
- Converting the IPS downlink message into an A620 message and sending to A620 Host
- Generation of IPS uplink from A620 input message
- Providing message integrity checking
- Providing Message Assurance response (as requested) to A620 Host
- Supporting multilink and mobility

3.3 IPS Aircraft – ATN/OSI End System

Figure 3-6 shows the communications path between the IPS Aircraft and an ATN/OSI End System. The DS peers are the IPS Aircraft (avionics) and the IPS Gateway. For IPS Aircraft to ATN/OSI End System data exchange the IPS Gateway:

- provides an IP termination point
- provides the ATNPKT - CLNP conversion for messages to/from the ATN/OSI End System
- manages the ATN/OSI connection with the ATN/OSI End System

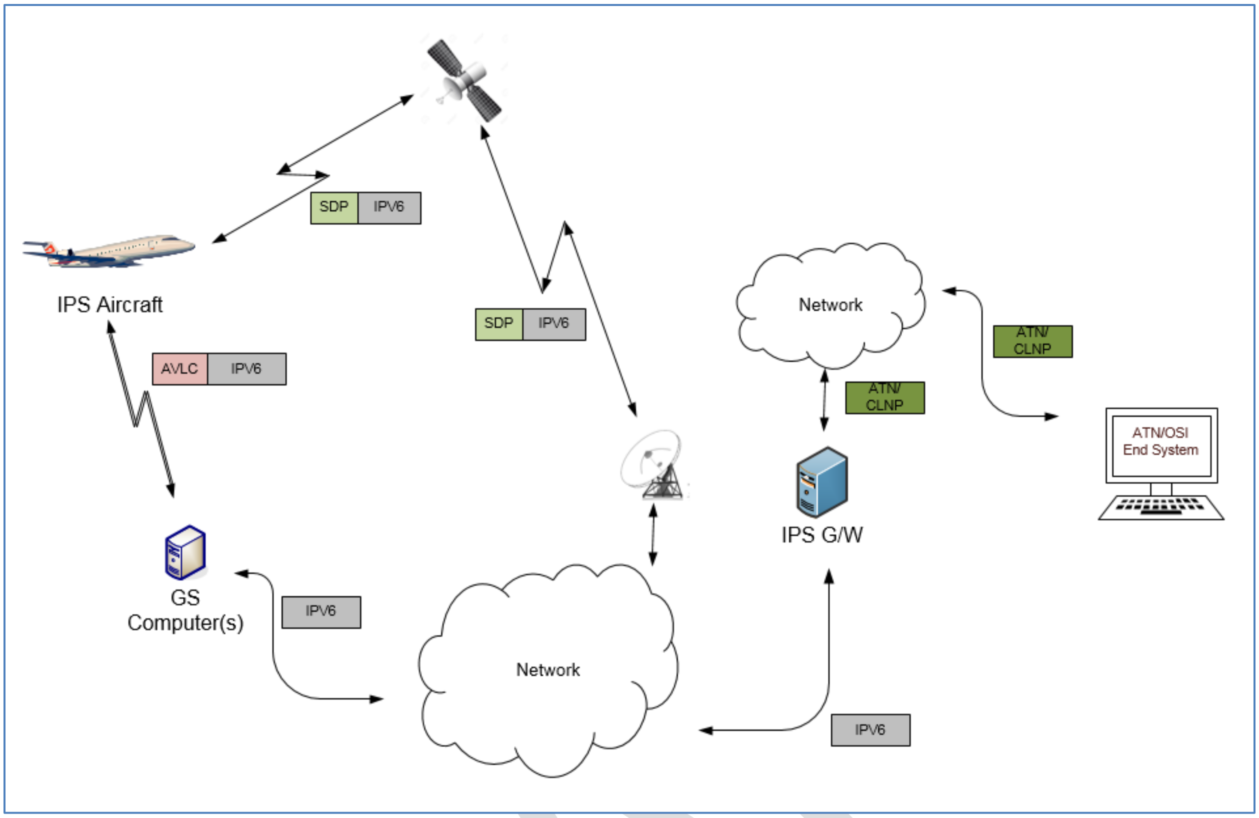


Figure 3-6 - DL Flow to/from ATN/OSI End System

The following are the general requirements for the IPS Gateway for IPS Aircraft to ATN/OSI End System communications which are similar to the general requirements for IPS Aircraft to A620 Host:

- Aircraft authentication
- Maintaining key aircraft information for each authentication event
- Maintain session information
- Managing sequence numbers
- Providing Compression, Segmentation and Reassembly functionality
- Converting the IPS downlink message into an ATN/OSI message and sending to ATN/OSI End System
- Generation of IPS uplink from ATN/OSI input message
- Providing message integrity checking
- Supporting multilink and mobility

3.4 IPS Ground System – Legacy (ACARS, ATN/OSI) Aircraft

Figure 3-2 shows the communications path between an ACARS Aircraft and an IPS Ground System. The DS peers are the IPS Ground System and the IPS Gateway. For an ACARS Aircraft communicating with a facility that only supports ATN/IPS, the IPS Gateway provides an IP termination point and supports the IP - ACARS conversion for messages to/from the ATN/IPS Ground System. For an ATN/OSI Aircraft communicating with a facility that only supports ATN/IPS, the IPS Gateway provides an IP termination point and supports the IP – ATN/OSI conversion for messages to/from the ATN/IPS Ground System.

The following are the general requirements for the IPS Gateway for IPS Ground System to Legacy (ACARS, ATN/OSI) Aircraft communications:

- Maintain session information
- Determining the appropriate message path and addressing
- Maintaining key aircraft information for each communications session
- Managing sequence numbers
- Providing Compression, Segmentation and Reassembly functionality
- Converting the IPS input message into an ACARS uplink message and sending to ACARS aircraft
- Generation of IPS output message from an ACARS downlink message
- Converting the IPS input message into an ATN/OSI uplink message and sending to ATN/OSI aircraft
- Generation of IPS output message from an ATN/OSI downlink message
- Providing message integrity checking
- Providing Message Assurance response (as requested) to the aircraft
- Supporting multilink and mobility

4 Media Specific Details

The IPS gateway will use all media available, prioritizing based on airline or ANSP preference. Each media has its own specific encapsulation of the data being transmitted. This section identifies the relevant details for both IP and non-IP media.

4.1 SATCOM

Transporting IPv6 data using satellite communications (SATCOM) is done in using IPv6 packets carried over the satellite SubNetwork Protocol Data Units (SNPDUs). The type of Satcom data is specified by ……

content to be developed

4.2 VDL Mode 2

Transporting IPv6 data using connectionless VDL Mode 2 involves including the IPS data within an AVLC frame.

> Note: Connectionless VDL Mode 2 operation is a requirement for IPS over VDL Mode 2. Details of connectionless VDL Mode 2 are being defined by the DLK AEEC committee. The details include the definition of a new protocol (the 'Orange' protocol) to provide the link layer segmentation. The pertinent details are included here for completeness.

This is illustrated in Figure 4-1 which shows the AVLC frame and Figure 4-2 which shows the breakdown of the information field inside the AVLC frame. Additional information on the AVLC frame is in in the **Manual on VHF Digital Link (VDL) Mode 2**, ICAO Doc 9776, 2nd edition.

Flag	Address	Link Control	Information Field	FCS	Flag
1	8	1	n (max 240)	2	1

Figure 4-1 – AVLC Packet

The AVLC information field for IPS consists of:

- Initial Protocol Identifier (IPI)
- Orange Protocol header
- Upper layer data (segmented as needed for max AVLC frame size)
- Message Integrity Check (MIC)

The 'Orange' protocol is a new protocol defined to provide link layer segmentation in VDL mode 2. The orange protocol is needed since the maximum IPv6 packet size is larger than the optimal efficiency size of the AVLC packet. The protocol provides for segmentation and for high water acknowledgement for segmented messages. The orange protocol header with message is shown in Figure 4-2.

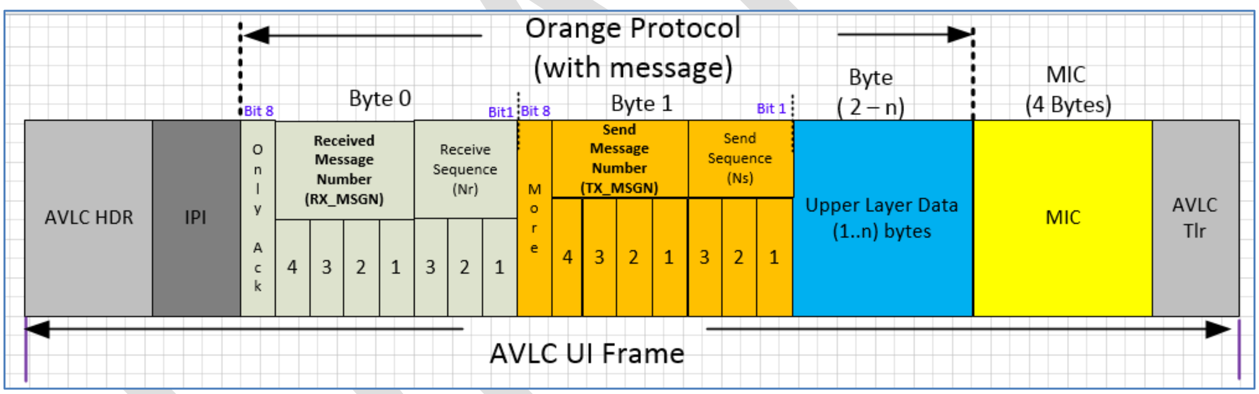


Figure 4-2 – Orange protocol header

The following are details of the AVLC UI Frame with segmentation support:

- IPS only uses UI frame
- For downlink Source, the AVLC address contains the aircraft address and Destination address contains the any valid ground address of the target DSP
- Layer 2 segmentation protocol is added to support RFC 8200 minimum MTU limit of 1280 octets
- Only Ack bit indicates if this is an acknowledgement only (if set then byte 1 and data bytes are not present).
- Send Message Number (TX_MSGN): used for all messages (single and multi-segment), starts from 0 going to 15 and continually cycled through. When the message is segmented the message number indicates each segment that belongs to the specific message.
- Sequence Number (Ns): Segment sequence number of this segment
- More bit indicates if another segment belongs to the current message

- When message is not segmented, the more flag is not set and the sequence number is 0 and an Ack is not required
- Receive Msg Number (RX_MSGN) indicates the last message number received
- Receive Sequence Number (Nr): latest received sequence number of a segment (Nr -1 segment is being acked) for a given message (RX_MSGN)
- A Data segment always acknowledges the last received segment, whether the latter be a single or a multi segment message. Thus a single segment message is acknowledged only if no other segment is sent before receiving a segment and if the next received segment is a Data segment
- MIC is calculated and authenticated for each frame after the mutual authentication is done. For the DTLS handshake MIC is not included
- MIC includes AVLC header as well as last octet of user data
- Retransmit timer at orange protocol layer is 3 seconds, up to 3 attempts only for fragmented messages (single seg flag set to 0) based on high water mark ACK.
- If no acks are received at Layer 2 then retransmission will be handled by the upper layer(s)

Figure 4-3 illustrates how the IPv6 packet is segmented and Figure 4-4 shows and example of this segmentation.

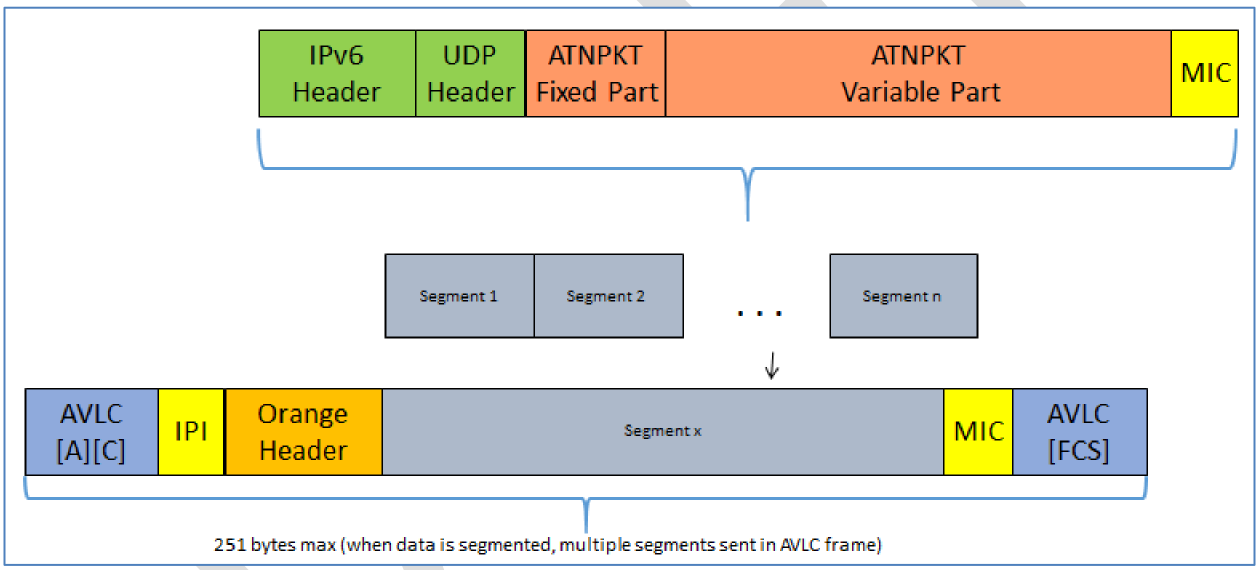


Figure 4-3 – Link layer segmentation for IPS

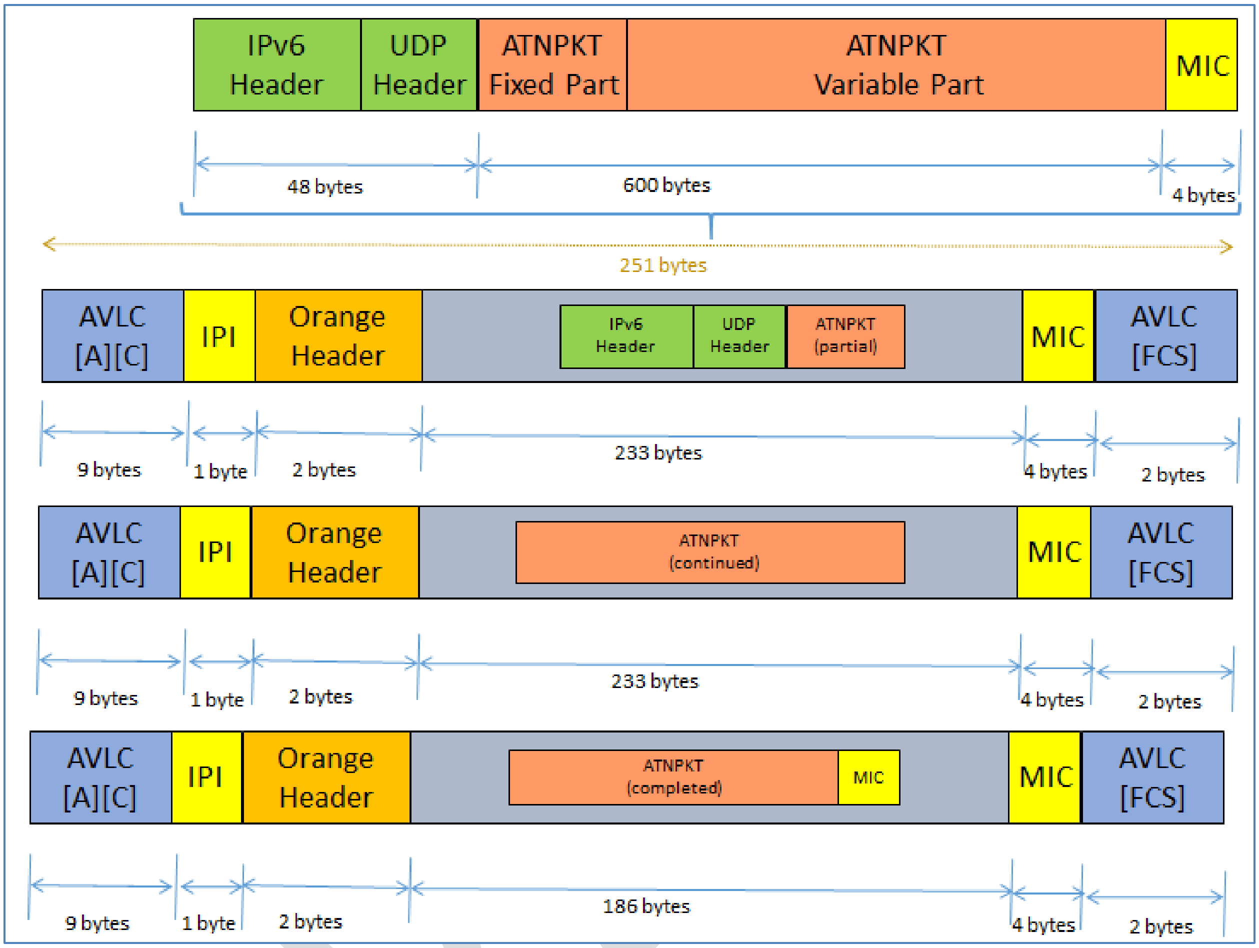


Figure 4-4 – Orange protocol segmentation example

4.3 IPS Service Availability

4.3.1 VDL Mode 2

To advertise IPS service, the ground station information frame (GSIF) will be modified by incorporating two additional parameters to indicate IPS availability, see section 7.1.1 for details. IPS Aircraft will use the GSIF as well as the AVLC header to determine the service provider and IPS availability.

4.3.2 Satcom

The availability of IPS service over Satcom service provider / link is determined by the avionics through a route solicitation message after establishment of the Satcom link.

5 Interface Characteristics

The key interface characteristics that the IPS Gateway is dealing with are:

- The IPS Protocol Stack supporting a number of different applications
- Authentication to access IPS service
- Message Integrity Checking for assurance of message delivery

- Key management to support certificate management
- IPS Information Message to support delivery options
- IP lookup service to provide name resolution
- Message encapsulation detailing contents of:
    - IPv6 packet
    - UDP packet
    - ATNPKT
- Error detection

5.1 IPS Protocol Stack

With the individual protocol layer involved it is useful to step back and understand how each layer interacts with each other to provide the IPS Service. Below is the IPS Protocol Stack depiction.

IPS Stack							
Layer							
Application	Native IP	B1/B2	FANS/AOC				
Presentation	Application	Adaptation	Convergance Function	name lookup	Authentication	Information Message	Key Management
Session		ATN PKT		Key Selector 0x0C	Key Selector 0x0A	Key Selector 0x0B	Key Selector 0x3X
Transport	UDP or TCP	UDP		UDP Port (5908)			
Network	IPV6						
Media Access	Air to Ground Media						

Figure 5-1 - IPS Protocol Stack

The ATNPKT as defined in ICAO Doc. 9896 [1] is the basic unit in IPS communications for existing applications, while future applications will most likely be native IP applications.

5.2 IPS Protocol Build-up

There are three modes to consider for the protocol build-up:

- Session establishment message exchange
- Session management message exchange
- Application message exchange

The Initial Protocol Identifier (IPI) is used to identify the presence of IPS data and the UDP port number is used to describe the type of IPS data. Additionally data on the authentication port (5908) has a key tag to further identify the type of message.

> Note: There is an ICAO requirement to provide ATC services by default. How this requirement is addressed by IPS is a policy issue. From the viewpoint of the IPS gateway, this could be handled such that if an aircraft has a valid key then the message can be delivered.

The specifics of the individual components of the protocol build-up are detailed further on in the document.

5.2.1 Session Establishment – IP Based Datalink

The protocol build-up for session establishment (authentication) is shown for IP-based communications (example of this is shown in Figure 5-2). Session establishment shall utilize UDP port 5908. Port 5908 is reserved for specific messages (authentication, post authentication message, key management, IPS information, and IP lookup); with the type of message being defined by the first byte (key tag) of the UDP data field. For authentication, the key tag field value must be 0x0A. Prior to authentication, UDP port 5908 will be the only available port. Note that a message integrity check (MIC) field [see section 5.4 for details] is not present during authentication because the session key has not been established. No other key tags will be accepted by the gateway prior to authentication.

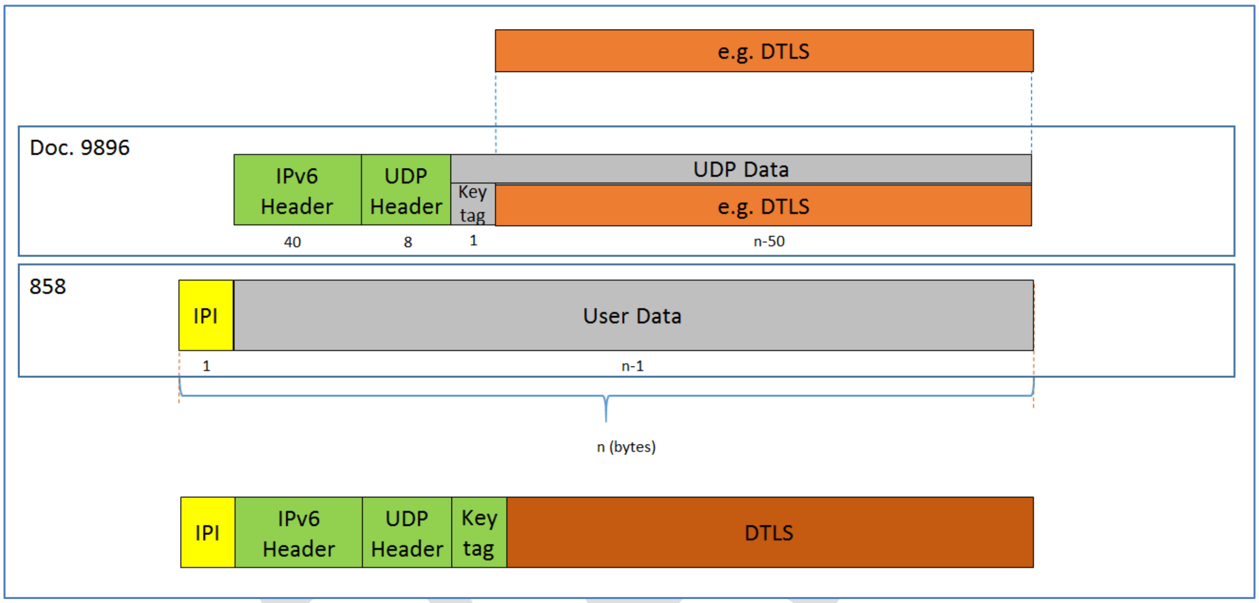


Figure 5-2 – IP-based Datalink (e.g. SATCOM) Session Establishment

5.2.2 Session Establishment – AVLC Based Datalink

AVLC unlike most other IP based media does not have media access layer security built in. To augment AVLC with security the AVLC layer will be used for authentication of the aircraft and the security parameters generated will be used for both the AVLC layer and the IPS layer.

The protocol build-up for session establishment (authentication) is shown for AVLC-based communications. For authentication, the key tag field value must be 0x0A. Prior to authentication, there will be no open UDP ports, only AVLC. Note that a message integrity check (MIC) field is not present during authentication because the session key has not been established. No other key tags will be accepted by the gateway prior to authentication.

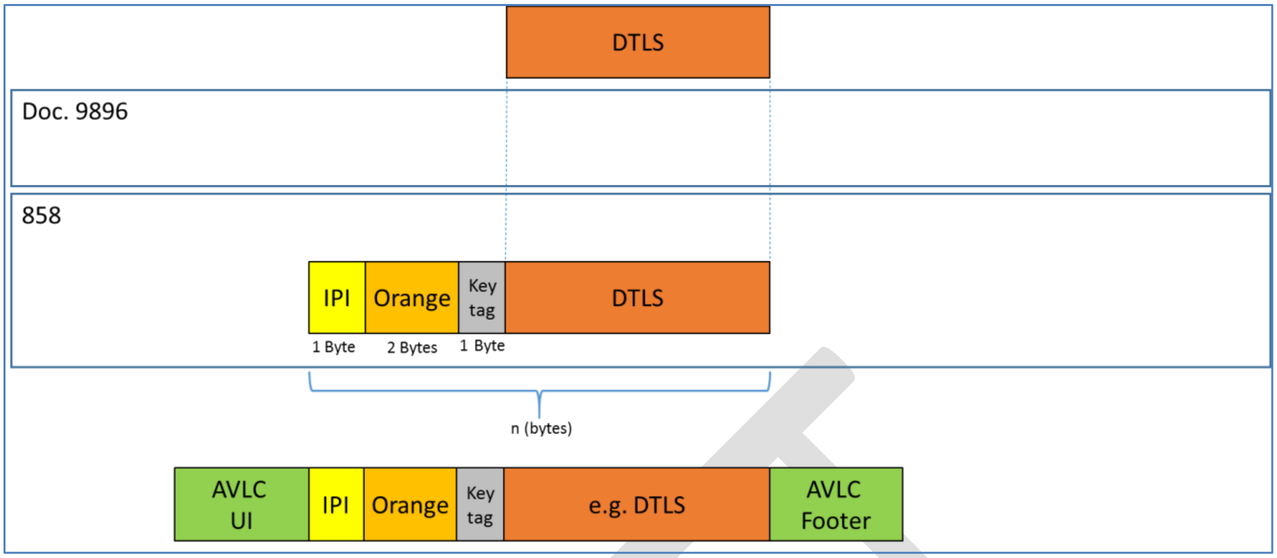


Figure 5-3 – AVLC-based Datalink (e.g., VDLM2) - Session Establishment

5.2.3 Session Management - All Media

This message exchange covers all other messages sent over UDP port 5908. All of these messages are DTLS encapsulated messages, with the specific type of message type being identified by the key tag. The format is the same as session establishment except that it includes MIC field since authentication has been completed.

It should be noted that all messages on UDP Port 5908 use the DTLS header. Furthermore all messages that use a DTLS header, post authentication, will be encrypted. Responses to simple IP lookups and post authentication messages will also be encrypted.

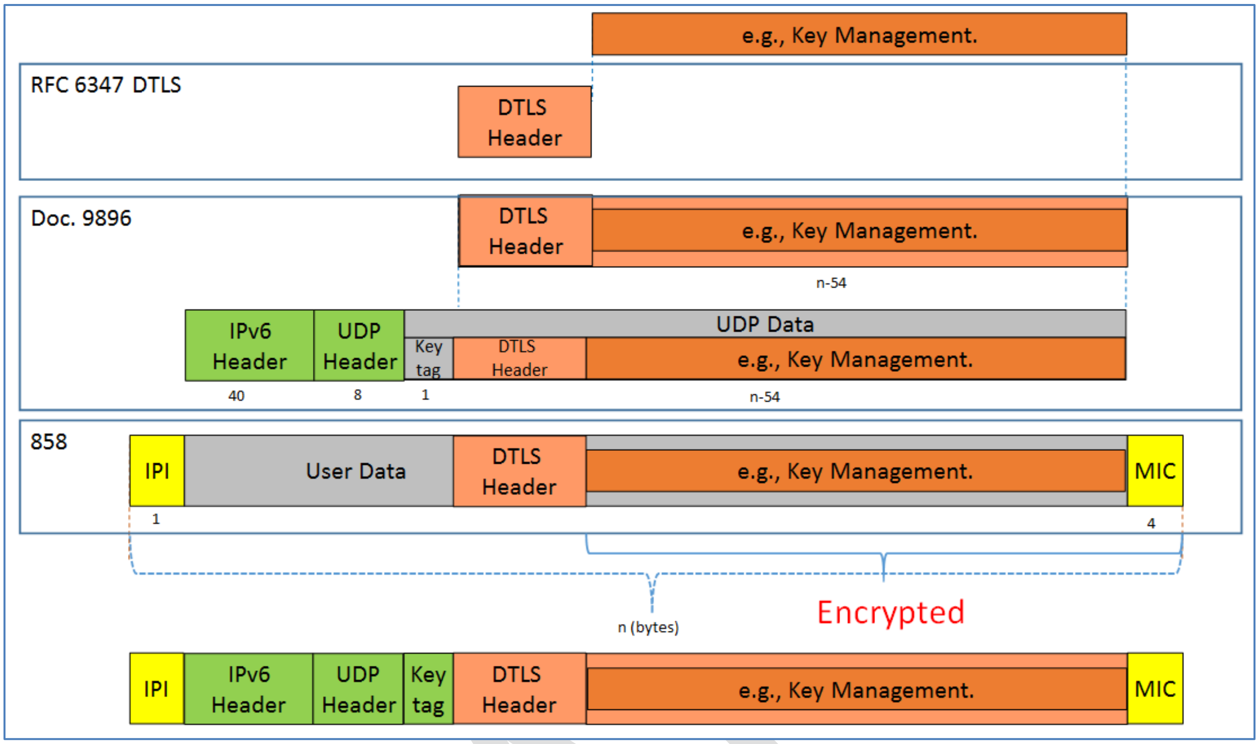


Figure 5-4 – IP-based Datalink (e.g. SATCOM) Session Management

5.2.4 Post Authentication Message – All Media

After the DTLS session is established, the avionics will use the standard IP IPS format found in Section 5.2.3 Session Management - All Media, to send an additional DTLS application packet. This application packet will use UDP port 5908 with key tag 0x0A. The DTLS header will indicate this is application traffic. The Post Authentication Message will contain the aircraft's fixed nomadic IP address, ATN address, tail number, Flight ID and a random start message number for downlinks. The server will respond with another random start message number for uplinks. After the post authentication message exchange has been completed, anything on port 5908 with a key tag of 0x0A will be a TLS Alert message and/or connection maintenance traffic. All connection maintenance and TLS alert messages will use the same format recorded in section 5.2.3 above. The purpose of the Post Authentication message is to allow IPS conversions to ATN/OSI or ACARS as necessary and to setup a random sequence number for MIC generation. See Figure 5-5 for the protocol buildup for Post Authentication Messages.

Aircraft Fixed Nomadic IP Address 16 Bytes	Aircraft ATN/OSI Address 20 Bytes	Tail # Length (1 nibble)	Flight ID Length (1 nibble)	Tail Number	Flight ID	Random Message Number Length for MIC generation 6 Bytes
		Length 1 Byte				

Figure 5-5 - Post Authentication Aircraft to Gateway Message Format

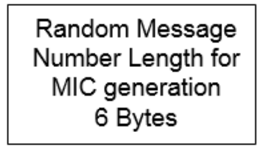


Figure 5-6 - Post Authentication Gateway to Aircraft Message Format

5.2.5 Aircraft Information and IP lookup Message

The IPS enabled avionics will periodically report information to the local gateway to maintain the DTLS connection using UDP port 5908 Key Tag 0x0B. The avionics can also query the gateway for end system information using a simplified IP lookup message using UDP port 5908 Key tag 0x0C. See Sections 5.6 IPS Information Message and Section 5.7 IP Lookup Message for more information. All messages on UDP port 5908 will use the encryption method negotiated during DTLS logon.

5.2.6 Application Messages

The application messages are sent on specific UDP ports other than port 5908. These messages do not require the key tag used for port 5908 messages. Application messages will not be encrypted, but will have a MIC to ensure message integrity while in transit. Examples of the protocol build-up are shown below for IP-based.

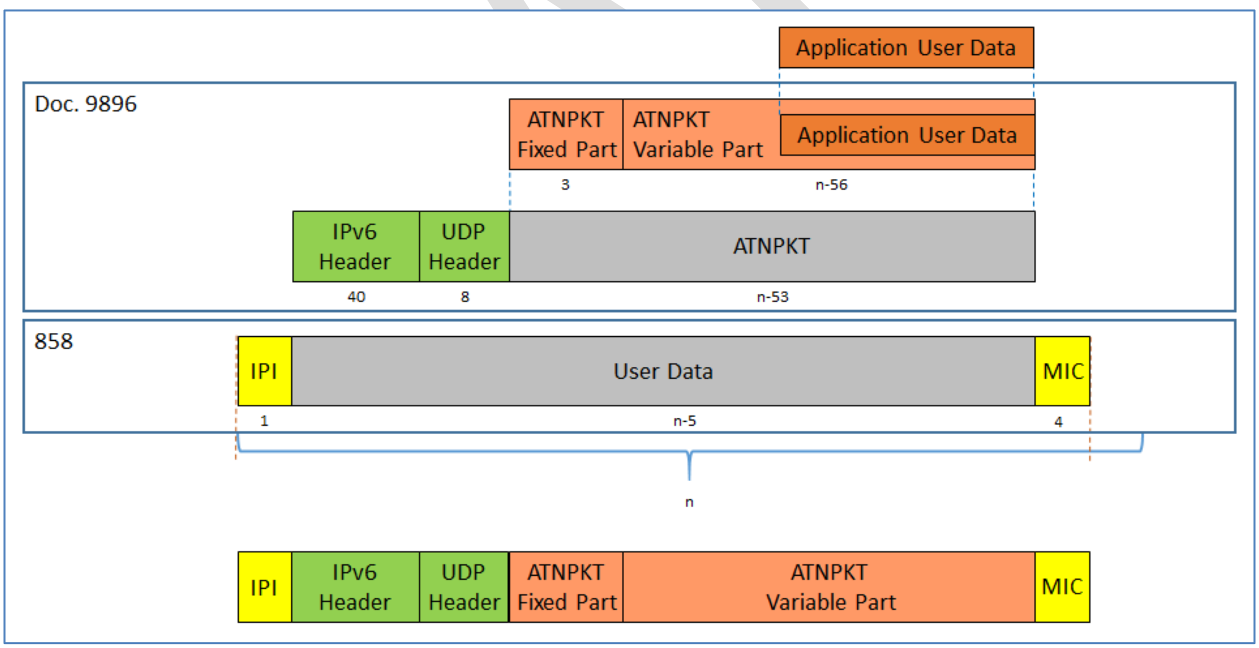


Figure 5-7 - IP-based Datalink (e.g. SATCOM) Application Message

5.2.7 Initial Protocol Identifier

The Initial Protocol Identifier (IPI) is a 1 byte field used to identify the presence of IPv6 data. IPI 0x8E value is identified for IPv6 per ISO/IEC TR 9577 1999 edition appendix C. The ground adds the IPI before the IPv6 header for all uplink messages.

For downlink messages, the ground station (VHF or Satcom) examines the IPI and routes IPv6 messages to the IPS Gateway. The IPI will be included as a part of the message in transmission to the IPS Gateway.

5.2.8 Port 5908 Key Tag Values

The port 5908 specific messages are defined by the first byte (the port 5908 key tag field) of the data field. The following are the messages and their codes:

Key	Message
0x0A	Authentication
0x0B	IPS Information
0x0C	IP Lookup
0x30 – 0x3F	Key Management

Table 5-1 - Port 5908 Key Tag Values

The messages are defined in the respective sections.

5.3 Authentication

The first step for an IPS aircraft communicating with any entity is to authenticate with the IPS Gateway. Authentication is initiated by the aircraft. The aircraft authentication is with the IPS Gateway so that the overall authentication checking and key management is simplified by the aircraft not having to authenticate with each IPS end system individually (this does not preclude end system applications security functions). DTLS will be implemented for authentication in order to protect the subnetwork that is being used.

The exchanging of PKI keys in DER format while efficient, will likely lead to multiple fragments to be transmitted across the communications media, especially when the media has a small MTU size.

5.3.1 IP Based Authentication

IP based communication media is assumed to have a media layer securing method. For this reason and for consistency with all other IPS traffic, DTLS will be transmitted on IP based media.

The transmission of DTLS in IP packet for authentication is illustrated in the following diagram and is detailed further in this document.

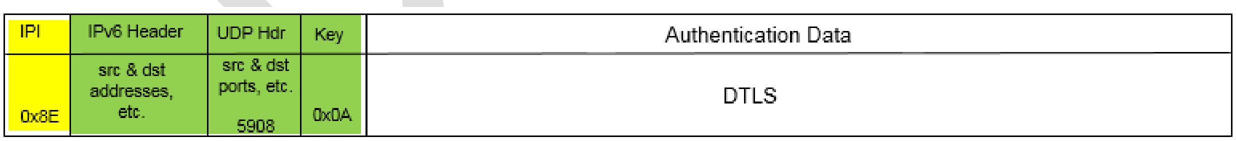


Figure 5-8 – Authentication packet on IP based media

The IPS Gateway will not have any UDP ports other than 5908 with a key tag of 0x0A available for unauthenticated aircraft over IP based media.

All messages in the authentication sequence will have UDP port 5908 and the first byte of the UDP data field will have a key tag value of 0x0A preceding the authentication data. During authentication, the IP packet carries the DTLS data in the user data After the DTLS Logon handshaking is complete the avionics will send a Post Authentication Message with the aircraft's IP address, tail number and Flight ID and a random sequence number. The Gateway will respond with a random sequence number. After authentication has been completed, anything on port 5908 with a key tag of 0x0A will be TLS Alert messages and/or connection maintenance traffic.

5.3.2 AVLC Based Authentication

Since AVLC based media does not possess a media layer security method. AVLC will be used to authenticate the aircraft prior to the initiation of IPS traffic. The security parameters will be reused for both the AVLC and ATN/IPS layers for the same service provider so that multiple key exchanges do not need to be performed with the same service provider.

> Note: Authentication at the AVLC layer (sub-network layer) is not specifically IPS functionality, however it is included in the document since VDL Mode2 is not secured like other IPS media and the addition of securing VDL Mode2 is specifically for the support of IPS.

The use of the AVLC layer for authentication is illustrated in the following diagram and is detailed further in this section.

IPI	Orange	Key Tag	Authentication Data
0x8E	Message # Ack #	0x0A	DTLS

Figure 5-9 - DTLS Authentication on AVLC based media

The IPS Gateway will not have any key tags other than 0x0A available for unauthenticated aircraft over AVLC based media.

All messages in the authentication sequence will have a key tag value of 0x0A preceding the DTLS application packet. During authentication, AVLC carries the DTLS data in the authentication data.

5.3.3 Post Authentication Message

In order to provide IPS with enough random values to ensure data integrity and to allow IPS to ATN/OSI and ACARS translations additional pieces of information must be exchanged between the aircraft and the gateway. This additional information is carried in the post-authentication message, the content is shown below.

Field Name	Length in Bytes	Reason for exchange
Aircraft Fixed Nomadic IP Address	16 Bytes length of an IPv6 address	Gateway needs IPv6 address to exchange IPS information. This is especially true when logon is via AVLC.

Field Name	Length in Bytes	Reason for exchange
Aircraft ATN/OSI Address	20 Bytes	Gateway needs this for ATN translation
Length in Bytes	1 Byte	Contains the Tail number length (1st nibble) and Flight ID length (2nd nibble), both can be variable. This allows for 0 to 15 characters in both
Tail Number	Variable – but must match the tail # length value in the Length in Bytes field (1st nibble)	Tail numbers are needed for ACARS conversions.
Flight ID	Variable – but must match the flight ID length value in the Length in Bytes field (2nd nibble)	Flight ID is required for ACARS Conversions.
Random Message number for downlinks	6 Bytes	Random message number for MIC generation. The value will be the sequence value for this message. Each additional transmitted message from this point will increment the value by 1. Value rolls over when necessary from 0xFF FF FF FF FF FF to 0x00 00 00 00 00 00.

5.3.4 DTLS Login

DTLS is an enhancement on TLS for secure UDP connections. The DTLS Protocol is recorded in RFC 6347.

There are 6 flights to a DTLS login, shown below.

```
Client                                                Server
------                                                ------

ClientHello             -------->                                Flight 1

                        <-------      HelloVerifyRequest         Flight 2

ClientHello             -------->                                Flight 3

                                             ServerHello    \
                                            Certificate*     \
                                      ServerKeyExchange*      Flight 4
                                     CertificateRequest*     /
                        <--------        ServerHelloDone    /

Certificate*                                                \
ClientKeyExchange                                            \
CertificateVerify*                                            Flight 5
[ChangeCipherSpec]                                           /
Finished                -------->                           /

                                      [ChangeCipherSpec]    \ Flight 6
                        <--------               Finished    /
```

Figure 5-10 – DTLS Login Flights

During the initial rollout of IPS the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 methods will be used. SHA256 is intended for legacy systems while SHA384 will be the main requirement. To facilitate maximizing the utilization of packets, the Deflate compression option already built into DTLS will be used.

Field	Value
Keys	ECDSA
Diffie Hellman	ECDHE
Elliptic Curve	secp256r1, secp384r1
Encryption	AES 128 GCM, AES 256 GCM
Hash	SHA 256 or SHA 384
Compression	Deflate

Table 5-2 – DTLS Session Parameters

5.3.5 ECDSA Keys

ECDSA keys pairs will be provided by the primary service provider for each aircraft subscribed to the IPS service. The keys will be signed by the primary service provider’s own or designates CA key and be verifiable by any entity possessing the service provider’s or designates public key. (A trusted companion service provider) For example: If ARINC was the service provider for American Airlines (AA) and a AA aircraft was operating in China, it would be able to authenticate with ADCC if ADCC possessed a copy of ARINC's or designate's Root Certificate.

Each aircraft will receive two public certificates and two private keys. The public certificate is used for authentication with the IPS Gateway(s) and the private key is kept secret with the aircraft. Each undoes the encryption of the other and must work in pairs to establish and maintain secured connections.

To minimize the size of the public keys, they will be encoded in X.509 certificate DER format. The private keys are never transmitted in an authentication exchange. Each key's valid dates will correspond with existing contract dates plus a grace period if applicable between the airline and the primary service provider.

In the event that an aircraft key is compromised, the aircraft will have a one-time-use back-up key that can be used for authentication. This back-up key will only be valid on the primary service provider's network to facilitate upload of replacement keys. After using a back-up certificate, if new keys are not uploaded the airline must data-load new certificates and keys. The Avionics will support a way to replace the existing public keys and certificates using both a physical media and also over the air. See Section 5.5 Key Management for more information on the replacement.

5.3.5.1 X.509 Certificate Parameters for aircraft

Each X.509 certificate has parameters that identify the valid user of the certificate. Certificates will include the aircraft's public key, a signed hash using the service provider's private key, and the following additional information.

Field	**Value**	**Example Using Delta Airlines with tail N123456 and Rockwell Collins ARINC North America**
Country Name [AU]:	2 letter country code of airline host	US
State or Province Name	Full Province or state name of airline host	Georgia
Locality Name	City of airline host	Atlanta
Organization Name	issuing airline	Delta Airlines
Organizational Unit Name	ICAO Airline Designator	DAL
Common Name	Tail Number.aircraft Type.ICAO_Code.Service	N12345.A380.DAL.IPS
Email Address []:	PKI Sponsor E-mail	PKI@delta.com
A challenge password []:		[None]
An optional company name		[None]
Issuer	Service providers information	Rockwell Collins ARINC NA
Validity	Dates and time period key is valid	[Contract specific]

Table 5-3 – X.509 Certificate Parameters for Aircraft

5.3.5.2 X.509 Certificate Parameters for non-aircraft

Maintenance devices may require certificates, which give permission for the generation of Certificate Signing Requests (CSR) for a particular airline and primary service provider. Having Certificates on the maintenance device(s) would allow that device to make CSRs for one particular airline, and service provider. Devices could then be kept secured to ensure that only authorized people and avionics receive valid certificates thus preventing unauthorized people from installing billable certificates on unauthorized avionics. The Certificate Policy and Certificate Practice Statement will expand on this concept further.

5.3.5.3 X.509 Certificate List

It shall be the responsibility of each service provider or designate to maintain a service key directory of X.509 certificates for all aircraft for which they are the primary service provider. It also shall be the responsibility of each primary service provider to maintain a valid public CA X.509 certificate in DER encoding with all other trusted companion service providers for which a trusted relationship is established.

5.3.5.4 Service Provider Trusted Relationships

Each service provider shall have the option to enter into roaming agreements with other service providers. These trusted roaming providers shall be called trusted companion service providers. If a companion service provider has a valid trust operating agreement then an exchange of public root CA certificates between providers or the establishing of a trust bridge will allow aircraft to utilize the companion network while in transit. Certificates shall be encoded in DER format.

5.3.5.4.1 Aircraft Roaming and Keys

It is up to each airline to determine which service providers they wish to allow their aircraft to connect with if any. This is bounded by the trust relationships between service providers. If a set of trusted service providers are desired, the aircraft avionics should be loaded with server certificates for each trusted service provider. The aircraft will then be able to authenticate the IPS Gateway and the IPS Gateway will be able to authenticate the aircraft.

By way of example if ADCC and SITA enter into a trusted relationship: Aircraft that have ADCC as their primary service provider will have the option to roam onto the SITA network, if the aircraft is equipped with SITA's gateway server certificate. Without this trusted relationship then aircraft will not be able to roam onto the other's network even if the avionics contained the SITA certificate. In this case the SITA IPS Gateway would reject aircraft presenting a certificate signed by ADCC.

Avionics should disable IPS if they do not at a minimum have an Aircraft Public Certificate, Aircraft Private Key, Primary Service Provider's Public Server Certificate and a Primary Service Provider's CA Certificate(s). Having a Onetime Use key and certificate is highly encouraged to recover aircraft whose keys expired while out of the primary service provider's area.

Assuming the aircraft is roaming onto another service provider's network area. The following truth table depicts whether the aircraft will accept or reject the Trusted Companion service provider's server key.

Service Provider Key store / **Aircraft key store**	Has Trusted Companion Public Certificate	Does not Have Trusted Companion Public Certificate for Aircraft's Primary Service Provider.
Has Secondary Service Provider Server Key	Server Key accepted – Logon continues	Ground issues a DTLS Alert message and discontinues the connection.
Does not have new Service Provider's server Key	Aircraft discontinues communication with this service provider. Aircraft may issue a DTLS Alert message	Ground issues a DTLS Alert message and discontinues the connection.

Figure 5-11 - Avionics Login Results Table (Trusted Service Provider)

Service Provider Key store / **Aircraft key store**	Has Primary Service Provider Server Public Certificate
Has primary service provider Server Key	Server Key accepted – Logon continues
Does not have primary service provider's server key	Misconfigured Aircraft cannot authenticate with Primary Service Provider

Figure 5-12 - Truth Table Logon Results (Primary Service Provider)

5.3.5.5 Certificate Revocation List (CRL)

Each primary service provider shall maintain a certificate revocation list. Any key generated by the primary service provider that is later compromised, other than by expiration shall be listed in a certificate revocation list until the certificate expires. This list is to be shared no less than daily with all trusted companion service providers, even if no changes are recorded. It is recommended that an encrypted method be established for sharing these lists.

One time use keys may be distributed to trusted companion service providers as a Certificate Revocation list as well. See Section 5.5.3.5 on one-time use keys for more information.

Online Certificate Status protocol is recommended between trusted service companions but not required. It will be up to each service provider to setup how it wants to interact with other trusted service providers. OSCP availability does not alleviate the need to publish CRLs to trusted companion service providers. OSCP is seen as a useful resource but not impervious to outages due to network connectivity issues and server hardware failures.

5.3.6 Diffie-Hellman

The Elliptic Curve Diffie-Hellman Ephemeral key generation function allows for dynamic negotiation of Diffie-Hellman parameters at the time of authentication. Diffie-Hellman is a secured key generation scheme that allows each participant in a communication channel to generate the same master secret key without sending the actual key over an insecure link. This is done by exchanging a Pre-Master secret key that will guide the other participant in the communication channel to calculate a Master-Secret Key. The Elliptic Curve Diffie-Hellman Ephemeral key (ECDHE) is generated along the Elliptic curve specified during the DTLS authentication. For a more in-depth discussion on the protocol please reference RFC-4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).

5.3.7 Elliptic Curves

To simplify the authentication exchange and session key generation a named pre-configured elliptic curve generally accepted by the security community will be used. The curves supported will be secp256r1 (for legacy systems) and secp384r1 (the primary requirement).

5.3.8 Encryption

AES 256 with GCM mode will be used for encrypting all message traffic on UDP port 5908 with a key tag of 0x0A, or 0x3X after authentication is complete and during any key maintenance operations. All other traffic on this and all other ports will be sent unencrypted; however a Message Integrity Code (MIC) will be generated to ensure the message was not tampered with while in transit.

5.3.9 Hash

Initially the hashing function shall be the same for the MIC as that used on the client's/aircraft's ECDSA Keys. The Hashing function for MIC generation will be negotiated during the authentication process. SHA 384 hashing algorithm is selected for MIC generation. All but the last 4 Bytes will be truncated to minimize the length of the hash while maintaining the security value.

5.3.10 Compression

With the ever increasing population of aircraft traveling the skies, IPS employs compression to increase bandwidth efficiency and to use available radio spectrum as efficiently as possible.

Each message (post the authentication messages on port 5908) regardless of the underlying media type shall be compressed using the method negotiated during authentication. Initially this method will be deflate. MIC codes will be generated after compression (if any) of IPS data is complete. DTLS Handshake messages will also be compressed.

The compression covers the network and transport layer along with the application data layer. The compression details are described below.

5.3.10.1 Lossless Compression Methods

Compression algorithms are reversible but not necessarily lossless procedures that help to increase bandwidth efficiency. Since communication between aircraft and ground IPS systems is defined to support safety-related services, all compression methods used must be lossless.
The following list summarizes the lossless compression methods considered for IPS:

1. Run-length encoding (RLE) – works best on repeating data
2. Huffman coding – Unix Pack, pairs well with other algorithms
3. Prediction by partial matching (PPM) – works best on plain text
4. Bzip2 – Burrows-Wheeler transform with RLE and Huffman coding
5. Byte Pair encoding – simple byte replacement aaa → X with lookup table.
6. Snappy (Zippy) – medium compression based upon LZ77 algorithm
7. Lampel-Ziv compression (LZ77 and LZ78) – dictionary-based algorithm basis for modern compression, examples of which
    a. DEFLATE – LZ77 and Huffman coding used by ZIP, gzip, PNG images
    b. Lempel-Ziv-Markov chain (LZMA) – very high compression Ratio 7zip and xz
    c. Lempel-Ziv-Oberhumer (LZO) – optimized for speed over compression
    d. Lempel-Ziv-Storer-Szymanski (LZSS) – used by WinRAR with Huffman coding
    e. Lempel-Ziv-Welch (LZW) -- used by GIF images and compress.
    f. Lempel-Ziv-Stac (LZS) – LZ77 with Huffman coding (Sliding Window of fixed 2k size)
    g. Lempel-Ziv-Ross-Williams (LZRW) – LZ77 with Hash Tables
    h. LZWL – Character Based LZW Compression
    i. LZX – File Archiver, Microsoft cabinet files.
    j. Others that have similar capabilities or are licensed products.

5.3.10.2 Minimum Supported Compression Methods for IPS

At a minimum, IPS avionics systems, IPS gateways, and IPS ground end systems shall support the following compression methods:

- ROHC – Robust Header Compression
- DEFLATE – LZ77 and Huffman coding

Additional compression methods may be added in the future. It is intended that future compression developments would allow for additional compression methods. The following sections describe how compression is applied to application data and to the protocol headers at transport, network, and link layers.

5.3.10.2.1 Application Data Compression

Application data (e.g., ACARS, FANS, AOC, B1/B2) is compressed using one of the methods listed in Section 5.3.10.2 Minimum Supported Compression Methods for IPS (currently only DEFLATE would be used). Compressed or uncompressed application data is encapsulated in the ATNPKT format specified in ICAO Doc. 9896. As shown in Figure 5-13, the User Data field is prefaced by a two-byte length parameter and a one-byte compression parameter. The length parameter specifies the length of the compressed payload, and the compression parameter indicates the data compression method/algorithm used to compress the payload data. Note that Native IP data may not be encapsulated in ATNPKT, so compression of the Native IP data will be application specific.

> **Commentary:** Some ASN.1 encoded messages have been found to increase in size when compressed. Defining a compression field allows the ground and/or aircraft to determine compressibility and choose the most efficient method of conveying the data.

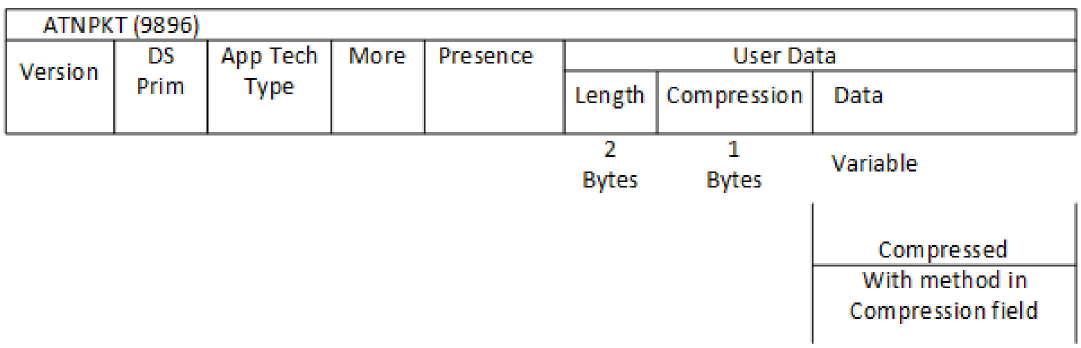


Figure 5-13 - Compression Indication in ATNPKT

Table 5-4 summarizes the compression parameter values. A value of 0x00 in the compression field indicates that no compression is applied to the data. A value of 0x01 indicates that DEFLATE compression is used. As compression technology improves, additional compression methods may be defined.

Compression Parameter (Hex)	Payload Compression Algorithm
0x00	None
0x01	DEFLATE

Table 5-4 - Compression Parameter Values

If necessary, the resulting compressed payload data is then fragmented to fit the maximum transfer unit (MTU) size for the connectivity service. If the payload requires more than one ATNPKT, then the 'More' bit indicates that an additional fragment is following this ATNPKT. In a fragmented payload, only the first ATNPKT contains the length and compression parameters.

5.3.10.2.2 Network and Transport Layer Compression

The Network IP layer and UDP/TCP transport layer headers are compressed together using Robust Header Compression. [ROHC defined in RFC 5795. IP RFC 3843 as amended, UDP RFC 3095 as amended and TCP RFC 6816]. Reducing the header size will allow for smaller packet sizes over the RF spectrum. Figure 5-14 shows an example of ROHC applied to IPv6 and UDP headers.

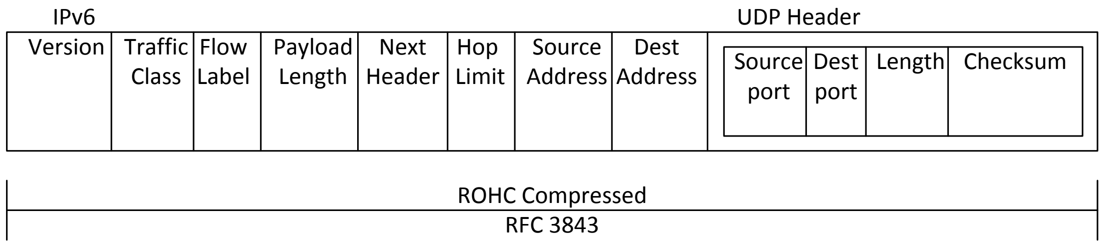


Figure 5-14 - Example of Pre-ROHC Compression

The first IP and UDP packet is sent full size and subsequent packets will be sent with ROHC if both sides support the protocol. The IP and UDP headers will be examined for changing information and the ROHC header created to include only the changing information. ROHC will be completed by the IPS Gateway and the avionics. For UDP/IP based communications the header may be reduced to a single byte.

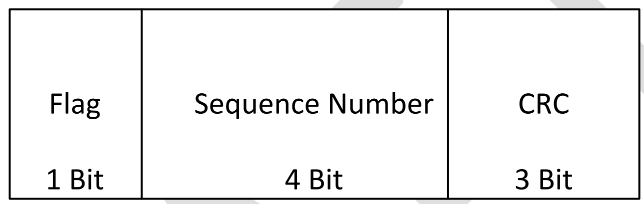


Figure 5-15 - Example of ROHC Compressed UDP/IP header

5.3.10.2.3 Datalink or Link Layer Compression

The Layer 2 framing of IPS data is not compressed so that each frame can be routed without the use of computationally costly decompression methods. The Message Integrity Check (MIC) is used at layer 2 between the aircraft and service provider for authenticating each message. The MIC is an HMAC derived from mutual authentication established at the beginning of the session with the service provider.

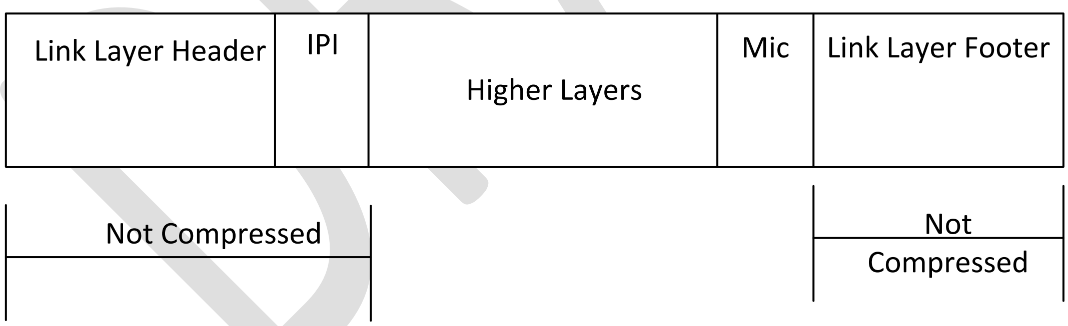


Figure 5-16 - General Example showing non-Compressed Link Layer Fields

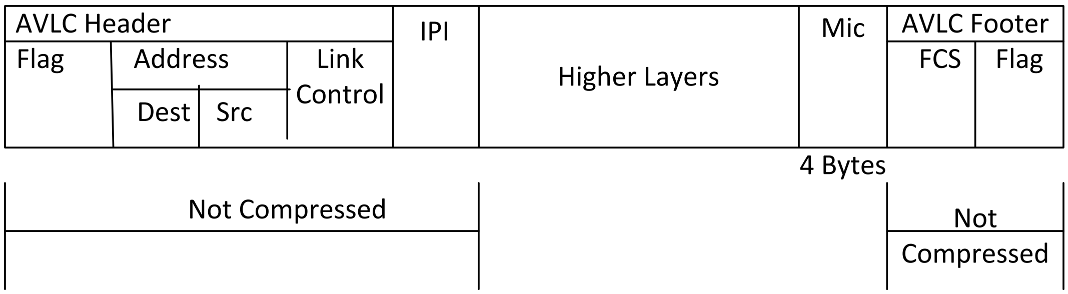


Figure 5-17 - VHF - specific Example showing non-Compressed Link Layer Fields

5.4 Message Integrity Check

The message integrity check (MIC) is computed for each IPv6 packet in order to provide data integrity and authentication. For non-IP networks the MIC may also be computed for each subnetwork packet transmitted in order to secure the subnetwork (this is the case for VDL Mode 2, other subnetworks may be different).

The MIC is computed after the aircraft authentication sequence has been completed.

5.4.1 MIC for IP Packet

The MIC is computed for each IPv6 packet. A fragmented application message, consisting of a number of IPv6 packets, will have a MIC on each IP packet. The MIC is computed after compression over the entire IPv6 packet, the scope of the MIC computation is shown in Figure 5-18. The last 4 bytes from the MIC computation are used to populate the MIC field, which is added at the end of the IPv6 packet by the IPS Gateway for uplink messages.

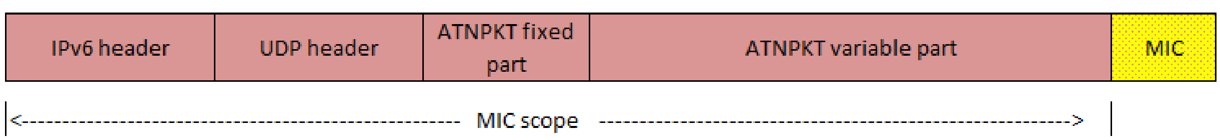


Figure 5-18 – MIC Scope for IP Packet

For downlink messages, the IPS Gateway computes the MIC the same way and compares the last 4 bytes against the value in the MIC field received in the downlink message. If the values do not match, the message is logged with the status of invalid MIC and a DTLS alert message (bad_record_mac) is generated in response. See Section 5.11 Error Detection for more information.

5.4.2 MIC for Subnetwork Packet (AVLC based media)

The MIC is computed for each subnetwork packet, this is illustrated by looking at the VDL Mode 2 network.

> Note: MIC computation at the AVLC layer (sub-network layer) is not specifically IPS functionality, however it is included in the document since VDL Mode2 is not secured like other IPS media and the addition of securing VDL Mode2 is specifically for the support of IPS.

The VDL Mode 2 subnetwork utilizes the 'orange' protocol to provide segmentation of messages that exceed the AVLC frame size. The 'orange' protocol receives the IPv6 packet (maximum size of 1280 bytes) and segments it as needed to fit within the AVLC frame size (251). Each of these segments will be in an AVLC frame with the IPS IPI and the 'orange protocol header and the computed MIC at the end of AVLC information field. This segmentation is illustrated in Figure 5-19.

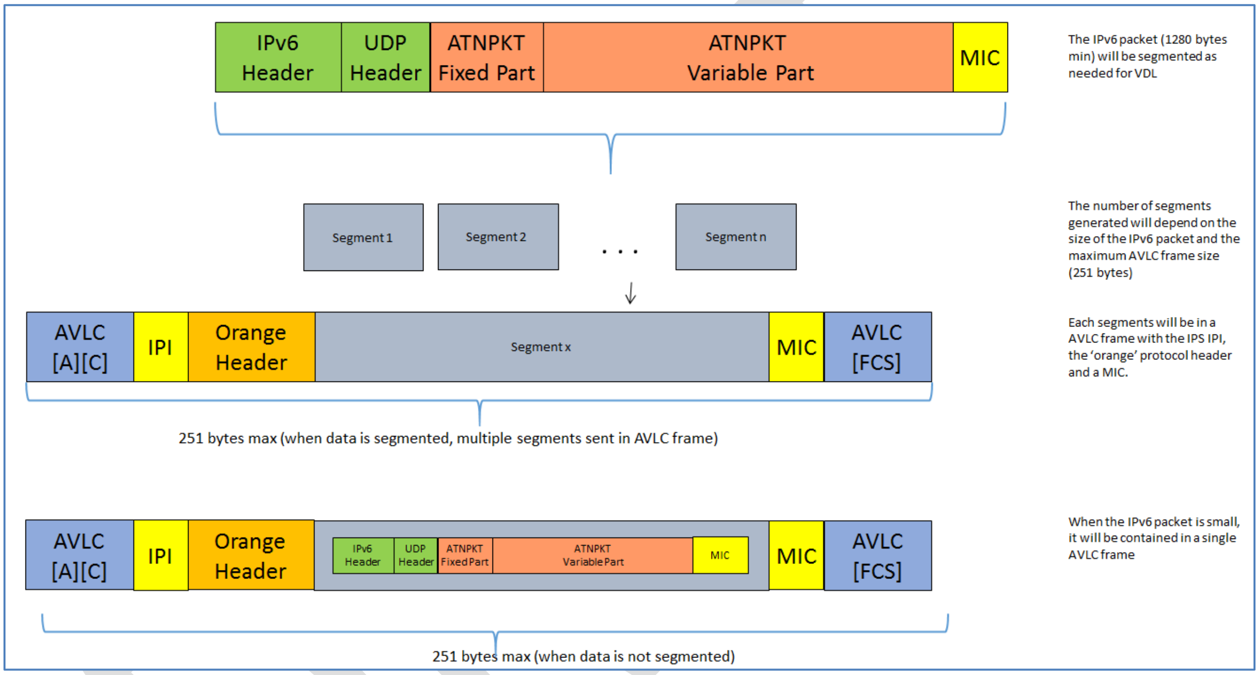


Figure 5-19 - VDL Mode 2 link layer segmentation for IPS

The MIC is computed over the AVLC header and the entire AVLC information field excluding the last 4 bytes which are reserved for the last 4 bytes of the MIC field. This is illustrated in Figure 5-20.

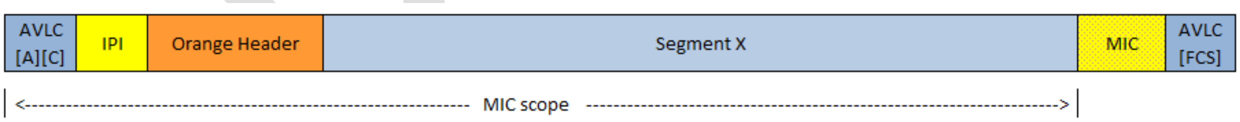


Figure 5-20 - MIC Scope for non-IP-based Datalink (e.g., VDL Mode 2)

5.4.3 MIC Generation Function for IPS IP packet

DTLS uses the following function to generate the message integrity code:

$$MIC = Truncate(4, PRF(App\ Data + Msg\# + Data\ Length\ with\ Msg\#, + Session\ Key + Key\ Length))$$

"+" denotes concatenation.

The MIC is generated before any encryption is applied. If encryption is applied it includes the MIC.

Variable Name	Explanation
Truncate	A Truncate function that reduces the size of the operator to a number of bytes. In this case the last 4 bytes of the message hash function will be used as a message integrity check.
PRF	Psudo Random Function: This is the hashing function negotiated during the initial DTLS handshake.
App Data	The application layer of data to be miced. For example in an http request the entire http request would be the app data.
Msg # (6 Bytes)	The random message number sent in the last message after authentication added with the total transmissions since that time. This Msg# is unique for downlinks and uplinks and starts with a random number sent after successful DTLS logon. For example the downlink message number could be 568 and the uplink message number could be 123. After one downlink the new downlink message number will be 569. The Message number rolls over to zero if it reaches it max. This message number is not to be confused with the Orange sequence number, if any.
Data Length with Msg# (6 Bytes)	The total length of the Application Data added to the current message number. If the results is greater than max value. Subtract max value. This is effectively a check on the data integrity.
Session Key (32 Bytes)	This is the lower 32 bytes of the session key derived as per RFC 5246 Section 6.3. Both the gateway (server) and aircraft (Client) have a session or master key and compute the counter parties' key using the procedure recorded in the RFC. This value is never transmitted making the PRF function difficult to duplicate by third parties.
Key Length (4 Bytes)	The total session key length in bytes.

5.4.4 MIC Generation Function for AVLC.

DTLS uses the following function to generate the message integrity code:

$$MIC = Truncate(4, PRF(App\ Data + Msg\# + Data\ Length\ with\ Msg\#, + Session\ Key + Key\ Length))$$

"+" denotes concatenation.

Note: The session key is shared between the segment (AVLC layer) and the message (IPS Layer). The computations of MIC are different resulting in a code that is difficult to fake at both layers.

The MIC is generated before any encryption is applied. If encryption is applied it includes the MIC.

Variable Name	Explanation
Truncate	A Truncate function that reduces the size of the operator to a number of bytes. In this case the last 4 bytes of the message hash function will be used as a message integrity check.
PRF	Psudo Random Function: This shall be negotiated at DTLS logon
App Data	The information frame to be miced. For everything between the AVLC header and footer
Msg # (6 Bytes)	The Message number shall start a 1 for the first downlink/uplink and be increased for each successive AVLC transmission. This Msg# is unique for downlinks and uplinks. For example the downlink message number could be 902 and the uplink message number could be 321. After one successful downlink the new downlink message number will be 903. The Message number rolls over to zero if it reaches it max. This message number is not to be confused with the Orange sequence number, if any.
Data Length with Msg# (6 Bytes)	The total length of the Information Frame Data added to the current message number. If the results is greater than max value. Subtract max value. This is effectively a check on the data integrity.
Session Key (32 Bytes)	This is the lower 32 bytes of the session key derived as per RFC 5246 Section 6.3. Both the gateway (server) and aircraft (Client) have a session or master key and compute the counter parties' key using the procedure recorded in the RFC. This value is never transmitted making the PRF function difficult to duplicate by third parties.
Key Length (4 Bytes)	The total session key length in bytes.

5.5 Key Management

All Crypto methods have a limited useful life time, the crypto period. It is the time from when they are derived to the point at which computing power becomes sufficient enough to brute force guess the private key in a reasonable amount of time, or a flaw is exposed in the key generation method.

In order to ensure that aircraft can initiate an IPS connection with any trusted provider, keys will need to be managed.

5.5.1 Key Management Functions

To facilitate the exchange and security of keys with an aircraft the following port 5908 key tag selectors have been defined for key management. All key tag values of 0x3X will use the encrypted connection negotiated upon DTLS logon.

Key Tag	Meaning
0x30	Upload a new Root CA Certificate
0x31	Upload a new Aircraft Private key
0x32	Upload a new Aircraft one time use Private Key
0x33	Upload a new Aircraft Certificate
0x34	Upload a new Aircraft one time use Certificate
0x35	Upload the primary service provider's certificate
0x36	Upload a secondary service provider's certificate
0x37	Change IP address to:
0x38	Reserved - Encrypted
0x39	Reserved - Encrypted
0x3A	Reserved - Encrypted
0x3B	Reserved - Encrypted
0x3C	Reserved - Encrypted
0x3D	Reserved - Encrypted
0x3E	Reserved - Encrypted
0x3F	Reserved - Encrypted

Table 5-5 - Key Management Key Tags

5.5.2 Initial Key installation

Upon manufacture completion, the avionics manufacturer will preload all root certificates for all valid service providers. The Avionics manufacturer will also upon sale load the primary service provider server certificate and work with the primary service provider to install aircraft specific certificates and keys for IPS operation. The IP address shall also be set by the avionic provider at the direction of the primary service provider. The airline may also request the installation of other trusted companion service providers server keys to allow roaming.

Failing pre-load by the avionics manufacturer or during subsequent lease or sale of an aircraft, it is recommended that avionics have a physical way, to load certificates, IP address configs and keys for IPS. It is recommended that avionics manufactures standardize the process for physical media and configuration files. The physical loading of keys should always be available. It will allow airline to recover aircraft that have been compromised or if keys expired before returning to the primary service provider's coverage area.

The Airline can request a new set of certificates (Primary Service Provider Server, Aircraft Cert, Aircraft Private key, one time use cert, one time use private key) from the primary service provider, or a new primary service provider at any time via the processes documented in the master certificate policy and service contract. If there is a change in primary service provider the keys must be loaded manually via ground maintenance device. The airline is responsible for maintaining the security of the maintenance device(s) after issue. Compromised keys shall be reported to the primary service provider as soon as possible.

5.5.3 Subsequent Key installation

Once Avionics are initially loaded with an IP, Certificates and keys, further management can be done via the primary service provider's communication network, as long as the primary service provider remains unchanged. If a change in primary service provider is required, physical configuration of the avionics will be necessary.

5.5.3.1 Upload a new Root CA Certificate 0x30

Avionics will be expected to maintain a list of Root CA certificates (the root CA Store) to validate provider certificates. It will be the responsibility of the airline to keep this store up to date. The primary service provider can upload new Root CA certificates as provided by airline host and trusted companion service providers. The UDP port 5908 with key tag of 0x3X will use encryption negotiated upon DTLS logon.

Root CA certificates are trust anchor points. Compromise of a trust anchor has significant financial and legal implications. The service provider should not initiate a RootCA Upload for foreign root certificates without appropriate signed permission and certification that the digital certificates are authentic, genuine and that the airline wants to be able to roam onto that network. The Primary Service Provider may upload updates to its own root certificate at any time, as long as it remains the primary service provider.

Avionics upon receiving a Root CA Certificate will update the root CA store with the incoming certificate. Only one Root CA certificate will be uploaded per instance. It is expected that avionics will replace any root CA certificate previously existing in the Root CA store issued by the same authority with that received. For example a Symantec root certificate with another Symantec root certificate. The avionics should maintain its own Root CA certificate store and remove any expired Root CA Certificates periodically. Uploaded certificates will be in DER format.

Only the primary service provider will be allowed to upload new Root CA certificates over the network.

Aircraft should maintain their DTLS connection with the primary service provider after installing a new Root CA certificate. Upon any new login or refreshing of the connection the current Root CA certificate store will be used to validate any service provider's authentication certificate(s). The port 5908 key tag for uploading a new Root Certificate will be 0x30, and will be followed by certificate (upload) or one additional byte (response).

Service Provider Sends	Aircraft Sends	Meaning
Root Certificate	0x00	Certificate accepted and installed.
Root Certificate	0x01	Certificate rejected. – Already have this certificate, invalid, expired, or otherwise.

Table 5-6 - Upload new Root CA Certificate Return Codes

Only one root certificate should be maintained on the aircraft per CA. Note, it is quite possible for two different service providers to use the same CA. If a new root certificate is loaded, then any previous root certificate for that same CA should be removed and replaced with the incoming root certificate. The return code will remain the same. More information will be included in the primary service provider's Certificate Practice Statement and Certificate Policy as well as the individual customer contract.

5.5.3.2 Upload a new Aircraft Private Key 0x31

In the event that the private key expires due to crypto period lifetime or becomes compromised via other means, the service provider can upload a new Private Key via the encrypted connection, using a port 5908 key tag of 0x31. It is expected that the primary service provider or airline would change the private key, and public certificate. The IP address and Primary Service Provider’s key can be changed as well if necessary.

Aircraft should maintain their DTLS connection with the service provider after installing a new private key. Upon any new login or refreshing of the connection the new private key will be used, until that time the old private key should be used. The Upload a new Aircraft Private Key will have a port 5908 key tag of 0x31, and be followed by the private key (upload) or one additional byte (response).

Service Provider Sends	Aircraft Responds	Meaning
Aircraft Private Key	0x00	New Private Key accepted and installed
Aircraft Private Key	0x01	New Private Key rejected.

Table 5-7 - Upload new Aircraft Private Key return codes

5.5.3.3 Upload a new Aircraft one time use Private Key 0x32

In the event that the onetime use key expires due to crypto period lifetime, becomes compromised via other means, or is used, the service provider can upload a new one time use private key via the encrypted connection, using port 5908 key tag 0x32. It is expected that the service provider would change the onetime use private key, and one time use public Certificate in the same DTLS session. The IP address and Primary Service Provider’s key can be changed as well if necessary.

Aircraft should maintain their DTLS connection with the service provider after installing a new one time use private key. Upon any new login or refreshing of the connection the new private key (if available) will be used. The onetime use private key will expire upon the first successful logon with that key to the primary service provider; it must be changed at that time. The Upload a new Aircraft private one time use key will have a port 5908 key tag of 0x32, and be followed by the private key (upload) or one additional byte (response).

Service Provider Sends	Aircraft Responds	Meaning
Aircraft One Time Use Private Key	0x00	New One Time Use Private Key accepted and installed
Aircraft One Time Use Private Key	0x01	New One Time Use Private Key rejected.

Table 5-8 - Upload new Aircraft Private One time Use Key return codes

5.5.3.4 Upload a new Aircraft Certificate 0x33

Each Aircraft will be equipped with a digital certificate, used for authentication with the primary service provider and all trusted companion service providers. Uploaded certificates will be in DER format. The corresponding private key will be maintained by the aircraft and primary service provider.

Aircraft certificates will be signed by the primary service provider. See Section 5.3.5 ECDSA Keys for more information. The Aircraft Certificate will be transmitted over an encrypted channel negotiated at DTLS logon.

Aircraft should maintain their DTLS connection with the service provider after installing a new aircraft certificate using the old certificate if necessary. The port 5908 key tag of 0x33 will be followed by an Aircraft Certificate when sent by the service provider. The aircraft will use the same port 5908 key tag of 0x33 to send a one byte return code indicating success or failure.

Service Provider Sends	Aircraft Responds	Meaning
Aircraft Certificate	0x00	New One time use certificate is accepted and installed
Aircraft Certificate	0x01	New One time use certificate is rejected.

Table 5-9 - Install a new Aircraft Certificate return codes

5.5.3.5 Upload a new Aircraft one time use Certificate 0x34

Each Aircraft will be equipped with a one-time use certificate from its primary service provider. These certificates will be included in CRL lists provided to trusted companion providers, effectively making these certificates one time use only on the primary service provider's network. In the event that the aircraft's primary certificate fails due to expiration or CRL revocation the aircraft can use this one-time use key on the primary service provider's network. The one time use key will expire upon first use. Having a one-time use key ensures that aircraft will not require physical media in order to replace its service keys. That is as long as it is connected with the primary service provider. Uploaded one-time use certificates will be in DER format and be via the DTLS encrypted channel negotiated at logon.

Aircraft should maintain their DTLS connection with the service provider after installing a new one time use certificate using the old certificate if necessary. The UDP port 5908 key tag of 0x34 will be followed by a one-time use certificate in DER format when sent by the Service Provider. The aircraft will use the port 5908 key tag of 0x34 and one additional byte to indicate success or failure.

Service Provider Sends	Aircraft Responds	Meaning
Aircraft One time use Certificate	0x00	New One time use certificate is accepted and installed
Aircraft One time use Certificate	0x01	New One time use certificate is rejected.

Table 5-10 - Upload a new Aircraft one-time-use Cert return codes

5.5.3.6 Upload the primary service provider's certificate 0x35

Part of the security system of the avionics is being able to recognize the primary service provider. When the aircraft is logged into the primary service provider via DTLS, then additional features will be unlocked to allow the primary service provider to maintain the keys, certificates and IP address of the aircraft. If the service provider certificate received during the DTLS logon does not match that of Primary Service Provider's, then the port 5908 key tags of 0x3X will be restricted from access. There will be only one primary service provider certificate within the avionics at any one time.

In the event that the primary service provider's server's certificate needs to change, perhaps due to nearing certificate expiration or crypto period expiry due to algorithm compromise.

Aircraft should maintain their DTLS connection with the service provider after installing a new primary service provider certificate until a re-authentication or new login is needed or requested. The port 5908 key tag of 0x35 will be followed by the Primary Service Provider's Certificate when sent by the Primary Service Provider. The aircraft will use a port 5908 key tag of 0x35 followed by one additional byte to indicate success or failure.

Service Provider Sends	Aircraft Responds	Meaning
Primary Service Provider's Certificate	0x00	New Primary Service Provider's certificate is Accepted and installed
Primary Service Provider's Certificate	0x01	New Primary Service Provider's Certificate is rejected.

Table 5-11 - Primary Service Provider Key upload return codes

5.5.3.7 Upload a secondary Service Provider's Certificate 0x36

Airlines often times contract with many service providers in order to have service if the primary service provider is not available. The primary service provider could upload via RF the secondary service provider's certificates; this is to limit who is authorized to update certificates over RF. Secondary Service provider certificate upload is limited to the customer agreement, Certificate Practice Statement and Certificate Policy, each service provider is free to develop their own policies as long as they meet or exceed the minimum standards outlined in the Master Certificate Policy.

Avionics upon receiving a secondary provider Certificate will update the secondary provider store with the incoming certificate. Only one secondary provider certificate will be uploaded per instance. It is expected that avionics will replace any secondary provider certificate previously existing in the secondary provider store issued by the same authority with that received. For example a SITA provider certificate with another SITA provider certificate. The avionics should maintain its own secondary provider certificate store and remove any expired secondary provider certificates periodically. There may be many secondary service providers' certificates in this store. Uploaded certificates will be in DER format.

Only the primary service provider will be allowed to upload new secondary provider certificates over the network. Airlines will be able to load them using on-ground avionics maintenance devices.

Aircraft should maintain their DTLS connection with the primary service provider after installing a new secondary provider certificates. Upon any new login or refreshing of the connection the current

Secondary provider certificate store will be used to validate any trusted companion service provider's authentication certificate(s). The port 5908 key tag for uploading a new secondary provider certificate will be 0x36, and will be followed by certificate (upload) or one additional byte (response).

Service Provider Sends	Aircraft Sends	Meaning
Root Certificate	0x00	Certificate accepted and installed.
Root Certificate	0x01	Certificate rejected. – Already have this certificate, invalid, expired, or otherwise.

Table 5-12 - Upload new Secondary Provider Certificate Return Codes

5.5.3.8 Change the IP address 0x37

The primary service provider should assign an IP address to each aircraft under contract. This should be coordinated with IANA and be updated along with a new Aircraft Certificate, service provider key, aircraft secret key. The IP address should be changed via an encrypted connection negotiated at DTLS logon to the primary service provider.

> Note: This specific command is only meant to be used infrequently due to a sale of an Aircraft or other major event.

Aircraft should maintain their DTLS connection with the service provider after installing a new IP address until a re-authentication or new login is needed or requested. The old IP address should be used until a new session is established. The port 5908 key tag of 0x37 will be followed by the new IP address when sent by the service provider. The aircraft will use a port 5908 key tag of 0x37 followed by one additional byte to indicate success or failure.

Service Provider Sends	Aircraft Responds	Meaning
New IP address	0x00	New Aircraft IP is accepted and installed.
New IP address	0x01	New Aircraft IP is rejected.

Table 5-13 - Change IP address return codes

5.5.4 Function of the One Time Private Key and Certificate

The Aircraft's One time use Key and Certificate are meant to be a failsafe mechanism to prevent aircraft from needing hands on maintenance in the event that an aircraft's key, certificate, or both become expired or compromised. It is intended that the one time use key will only be usable on the Primary Service provider's network. This will be enforced by adding the one-time use certificate to the Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) shared with trusted companion service providers.

Each Primary Service Provider will need to keep two CRLs one of one-time use keys and the other of revoked certificates - other than by expiry. Primary service providers should accept logons via one-time use keys, but the detection of that key should trigger an immediate upload of a new aircraft primary key and certificate as well as one-time use Key and Certificate.

To emphasize, one-time use certificates and keys will only be usable on the primary service provider's network and then only once. They will be treated as revoked certificates on trusted companion service provider networks. Untrusted companion service providers will see them as invalid certificates.

5.5.5 Key Maintenance Operations Packet Format

Key maintenance operations are available for the primary service provider only. The DTLS Header and payload is encrypted to protect the keys and certificates while in transit. The key management packet shall look like:

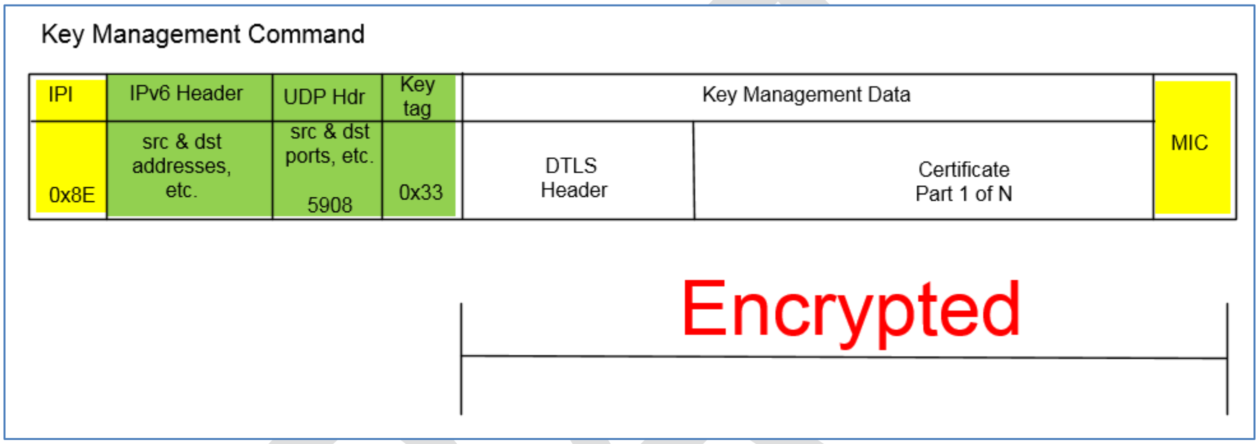


Figure 5-21 - Key Management Command format

In this example the primary service provider is sending up a new aircraft primary certificate for use on all new connections.

The response to a Key Management command shall use the DTLS Header and a response code usually 0x00 or 0x01 to indicate success or failure of the key command respectively. Please review each key management command for appropriate response codes.

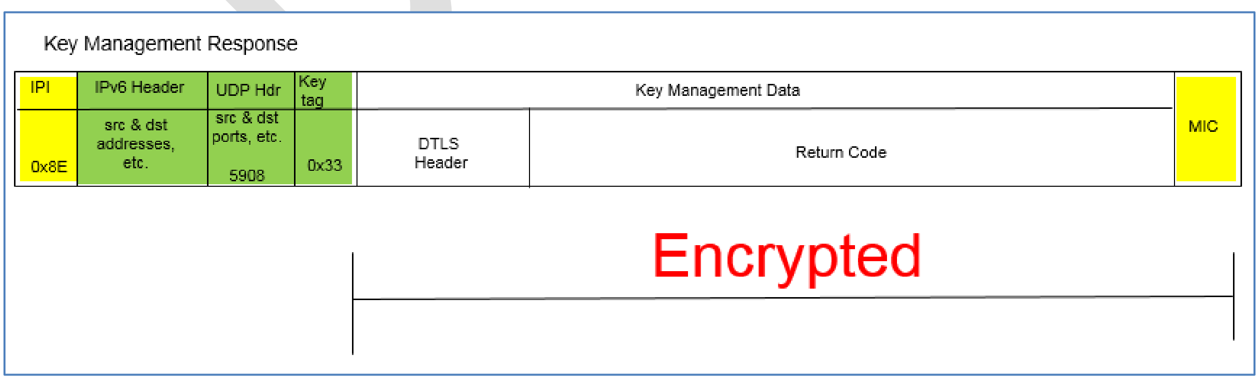


Figure 5-22 - Key Management Response format

5.6 IPS Information Message

The IPS Information message will be generated by the aircraft every 10 minutes in order to provide aircraft information for the ground to update its uplink delivery options. The IPS Information message will also be useful as a supplemental source of position information.

The message will be sent with the IPS IPI (0x8E) and the first byte of the UDP data field will have a key tag value of 0x0B preceding IPS Information message to indicate that this is an IPS Information message. The IPS Information message is shown in Figure 5-23.

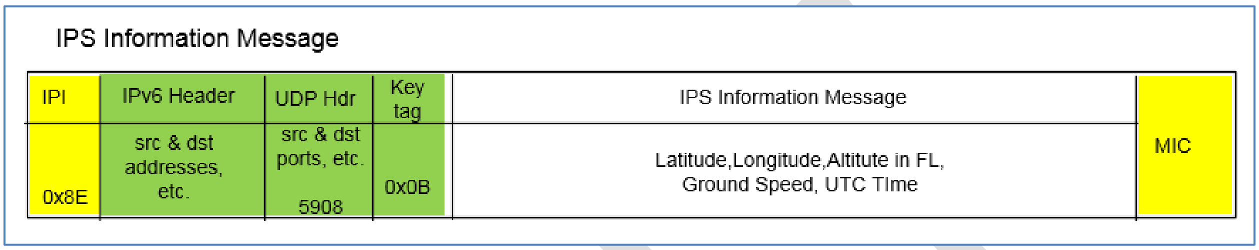


Figure 5-23 – IPS Information Message

The IPS Information message will contain latitude, longitude, altitude, ground speed and UTC. The layout and details of the position report data are shown in Figure 5-24 and Table 5-14.

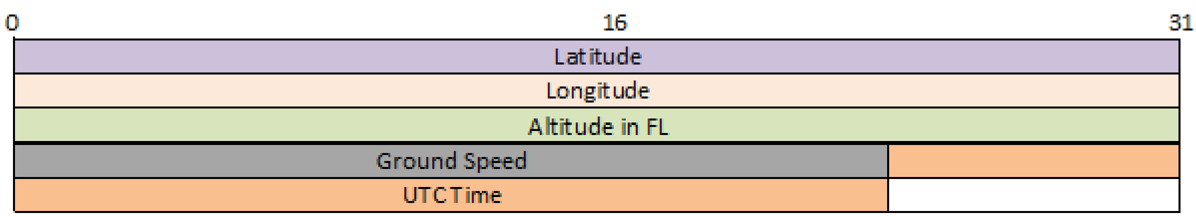


Figure 5-24 – IPS Information Message Data Format

Field	Format	Remarks
Latitude	Radians	pi/2 to -pi/2 negative South of equator
Longitude	Radians	pi to –pi negative West of meridian
Altitude	Flight levels (in hundreds of feet)	0 to 999
Ground Speed	In knots	0 to 999
UTC	Year 8 bits { 0 = 2017}, 4 bit Month {1-12}, 5 bit Day of the Month (1-31}, 6 bit Minute (0-59), 5 bit Hour (0-23), 4 bits Seconds (1-15)	Seconds resolution of 4 seconds or increment of 4 i.e. 21 seconds to be encoded to 6

Table 5-14 – IPS Information Message Details

5.7 IP Lookup Message

The IPS Gateway shall provide an IP lookup service. This service will allow the aircraft to request the IPv6 address of a facility or ground system. An aircraft can generate multiple name lookup requests at any given time.

The request will be sent with the IPS IPI (0x8E) and the first byte of the UDP data field will have a key tag value of 0x0C to indicate that this is an IP Lookup message. The IP Lookup message will be generated by the aircraft when it needs to obtain a specific IP address. A Simple IP Address Name Lookup flow example is in Figure 5-25.

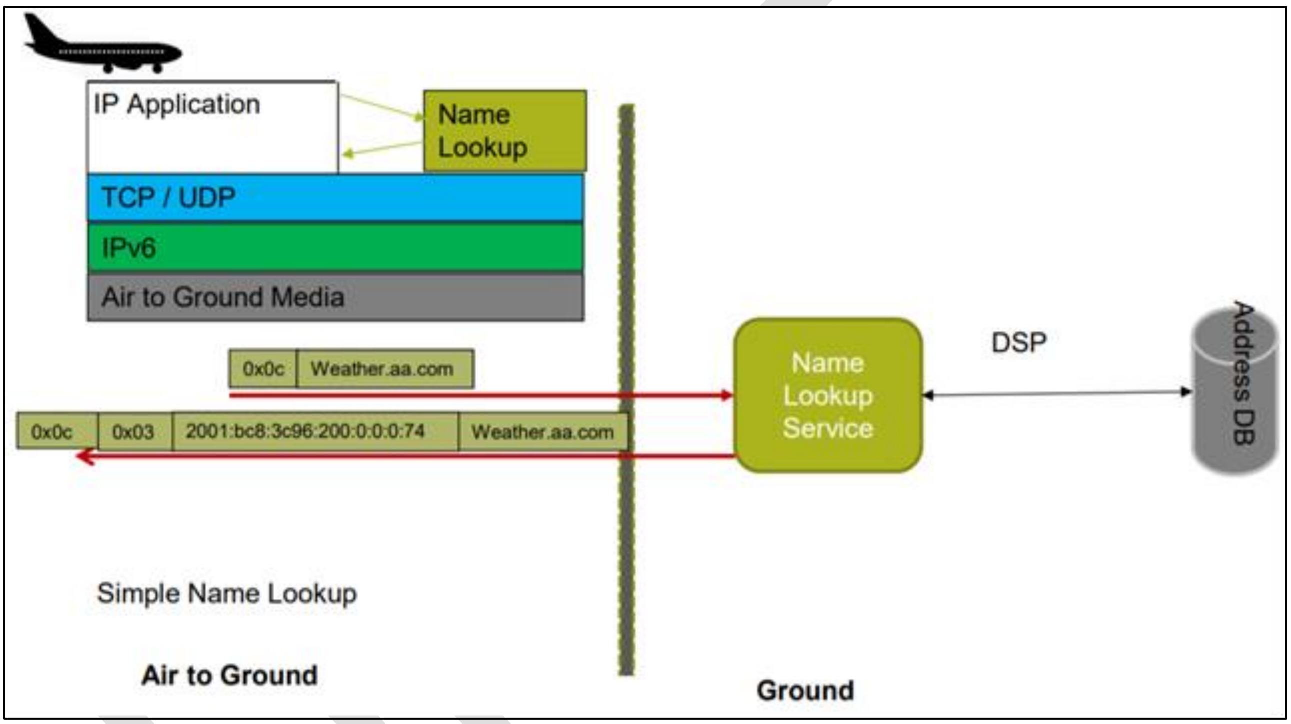


Figure 5-25 – Simple Name Lookup Example

The format of the IP lookup request is shown in Figure 5-26 and the detail of the request field is shown in Figure 5-27.

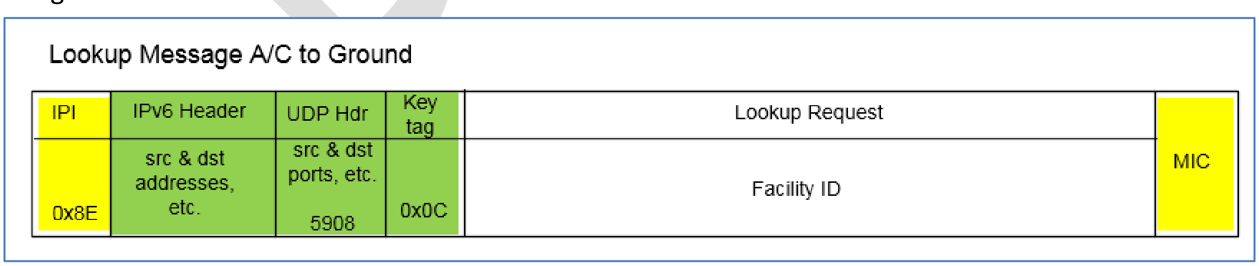


Figure 5-26 – IP Lookup Message Format

The request will contain the domain name to be resolved into an IP address (for example EDYY or EDYYTEST).

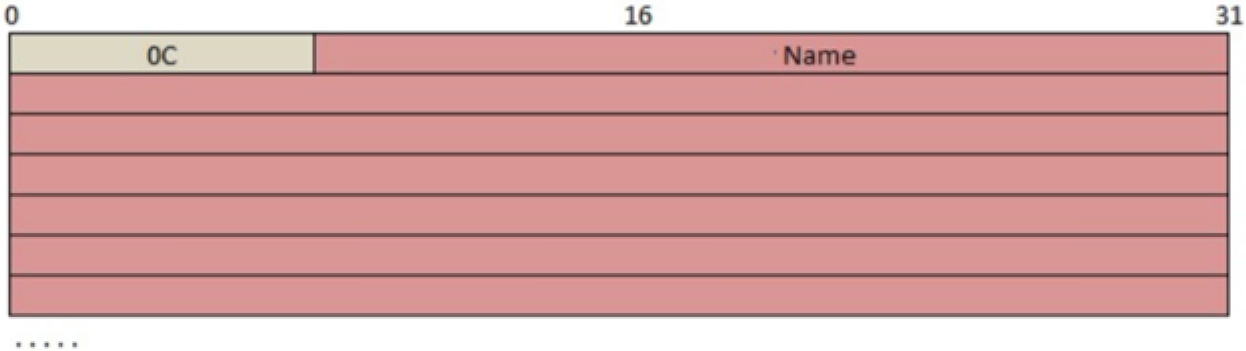


Figure 5-27 - IP Lookup Request Message Data

The response will contain the facility type, the facility address followed by the facility ID in the request. The facility address will be dependent on the facility type. Table 5-15 contains the possible values for the facility type and the corresponding address field.

> Note: The IPS Gateway will maintain an IP address database. The communication service provider will update the IP address database based on the ICAO publication cycle.

Response message format and data are shown in Figure 5-28 and Figure 5-29 respectively.

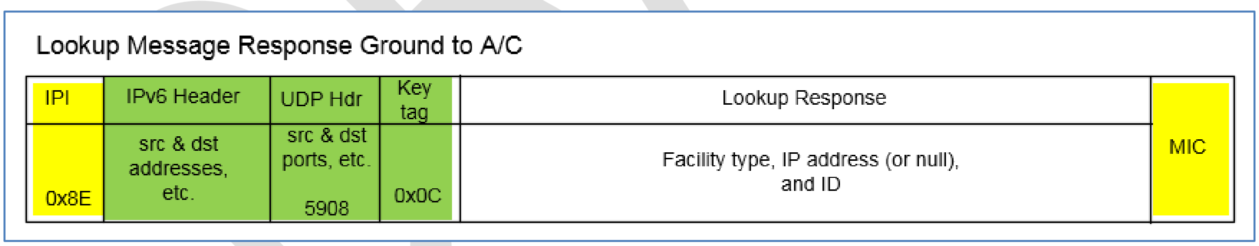


Figure 5-28 – IP Lookup Response Message Format

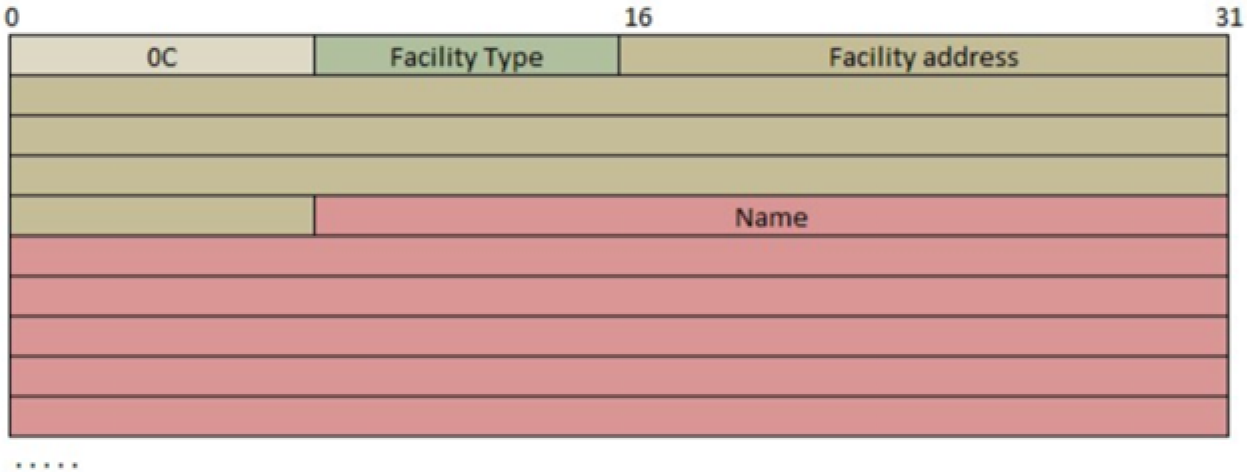


Figure 5-29 – IP Lookup Response Message Data

Value	Facility Type	Facility Address
0x00	No address / unknown facility	Field is Blank / NULL (No value)
0x01	A620 Host	128 bit address of IPS Gateway
0x02	ATN/OSI Facility	128 bit address of IPS Gateway
0x03	IPS End System	128 bit address of IPS End System or Host/Node
0x04 – 0xFF	Reserved for future protocols	Reserved

Table 5-15 – Facility Type Values

5.8 IPv6 Packet

The IPv6 packet consists of header and data, where for IPS the payload data consists of the UDP header, the ATNPKT, and the last 4 bytes of the computed MIC as shown in Figure 5-30.

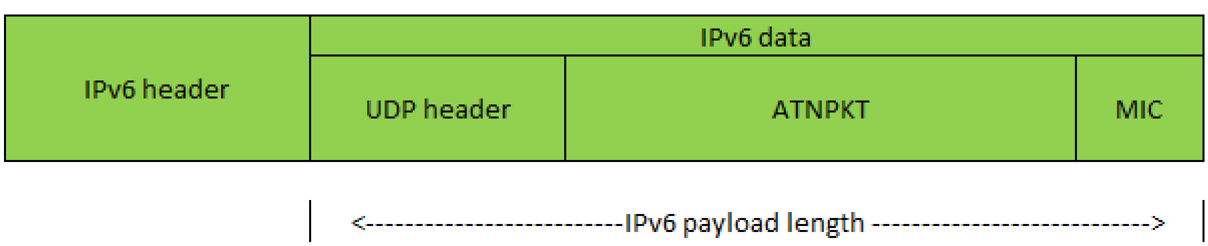


Figure 5-30 – IPv6 packet

The maximum size of the IPv6 packet, per RFC 8200, is 1280 octets. Because of the ICAO Doc. 9896 limitations on the size of the ATNPKT, the maximum IPv6 packet for IPS will be slightly under this as shown in Figure 5-31.

IPv6 header	UDP header	ATNPKT fixed part	ATNPKT variable part		MIC
			other than user data	user data	
40	8	3	max 31 bytes	max 1024 bytes	4

<-- max 1110 bytes -->

Figure 5-31 – IPv6 Packet sizing for IPS

5.8.1 IPv6 Header

The IPv6 header is the first 40 bytes of the IPv6 packet and is laid out as follows:

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination Address																															
28	224																																
32	256																																
36	288																																

Figure 5-32 – IPv6 Header Format

The IPv6 header consists of:

- Version – the constant 6 – "0110"
- Traffic Class - These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN). Default is all bits set to "0".
- Flow Label – used to maintain sequential flow of packets. Default is all bits set to "0".
- Payload Length – The 16-bit Payload Length field contains the payload length, that is, the length of the data field following the IPv6 header, in octets. (The length is across the UDP header, the ATNPKT, and the MIC (as shown in Figure 5-30)
- Next Header – The 8-bit Next Header field identifies the type of header immediately following the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet. The value of 0x11 in this field identifies the UDP transport protocol used by a packet's payload.
- Hop Limit - This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
- Source Address – follows IPS aircraft and ground addressing described below
- Destination Address – follows IPS aircraft and ground addressing described below

<u>Aircraft Addressing</u>

Each IPS aircraft will have a unique network address. This address is structured as shown in Figure 5-33.

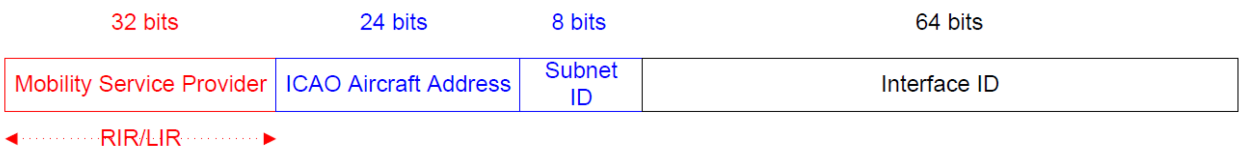


Figure 5-33 – IPS Aircraft Addressing

The aircraft address includes

- Mobility Service Provider – the 'home' entity based on the assigning service provider (i.e. ARINC North America, SITA, ADCC, KAC, AeroThai, Airline Agency, etc.)
- ICAO Aircraft Address - the 24 bit ICAO aircraft address; this address shall be used by the IPS Gateway to look-up the aircraft tail number
- Subnet ID – Mobility Service Provider assigned value (could be based on agency ID [airline ID])
- Interface ID – Mobility Service Provider assigned value (could be based on fleet, tail, etc.)

Each aircraft will have a nomadic fixed address assigned, by the primary service provider / ICAO, to the aircraft for all interfaces. Each interface has a DSP assigned and media specific globally routable IPv6 prefix.

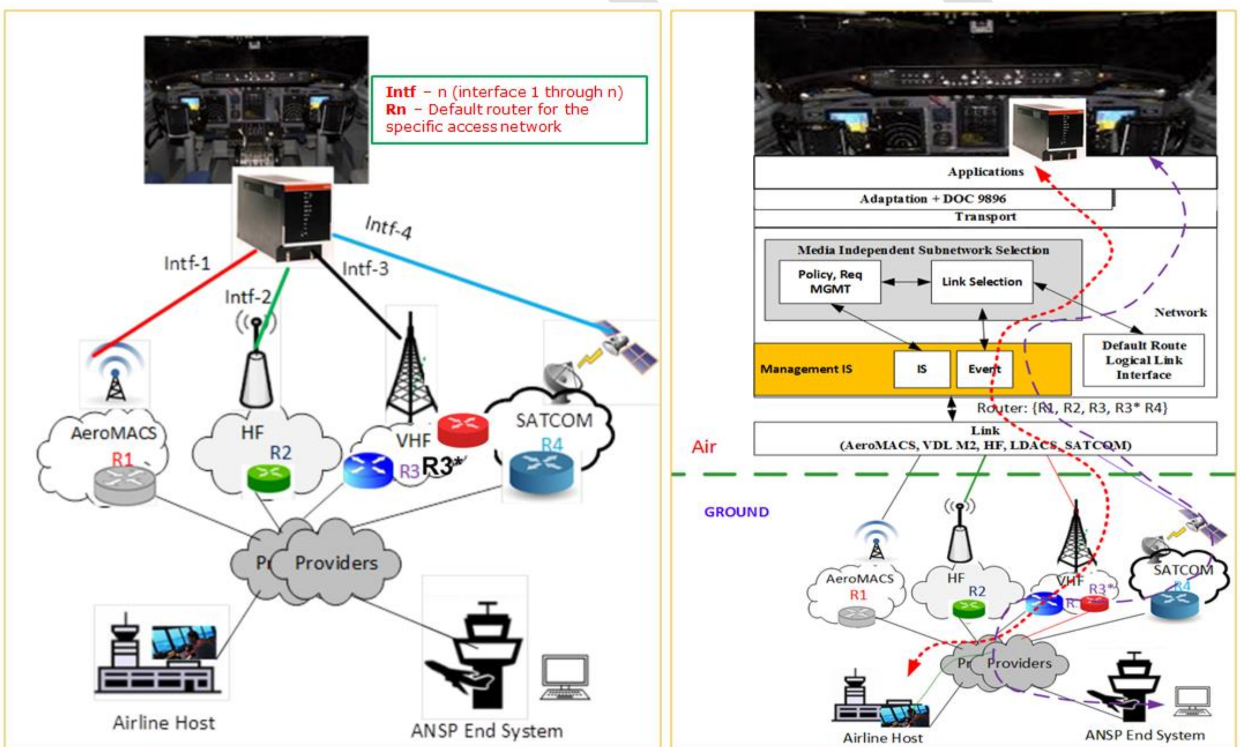


Figure 5-34 – Multihoming with Multiple Addresses

Traffic originated or destine to aircraft will use the aircraft nomadic IPv6 address as the source or destination IP address regardless of air to ground media. The avionics host follows the default gateway mechanism, which will choose the unify gateway among more than one default route.

Communication service provider will manage their own address; their Administrative Domains obtains IPv6 address prefix assignments from their Local Internet Registry (LIR) or Regional Internet Registry (RIR).

<u>Ground Addressing</u>

Figure 5-35 shows the structure of the IPS Ground Address.

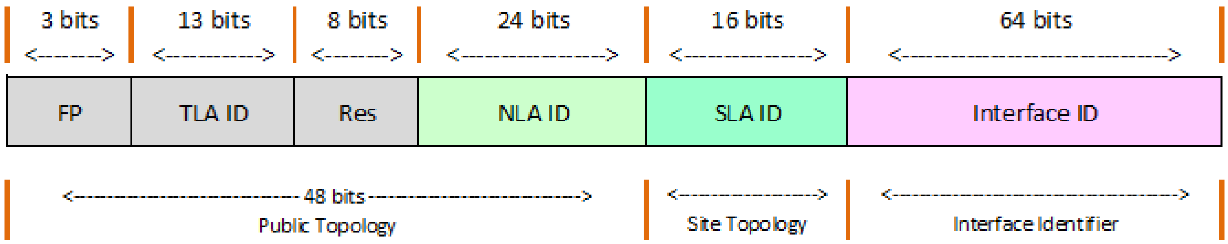


Figure 5-35 – IPS Ground Addressing

The ground address is an IPv6 global address and is composed of the following fields:

- FP – Format Prefix, 001 for aggregatable global unicast addresses
- TLA ID – Top level Aggregation Identifier, these are allocated by IANA to local internet registries
- RES – reserved for future use (for expansion of TLA ID or NLA ID)
- NLA ID – Next Level Aggregation Identifier identifies a specific customer site.
- SLA ID – Site Level Aggregation Identifier, identifies subnets within a specific site.
- Interface ID – Interface Identifier, identifies the interface of a node on a specific site.

Additional information on IPv6 addressing is available in RFC 4291.

5.8.2 IPv6 Payload

The IPv6 payload consists of the UDP packet which is carrying the ATNPKT or Native IP application data. These are described separately.

> Note: UDP is considered the primary transport protocol for IPS for initial implementation; this does not preclude the use of TCP for IPS (ICAO WG-I to decide on TCP)

5.9 UDP Packet

The IPv6 payload consists of UDP packet made up of an 8 byte header and variable data portion. The UDP packet layout is shown in Figure 5-36.

Source Port	Destination Port
Message Length	Checksum
Data………	

Figure 5-36 – UDP Packet

5.9.1 UDP Packet Header

The UDP packet header consists of four fields which include Source Port, Destination Port, Message Length, and Checksum.

5.9.1.1 Source and Destination Port

The port number defines the service access point. The following ports have been defined.

Service Name	Port	Notes
Authentication / Management	5908	
(ATN) CM	5910	IP App
(ATN) CPDLC	5911	IP App
(ATN) ADS-C	5913	IP App
AOC	5914	A620 data
(FANS) AFN	5915	A620 data
(FANS) CPDLC	5916	A620 data
(FANS) ADS-C	5917	A620 data
Others	other	Native IP Apps

Table 5-16 – UDP Ports

Other services have not been defined but are assumed to be IP applications.

Prior to authentication, the only port open is 5908. After aircraft authentication, port 5908 will also be used for other messages including the key management and IP lookup messages.

5.9.1.2 Message Length

The message length field specifies the length in bytes of the UDP packet (header and data).

5.9.1.3 Checksum

Checksum is mandatory for UDP running over IPv6. UDP checksum is computed by taking the one's complement of the one's complement sum of all 16 bit words in the header (a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets). In other words, all 16-bit words are summed using one's complement arithmetic. Add the 16-bit values up. Each time a carry-out (17th bit) is produced, swing that bit around and add it back into the least significant bit. Reference for the computation is in https://en.wikipedia.org/wiki/User_Datagram_Protocol (note 8). The sum is then one's complemented to yield the value of the UDP checksum field. The layout of this IPv6 pseudo header is shown in Figure 5-37.

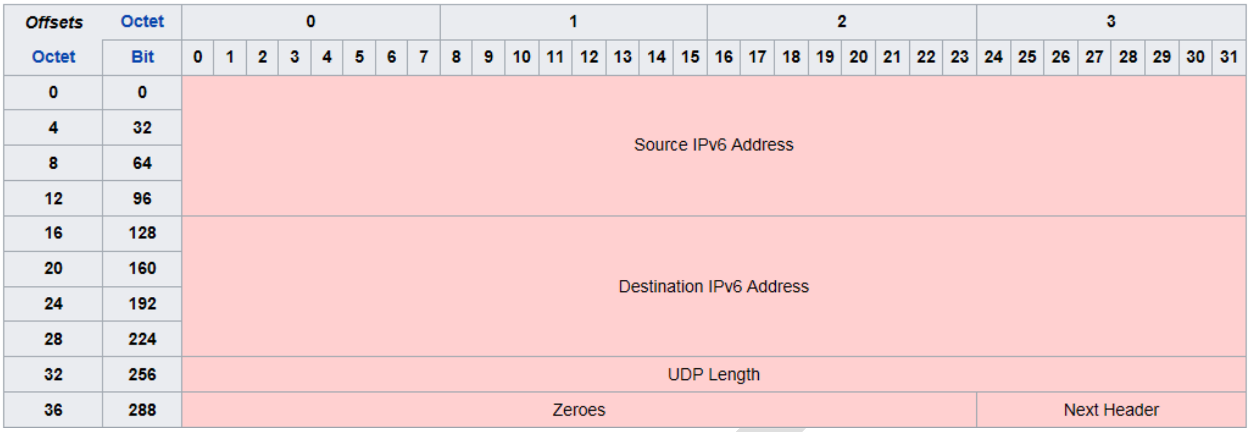


Figure 5-37 – IPv6 Pseudo header

If the checksum calculation results in the value zero (all 16 bits 0) it should be sent as the one's complement (all 1s).

5.9.2 UDP Data

The data field of the UDP packet is dependent on the destination port number. For port 5908 the data field is used for specific messages (authentication, keep alive, and IP lookup) as described in section 3.2.5. For all other ports, the data field contains aeronautical telecommunication network packet (ATNPKT) data.

5.10 ATNPKT

The ATNPKT is defined in ICAO Doc. 9896 [1] and is described herein as to its application by the IPS Gateway. The ATNPKT consists of a fixed part and a variable part consisting of supplementary header information followed by user data.

The layout of ATNPKT is shown in Figure 5-38.

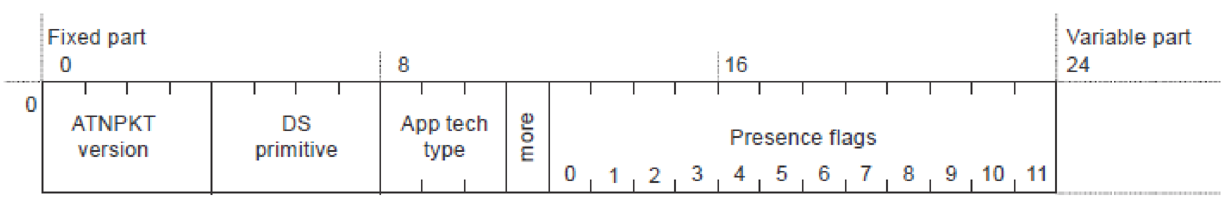


Figure 5-38 – ATNPKT Format

5.10.1 Fixed Part

5.10.1.1 ATNPKT Version

The ATNPKT Version is a 4 bit field and shall be set to 1. This number may be incremented in the future for modifications of the ATNPKT.

5.10.1.2 DS Primitive

The Dialogue Service (DS) primitive is a 4 bit field with the following values assigned for use in the IPS Messaging. The DS peers are the aircraft (avionics) and the IPS Ground System

Value	Assigned DS Primitive
1	D-START

2	D-START cnf
3	D-END
4	D-END cnf
5	D-DATA
6	D-ABORT
7	D-UNIT-DATA*
8	D-ACK
9	D-KEEPALIVE*

* The D-KEEPALIVE DS primitive is different than the IPS Information Message implemented as a part of the port specific messages at the UDP packet level. The IPS Gateway will not generate or process D-KEEPALIVE other than being pass-through for these..

Table 5-17 – ATNPKT DS Primitives

5.10.1.3 App Tech Type

This field identifies the type of application data that is being carried. Four application technology types have been defined:

- b000 – indicating ATN/IPS DS
- b101 – indicating AOC DS
- b010 – indicating management
- b011 – indicating FANS/IPS DS

The IPS Gateway is a pass-through for this field since it does not need to use this field as the port in the UDP header will define the message data.

5.10.1.4 More Bit

The More bit is used to indicate segmentation of the UDP datagrams (specifically the ATNPKT). The More bit usage is as follows:

- 0 – a single segment or the last segment of a segmented message
- 1 – the first or an intermediate segment of a segmented message

The More bit will always be set to “0” for DS Primitives 6, 7, 8, and 9.

5.10.1.5 Presence Flags

The presence flags are 12 bits which indicate the presence of optional fields within the variable part of the ATNPKT. A value of 1 is used to indicate the presence of the optional field. The following are the presence flags as well as the format of the presence field.

Bit	Optional Field	Size (bits)*		Description	Notes
		Length	Value		
0	Source ID	N/A	16	DS connection identifier of the sender	
1	Destination ID	N/A	16	DS connection identifier of the recipient	
2	Sequence Numbers	N/A	8	Sequence numbers (Ns, Nr) Sequence numbers can range from 0 to 15	
3	Inactivity Time	N/A	8	Inactivity timer value of the sender (in minutes)	
4	Called Peer ID	8	24 to 64	Called peer ID (provided by the local DS-user)	1
5	Calling Peer ID	8	24 to 64	Calling peer ID (provided by the local DS-user)	1
6	Content Version	N/A	8	Version of the application data carried	
7	Security Indicator	N/A	8	Security requirements: 0 – no security (default value) 1 – Secured dialogue supporting key management 2 – Secured dialogue 3 … 255 – reserved	
8	Quality of Service	N/A	8	ATSC routing class: 0 – no traffic type policy preference 1 – “A” 2 – “B” 3 – “C” 4 – “D” 5 – “E” 6 – “F” 7 – “G” 8 – “H” 9 … 255 – reserved	
9	Result	N/A	8	Result of a request to initiate or terminate a dialogue: 0 – accepted (default value) 1 – rejected transient 2 – rejected permanent 3 … 255 – reserved	
10	Originator	N/A	8	Originator of the abort: 0 – user (default value) 1 – provider 2 … 255 – reserved	
11	User Data	16	0 to 8184	User data (provided by the local DS-user)	

1 = this field has customized meaning for A620 data (see corresponding section for definition)

* = when length is present it always precedes the value

Table 5-18 – ATNPKT Presence Fields

5.10.2 Variable Part

The variable part of the ATNPKT is dependent on the presence fields flagged in the fixed part of ATNPKT, the DS primitive being invoked, and the state of the DS.

The following table identifies the ATNPKT parameters present for each of the DS protocol messages. The table includes the fixed variables (always present) and the variable fields.

Protocol Message	**D-START**	**D-START cnf**	**D-DATA**	**D-UNIT-DATA**	**D-END**	**D-END cnf**	**D-ABORT**	**D-ACK**	**D-KEEPALIVE**
Fixed part									
ATNPKT version	M	M	M	M	M	M	M	M	M
DS Primitive	M	M	M	M	M	M	M	M	M
Application Technology Type	M	M	M	M	M	M	M	M	M
More	M	M	M	M(5)	M	M	M(5)	M(5)	M(5)
Presence Flags	M	M	M	M	M	M	M	M	M
Variable part									
Source ID	M(4)	M(4)	-	-	-	-	(1)	-	-
Destination ID	-	M(4)	M(4)	-	M(4)	M(4)	M(2)	M	M
Sequence numbers	M(4)	M(4)	M(4)	M	M(4)	M(4)	M	M	M
Inactivity time	O(3)	O(3)	-	-	-	-	-	-	-
Called peer ID	O(3)	-	O(6)	O	-	-	-	-	-
Calling peer ID	O(3)	-	O(6)	O	-	-	-	-	-
Content version	O(3)	O(3)	-	O	-	-	-	-	-
Security indicator	O(3)	O(3)	-	O	-	-	-	-	-
Quality of service	O(3)	-	-	-	-	-	-	-	-
Result	-	M(3)	-	-	-	M(3)	-	-	-
Originator	-	-	-	-	-	-	O	-	-
User Data	O(4)	O(4)	M(4)	M	O(4)	O(4)	O	-	-

(O = optional, M = mandatory, - = precluded to use)

(1) Source ID is present if D-ABORT is sent after D-START and before D-START cnf is received.

(2) Destination ID is absent if D-ABORT is sent after D-START and before D-START cnf is received.

(3) For segmented messages, this parameter is present only in the first segment.

(4) For segmented messages, this parameter is present in all the segments.

(5) The More bit is always set to “0”

(6) Used for A620 messages (see Table 5-20), for segmented messages, only present in first segment.

Table 5-19 – ATNPKT Content for DS Protocol Messages

The custom use for A620 data of select fields is further detailed in Table 5-20.

	Called Peer		Calling Peer	
	Downlink	Uplink	Downlink	Uplink
AOC	-	-	Flight ID*	-
FANS1/A	Center name	-	Flight ID*	Center name

*included only when ID changes for flight reauthenticates

Table 5-20– Custom field use for A620 data

5.10.2.1 Source ID

The Source ID identifies the DS connection at the sender side when present in the D-START, D-START cnf, and D-ABORT primitives. The source ID is a 2 byte field that conforms to ISO 8208 field definition.

5.10.2.2 Destination ID

The destination ID identifies the DS connection at recipient side and is present in the D-START cnf, D-DATA, D-END, D-END cnf, D-ABORT, D-ACK and D-KEEPALIVE primitives. The destination ID is a 2 byte field that conforms to ISO 8208 field definition.

5.10.2.3 Sequence Numbers

The sequence number is an 8 bit field and is present in all DS primitives. The field consists of the sequence number sent and the next sequence number to be received and is laid out as shown in Figure 5-39.

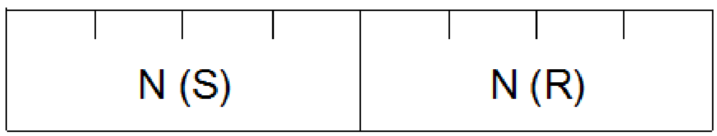


Figure 5-39 – Sequence Number Format

N(S) – sequence number of ATNPKT sent

N(R) – next expected ATNPKT sequence number to be received

There are 16 [0..15] possible sequence numbers. For D-ACK and D-KEEPALIVE, only the N(R) number is meaningful.

5.10.2.4 Inactivity Time

The inactivity time represents the time (in minutes) of the inactivity timer on the send side. The use of this field is not required for IPS Communications where the IPS Gateway is the IP termination point (for A620 Host communications). Use of this for IPS Aircraft to IP Ground System is to be defined by those end systems.

5.10.2.5 Called Peer ID

The called peer ID identifies the intended peer DS-user. The called peer ID will be either a 24-bit ICAO aircraft identifier or a 3–8 character ICAO facility designation and have the format 24 to 64 bits. This is an optional field with D-START.

If the D-DATA or D-START primitive is for FANS 1/A data downlink, then this field is a 4-7 byte mandatory field and the meaning of this field is defined to be the Center Name.

5.10.2.6 Calling Peer ID

The calling peer ID identifies the initiating peer DS-user. The calling peer ID will be either a 24-bit ICAO aircraft identifier or a 3–8 character ICAO facility designation and have the format 24 to 64 bits. This is an optional field with D-START.

If the D-DATA or D-START primitive is for AOC data downlink, then this field is an 8 byte optional field and the meaning of this field is redefined to be the ICAO flight ID. This field will be populated by the aircraft whenever the flight ID has changed or the aircraft has re-authenticated.

If the D-DATA or D-START primitive is for FANS 1/A data downlink, then this field is a 4-7 byte mandatory field and the meaning of this field is defined to be the Center Name.

5.10.2.7 Content Version

The content version field is used to indicate the application's version number.

5.10.2.8 Security Indicator

The security indicator is an 8 bit field used to convey the level of security. The possible values of this field are shown in the Table 5-21.

Value	Security Level
0	No security (default value)
1	Secured dialogue supporting key management
2	Secured dialogue
3 - 255	Reserved

Table 5-21 – ATNPKT Security Indicator Presence Field

The IPS Gateway will not use this indicator as security is handled at the IPv6 level. The IPS Gateway will forward the content to IPS Ground System.

5.10.2.9 Quality of Service

The Quality of Service (QoS) is an 8 bit field use to convey the quality of service. The IPS Gateway will not use this optional field. The IPS Gateway will forward the content to IPS Ground System.

5.10.2.10 Result

The result is an 8 bit field set by the destination DS-user in order to indicate whether or not the requested dialogue initiation or termination completed successfully. The possible values of this field are shown in the Table 5-22.

Value	Result Definition
0	Accepted
1	Rejected (transient)
2	Rejected (permanent)
3 - 255	Reserved

Table 5-22 – ATNPKT Result Field

5.10.2.11 Originator

The originator is an 8 bit field that indicated the source of a D-ABORT. The possible values of this field are shown in Table 5-23.

Value	Originator Definition
0	User (default)
1	Provider
2 - 255	Reserved

Table 5-23– ATNPKT Originator Field

5.10.2.12 User Data

The user data field of the ATNPKT contains application data. The user data is variable size, 0 bytes to a maximum of 8184 bytes.

The first two bytes contain the user data length (in bits). Following the 2 bytes of the length there is a single byte (compression byte) used to indicate whether the user data is compressed.

Bit	Meaning	Description
1-4 (LSB)	Compression field	0 - No compression 1 - indicates deflate compression 2-15 to be defined for future compression method to be used
5-8	Reserved	

Table 5-24 – Compression byte content

<u>Data Fragmentation</u>

The ICAO Doc. 9896 [1] requirement is that a D-DATA with a user data part exceeding 1024 bytes shall be segmented using the More bit in the ATNPKT fixed header part. This requirement defines the maximum size of the D-DATA that the IPS Gateway will receive.

The maximum size of the IPv6 packet is 1280 bytes. The following table illustrates that the maximum ATNPKT size fits easily fits into the IPv6 packet.

Allocation	Bytes
IPI	1
IPv6 Header	40
UDP Header	8
ATNPKT Fixed part	3
ATNPKT variable part (excluding user data), includes length of user data	31
ATNPKT user data	1024
MIC	4
Total	**1111**

Table 5-25 – IPv6 packet allocation

5.11 Error Detection

IPS communications can encounter many different types of errors, from busted messages while in transit to/from the ground station, the IPS Gateway down, the Ground Systems down, the IPS Aircraft avionics impaired, and etc. This section details the error messages that are supported by the IPS Gateway.

5.11.1 ICMPv6 messages

When a message successfully transits the RF from Aircraft to Ground station, there are still many issues that could occur. The ground network will attempt to deliver each message to its intended destination via the IPS Gateway. There are a few issues that could arise; each will be responded to via an ICMPv6 message.ICMPv6 Messages take the form shown in Figure 5-40.

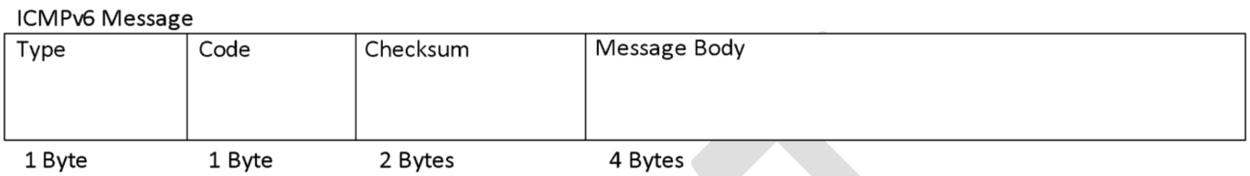


Figure 5-40 - ICMP Message Format

While there is an extensive set of ICMP messages that could be sent in an IPv6 network. The following ICMP messages will be initially supported.

Type	Code	Error Message	Example Scenario
1	0	No route to destination	If an IPS Ground System network is down then this message will inform the aircraft.
1	3	Address Unreachable	The particular computer this message is addressed for is powered off.
1	4	Port Unreachable	The particular application this message is address for is not running
1	5	Source address failed ingress/egress policy	Sent message is restricted from transmission by country or DSP policy. IE encryption in China
128	0	Echo Request	The Aircraft or IPS Gateway wishes to verify connectivity is up. This message is sent at the direction of the operator(s).
129	0	Echo Reply	The Aircraft or IPS Gateway is responding to the Echo Request and is operational.

Table 5-26- Supported ICMP Messages

5.11.2 IPS Gateway DTLS/TLS Alert Messages (port 5908 key tag 0x0A)

The IPS Gateway will send DTLS/TLS Alert Messages to indicate warnings, and fatal errors during the authentication process (port 5098 key tag 0x0A) for IP based media. Key tag 0x0A for AVLC based media.

Aircraft should be able to receive these messages without negative consequences. While it is desirable that the aircraft use these messages to guide the authentication and connection processes, each avionics manufacturer may develop their own methodology. Alert messages will only be sent for messages that header information is intact; otherwise messages busted in RF will be ignored. The Alert Protocol Message shall be the same as recorded in RFC 5246 and takes the form:

Alert Protocol

Alert Level	Alert Description
1 Byte	1 Byte

Alert messages will take the form of Warning and Fatal errors. Warnings can be ignored however it would be useful to log or present the error to the operator. While the IPS Gateway will be able to handle all alert types, the following alert types would be useful to the avionics.

Alert Levels can be one of:

Alert Level	Example	Meaning
Warning	0x01	This is an informational message, and should probably be logged.
Fatal	0x02	There has been an unrecoverable error with the login. Details in Description.

Table 5-27 - DTLS Alert Levels

Useful Alert Descriptions can be

Alert Description	Example	Meaning
close_notify	0x00	The aircraft or IPS Gateway would like to close the connection. The IPS Gateway may send this when the session has been open for 8 hours and requires renegotiation. This may also be sent after key management commands.
handshake_failure	0x40	A general error with the negotiation. Usually fatal and requires a new handshake.
Unsupported_certificate	0x43	The certificate presented is not authorized for use on the ground network for this provider. Fatal message.

Table 5-28 - DTLS Useful Alert Messages

The following alerts will all be Fatal, however they will never be transmitted to the aircraft. The IPS Gateway log will record the fatal message and associated certificates presented that generated the alerts, as well as any relevant information regarding the failure. Silently recording these fatal messages will prevent Denial of Service attacks against the local provider’s network or the avionics.

Alert Description	Example	Meaning
Certificate_revoked	0x44	The certificate presented exists on a certificate revocation list. Fatal message.
Certificate_expired	0x45	The certificate presented validity dates are outside of the current date. (Either used before validity or after validity). Fatal message.
Unknown CA	0x48	The certificate presented is signed by a CA that is not recognized by this service provider. Fatal message.

Table 5-29 - DTLS Log only alerts

* If aircraft tries more than 3 times the revoked certificate, then the aircraft should be added to the revoked client list until human interaction can be established.

5.11.3 IPS Gateway TLS/DTLS Message Alert Messages (non-authentication)

Some TLS Alert Messages may be generated after the authentication process. The alert protocol is the same as described above, using port 5098 key tag of 0x0A. The following are the anticipated alerts.

Alert Description	Example	Meaning
bad_record_mac	0x20	Message received did not pass the message integrity check. This is often a warning message.
decompression_failure	0x30	Message received could not be decompressed. This is often a warning message.

Table 5-30 – IPS Gateway Alert Messages (non-authentication)

6 Interface Details

As shown in Figure 3-1Figure 3-1, the IPS Gateway supports IPS Aircraft Communications through:

- Authentication Processing between the IPS Aircraft and the IPS Gateway
- IPS (IPv6) Ground System Session Establishment and Messaging
- A620 (Legacy) Host System Messaging
- ATN/OSI Ground System Connectivity and Messaging

This section looks in detail at various messaging to or through the IPS Gateway.

6.1 Authentication

Authentication is initiated by the IPS Aircraft to the current services provider's IPS Gateway. Authentication messages are not forwarded to any companion service area's IPS Ground System.

Authentication will be performed through many steps called DTLS Flights (shown in Figure 6-1) where security parameters will be exchanged and a secured communication path will be established. The IPS Aircraft and the IPS Gateway shall use Deflate compression on all the messages including all the authentication handshake process messages. Message Integrity code (MIC) checks are not included until after the authentication process is complete.

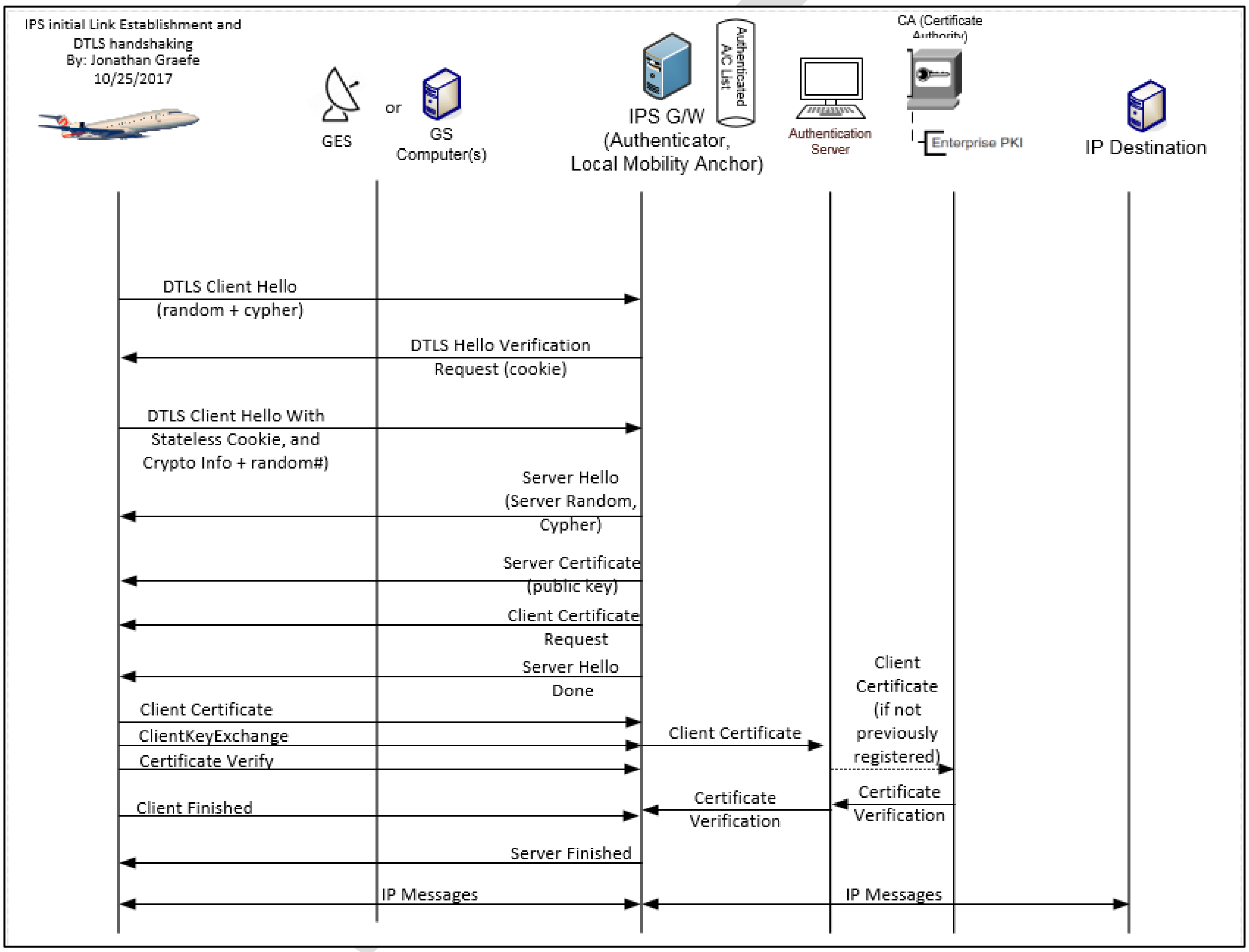


Figure 6-1 – IPS/DTLS authentication flights

General order of operation for a new connection:

1) Aircraft detects IPS availability (either GSIF advertising or route solicitation)
2) Aircraft sends a DTLS Client Hello Message leaving the opaque cookie blank.
3) The IPS Gateway responds with a HelloVerifyRequest providing an opaque cookie.
4) Aircraft resends the DTLS Client Hello Message but inserts the opaque cookie into the message.
5) Gateway sends a series of server authentication messages including:

   a. A Server Hello with the parameters of this session
      i. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
      ii. Curve is secp384r1
   b. The IPS Gateway sends a x.509 DER encoded public certificate to the aircraft
   c. ServerKeyExchange: The elliptic curve parameters including the ECDHE key are sent
   d. A request for the aircraft’s certificate specifying the curve it expects
   e. A message stating that the Gateway has completed its side of the authentication
6) Aircraft sends a burst of messages including:
   a. The aircrafts public x.509 DER encoded certificate is sent to the gateway
   b. ClientKeyExchange: an ECDH Ephemeral key
   c. A certificate verify message passing a signed hash of all messages up to this point. Proves the aircraft has the private key.
   d. Message to begin applying the negotiated DTLS parameters
   e. an encrypted, MICed and compressed message indicating the client is finished with the authentication
7) The Server completes the authentication process by applying the negotiated parameters
   a. Server issues a Session Ticket
   b. Server sends a changeCipherSpec in the clear
   c. An encrypted, MICed and compressed message indicating that the server is finished with the authentication and the DTLS session is now fully established.
8) The Aircraft send via the MICed authentication channel:
   a. Aircraft sends IPv6 address, Tail ID and Flight ID to the gateway

6.1.1 Aircraft Detects IPS Availability

VDL enabled ground stations will advertise the availability of services periodically via a Ground Station Information Frame (GSIF). Upon hearing a GSIF that advertises IPS availability the aircraft may initiate a DTLS connection with the IPS Gateway. The ground stations that do not support IPS will ignore any request for IPS service(s). For Satcom after establishment of the Satcom link, availability of IPS service is determined by the avionics through a route solicitation message.

6.1.2 Initial Client Hello

Upon hearing a GSIF that advertises IPS availability the aircraft can immediately initiate an IPS/DTLS logon when the frequency is clear. The initial client hello (shown in Table 6-3) will be missing an opaque cookie later provided by the IPS Gateway. The cookie is used to detect denial of service attacks against the service provider. It is intended that the initial Cipher Suite for IPS will be TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and all IPS messages including authentication messages will be compressed using the Deflate compression method. It is expected that the supported cipher list will expand in time as new methods are invented and legacy methods retired.

The Client Hello Message informs the server about the capabilities of the client.

DTLS Header Fields DTLS Handshake messages and their Meaning:

Field Name	Example Value	Meaning
Content Type	0x16 [1 Byte]	The following message is a DTLS Handshake Protocol Message – these are primarily used for authentication and session management.
Protocol Version	0xFE 0xFD [2 Bytes]	The aircraft supports DTLS Version 1.2 and below.
Epoch Cypher #	0x00 0x00 [2 Bytes]	This message is using the first cipher method negotiated. In this case the default, no encryption or Message integrity code, but compressed using deflate.
Message Seq#	0x00 0x00 0x00 0x00 0x00 0x00 [6 Bytes]	Message Sequence Number. Number represents the number of messages sent starting at 0x00. Both the server and client have their own unique counter and increment them for messages sent by each respective side.
Length	0x00 0x65 [2 Bytes]	The Total length of the data payload of the message. In this case starting from the Handshake Protocol header

Table 6-1 - DTLS Header Fields for DTLS Handshake Messages

Handshake Protocol Header fields for Initial Client Hello and their Meaning:

Field Name	Example Value	Meaning
Handshake Type	0x01 [1 Byte]	This is a Client Hello message
Length	0x00 0x00 0x59 [3 Bytes]	The total length of the Client Hello header
Message Seq	0x00 0x00	Message Sequence Number. Similar to the Message sequence number

	[2 Bytes]	of the DTLS header, but counts the steps of the authentication handshake. This sequence number does not necessarily need to be the same as the DTLS header message sequence number but it could be.
Fragment offset	0x00 0x00 0x00 [3 Bytes]	The first byte of this fragment position in the entire message. For instance this may be a fragment in the middle of the message, in that case this field is the position of the first byte of this packet in the assembled message.
Fragment Length	0x00 0x00 0x59 [3 Bytes]	The length of this fragment. If this fragment contains the full message then the length field and this field will match.

Table 6-2 - Handshake Protocol Header for initial Client Hello

Client Hello Header fields and their Meaning:

Field Name	Example Value	Meaning
Protocol Version	0xFE 0xFD [2 Bytes]	Represents the aircraft supports the DTLS 1.2 protocol and below for handshakes.
Random	Varies [4 Bytes + 28 Bytes]	A two part random number. The first 4 Bytes is the number of seconds since January 1, 1970. The Last 28 Bytes are a random number generated by the client.
Session ID	Varies [2 Bytes + Variable Bytes]	The first 2 Bytes represent the length of data to follow for this field. The remaining bytes are the session ID issued by the server (IPS Gateway), that this aircraft would like to resume. It is acceptable that the aircraft initiates a new connection for each authentication.
Opaque Cookie	0x00 [1 Byte + Variable]	The opaque cookie is a server based denial of service detection method. Initially this will be a 1 Byte length field of 0x00 and a variable part of 0 Bytes.
Cipher Suite	0x00 0x04 0xCO 0x2C 0x00 0xFF	This is the field where the client informs the server all the cipher suites that it can support the server later will choose one. The list is presented in order of preference. The first 2 Bytes is the length in Bytes of the list The second 2 Bytes represent TLS_ECDHE_ECDSA_WITH_AES_GCM_SHA384 The third 2 Bytes represent TLS_EMPTY_RENEGOTIATION_INFO_SCSV
Compression	0x02	Represents the compression methods that the client can support. The

	0x01 0x00	list is presented in order of preference. The first Byte is the length in Bytes of the list The second Bytes represents DEFLATE compression The third Byte represents none compression

Table 6-3 – Initial Client Hello Message

6.1.2.1 Client Hello Extensions Format

Client Hello Extensions are used to convey additional information or request a modification to the behavior of standard DTLS connections. IANA maintains a list of currently accepted Extension Types which can be found in the Applicable documents section.

The DTLS/TLS extension header consists of a single length field representing the total length of all extensions summed together.

Each DTLS/TLS extension has the following format:

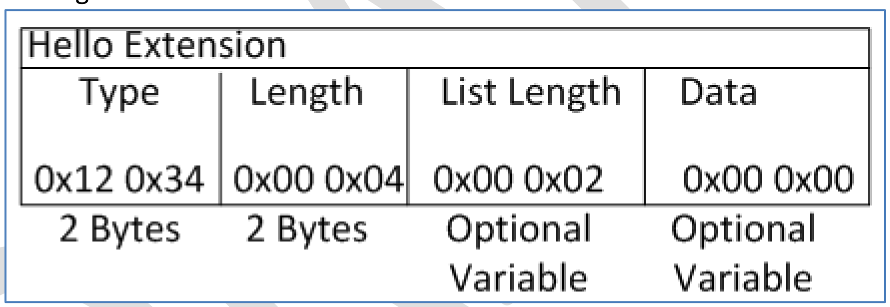


Figure 6-2 – DTLS Hello Extension Format

Field Name	Example Value	Meaning
Type	0x12 0x34 [2 Bytes]	Identifies the Extension name that is being modified or feature being requested.
Length	0x00 0x04 [2 Bytes]	The length of the List Length and Data field in bytes.
List Length	0x00 0x02 [0 or 2 Bytes]	This field may or may not be present. If it is present, it is two bytes. This field is present every time there is the possibility of a list of items; it represents the number of bytes of the list and is two less than the length field.

Data	0x00 0x00 [Variable 0 – 65535 Bytes]	The actual requested method for this extension type. This could be blank in the client hello to represent that the client supports this service.

Table 6-4 – Extended Hello Format

6.1.2.2 Client Hello

For purposes of IPS it is recommended that the client maintain at least the following extension capabilities however support for all extensions is recommended. Servers are expected to support most extensions including those listed below.

1. Elliptic Curve Point Format – Defined in RFC 4492. This extension informs the Gateway that the aircraft can support custom elliptic curves where the points are transmitted in a certain format. This field is recommended when elliptic curve cryptography is used, even when using named curve.
2. Supported Groups – Defined in RFC 4492. This extension informs the Gateway that the aircraft supports named elliptic curves. This field includes a list of all curves supported.
3. Session Ticket TLS – Defined in RFC 5077. This extension informs the Gateway that the aircraft supports session tickets. Tickets can be used to resume sessions with gateways that are load balanced and have a large number of supported aircraft.
4. Signature Algorithms – Defined in RFC 5246 this extension informs the Gateway of all the signature and hashing algorithms that the aircraft supports.
5. Extended Master Secret – Defined in RFC 7627. The Aircraft supports man in the middle attack detection and will generate a master secret that is resistant to man in the middle style of attack.

Field Name	Type Value assigned	Length Example	List Length (if applicable)	Data Example and meaning
Elliptic Curve Point Format	0x00 0x0B	0x00 0x05	0x00 0x03	0x00 Uncompressed 0x01 Compressed Prime 0x02 Compressed Char2
Supported Groups (AKA Elliptic Curves)	0x00 0x0A	0x00 0x04	0x00 0x02	0x00 0x18 secp384r1
Session Ticket TLS	0x00 0x23	0x00 0x00	(--)	-- Supported
Signature Algorithms	0x00 0x0D	0x00 0x04	0x00 0x02	0x05 0x03 SHA384 with ECDSA
Extended Master Secret	0x00 0x17	0x00 0x00	(--)	-- Supported

Table 6-5 – Client Hello

The DTLS heartbeats will be handled via the IPS Information messages the aircraft will send periodically. See section 5.6 for more information.

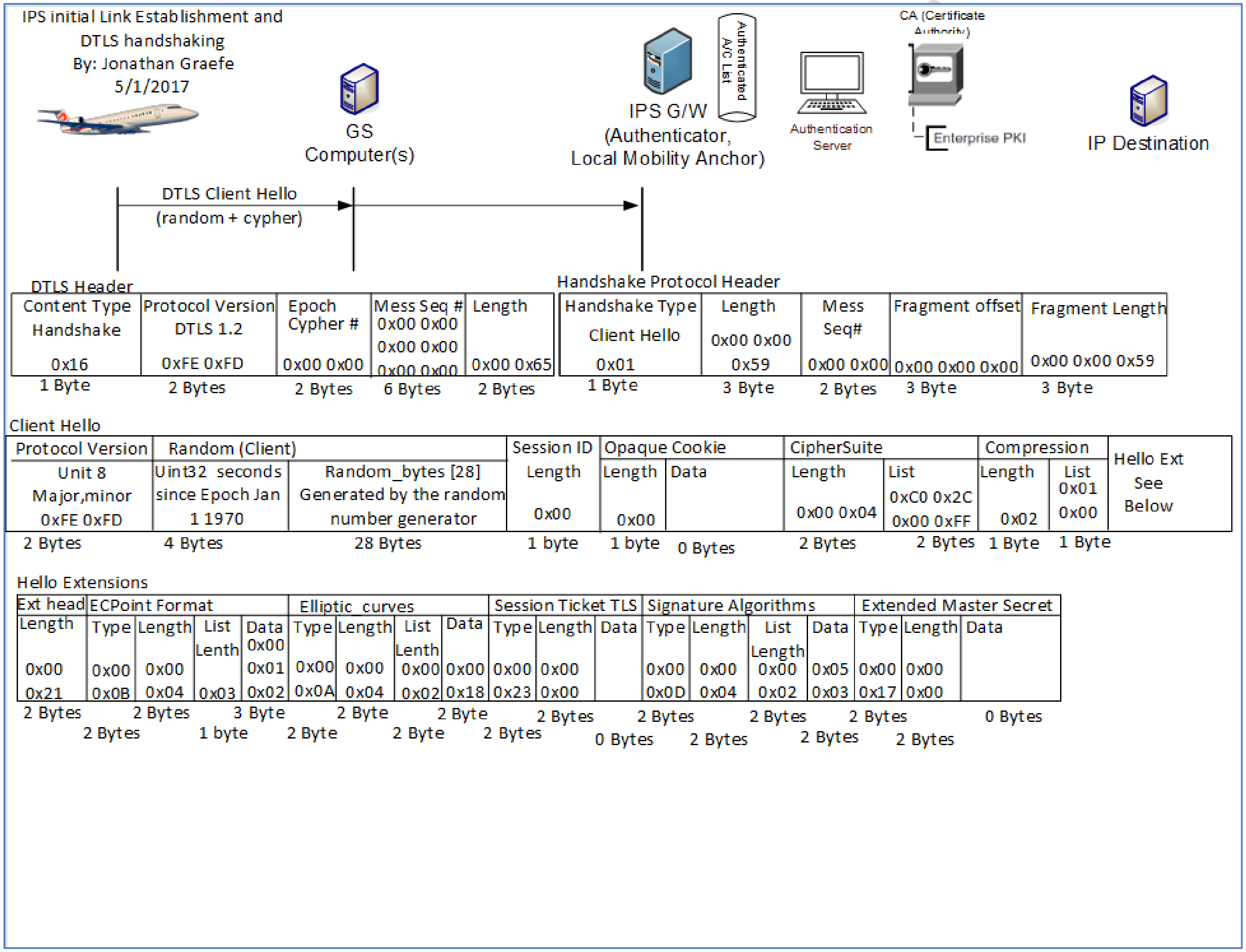


Figure 6-3 – Initial Client Hello

6.1.3 Hello Verify Request

In order to detect denial of service (DOS) attacks and also detect replay attacks, the IPS Gateway generates a random opaque cookie and sends it to the aircraft. The aircraft proves that it can receive messages from the IPS Gateway by including the opaque cookie in its follow up client hello message. The opaque cookie is random and shall not be the same as any previous resumable session. The Hello Verify Request is the message that contains the opaque cookie and is detailed below.

The DTLS header fields descriptions are the same as recorded in section 6.1.2 (Initial Client Hello). The Handshake Protocol header is similar to the Initial Client Hello with the exception that the Handshake Type is: 0x03 Hello Verify Req.

The Hello Verify Request Message has the following fields:

Field Name	Example Value	Meaning
Protocol Version	0xFE 0xFD [2 Bytes]	Represents that the Gateway supports the DTLS 1.2 protocol and below. DTLS 1.2 will be used for this handshake.
Length	0x14 [1 Byte]	The Length of the opaque cookie
Opaque Cookie	Varies [0-255 Bytes]	This is the cookie the IPS Gateway directs the aircraft to use.

Table 6-6 – Hello Verify Request

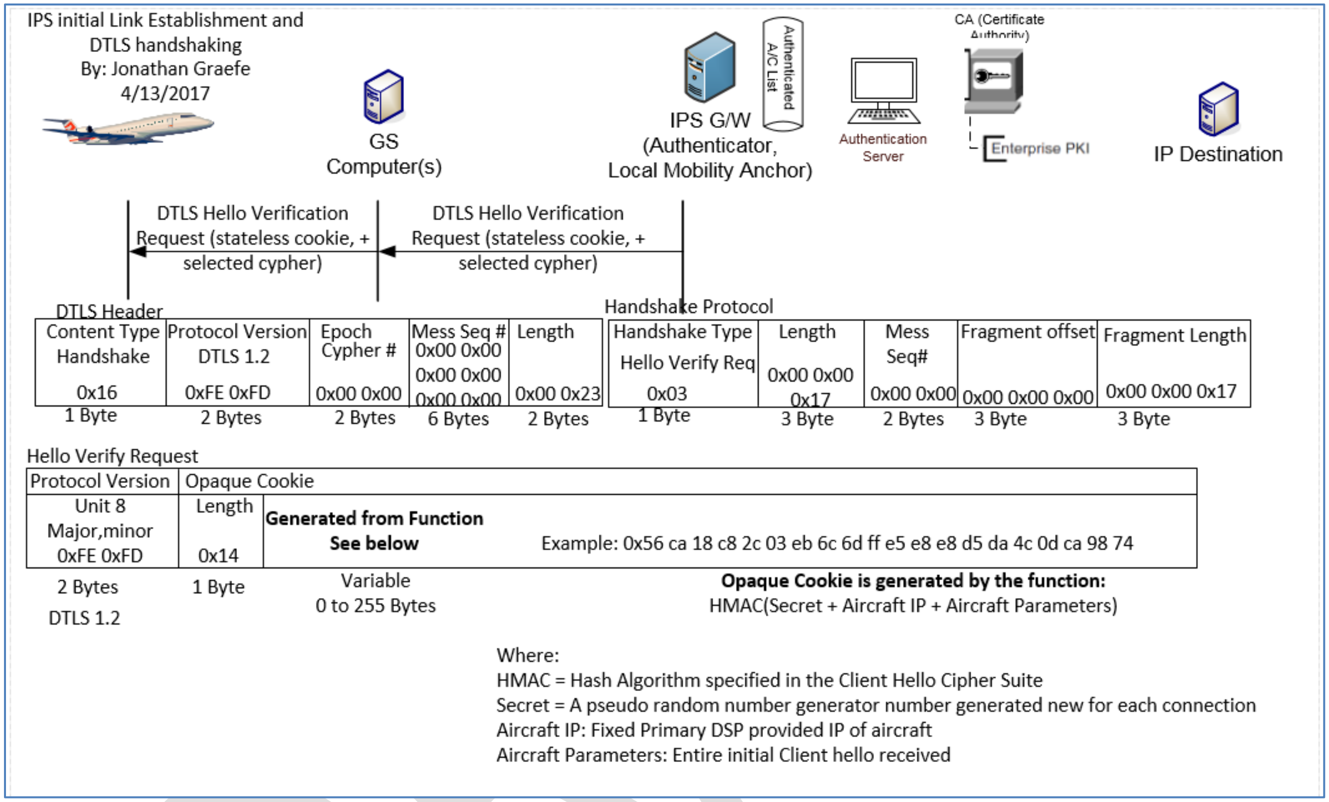


Figure 6-4 – Hello Verify Request

6.1.4 Second Hello Request

The aircraft upon successfully hearing a Hello Verification request from the IPS gateway shall extract the Opaque Cookie and insert it into the Client Hello Message. Transmission of the second Client Hello message will guarantee that the server can successfully send messages to the Aircraft and the aircraft can successfully transmit to the IPS Gateway. The Gateway expects the client hello to remain the same except for a few fields. Any other changes will result in a failed handshake.

The only fields that have changes from the initial client hello are:

Field	Explanation
DTLS Header Message Sequence Number	The Message Sequence number increments for every message sent. Since this is the 2nd message sent by the aircraft it is assigned sequence number 1.
DTLS Header Length	With the addition of the opaque cookie, the length of the packet has increased. Length captures the new length.
Handshake Protocol Header Length	With the addition of the opaque cookie, the length of the packet has increased. Length captures the new length.
Handshake Protocol Header Message Sequence Number	The Message Sequence number increments for every message sent during this handshake the IPS Gateway uses this number to determine that this is the second client hello and it should expect to find an opaque cookie matching what it sent previously.
Handshake Protocol Header Fragment Length	Assuming the message does not require fragmentation this Length would equal the Handshake Protocol Header Length
Client Hello Opaque Cookie Length	Length will change from 0x00 to the length of the opaque cookie.
Client Hello Opaque Cookie Data	This opaque cookie received in the Hello Verify Request will be placed here.

1887 **Table 6-7 – Second Hello Request**

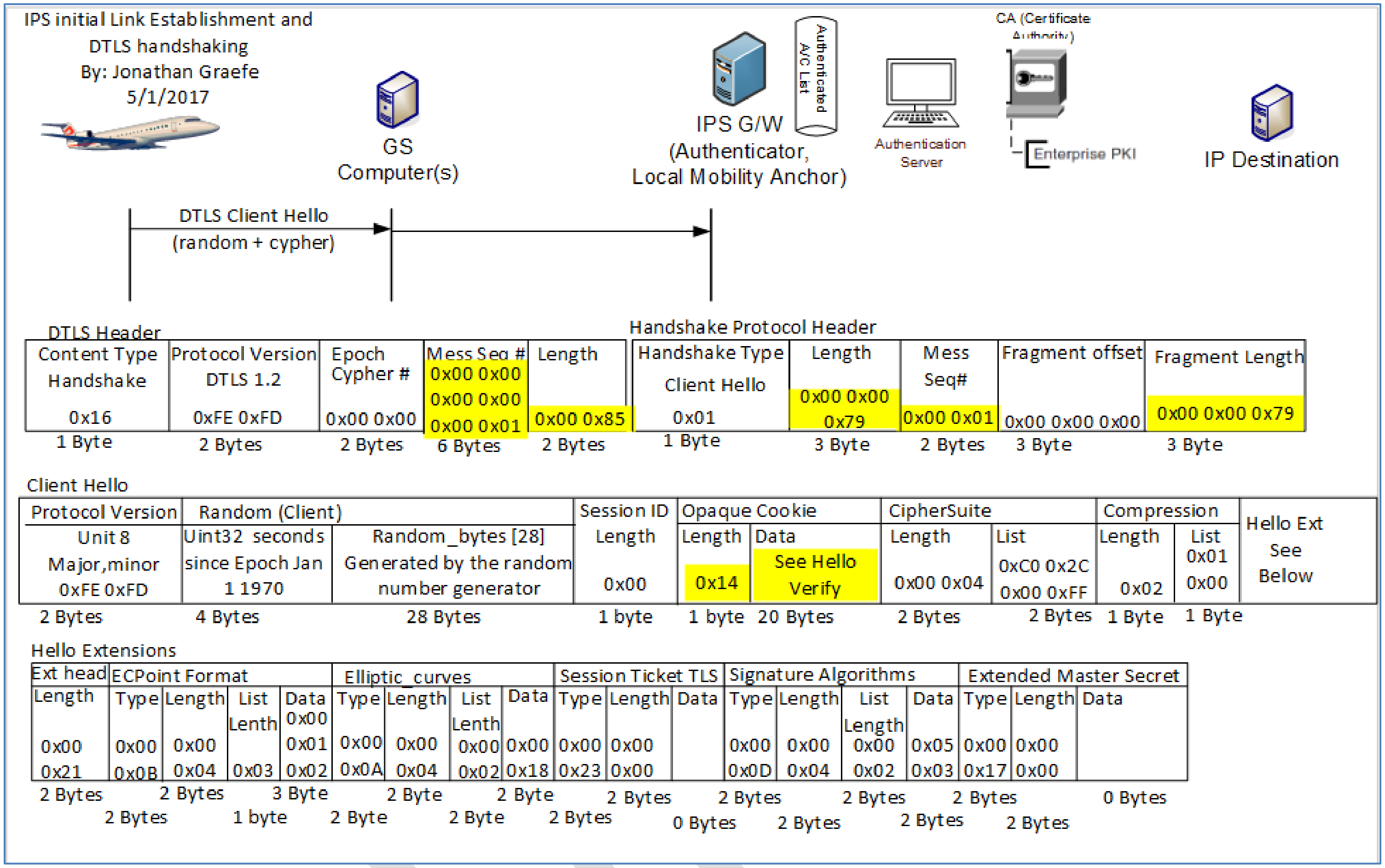


Figure 6-5 – Second DTLS Client Hello

6.1.5 IPS Gateway Authentication Messages

The IPS Gateway sends a burst of messages to authenticate itself to the aircraft. These messages include a Server Hello, Server Certificate message, a Server ECDHE Key exchange, a client certificate request and a server finished message.

6.1.5.1 Server Hello

The IPS Gateway initiates a server hello message to the client, specifying the maximum DTLS version number it supports, the cipher it has chosen for this session, compression method and a random integer. These choices are based upon the capabilities presented during the client hello message(s) received from the aircraft earlier. The client is expected to use the server hello message information to build a secured communication method to the IPS Gateway. The Sever Hello Message may take the suggested form detailed below.

The DTLS Header field descriptions are the same as recorded in 6.1.2 (Initial Client Hello); the only difference is in this case the server (IPS Gateway) is sending a message to the client (Aircraft). The Handshake Protocol Header is similar to the Initial Client Hello with the exception that the Handshake Type is 0x02 Server Hello. The details are provided below:

Handshake Protocol Header

Field Name	Example Value	Meaning
Handshake Type	0x02 (1 Byte)	This is a Server Hello Message

Server Hello Message

Field Name	Example Value	Meaning
Protocol Version	0xFE 0xFD [2 Bytes]	The server supports DTLS Version 1.2 and lower
Random	Varies [4 Bytes + 28 Bytes]	A two part random number that is unique from the client random. The first 4 Bytes represent the seconds since Epoch – January 1, 1970. The Last 28 Bytes are a random number generated by the server. This 28 Bytes should be different from the client random; otherwise a man in the middle attack is possible.
Session ID	Varies [2 Bytes + Variable Bytes]	The first 2 Bytes represent the length of data to follow for this field. The remaining bytes are the session ID issued by the server (IPS Gateway). This number is unique for every active connection. The server may choose to not include a session ID if sessions are not resumable, or if the session resumption is

		handled via a different method.
CipherSuite	0xC0 0x2C [2 Bytes]	This is the cipher suite chosen by the server (IPS Gateway). The server has chosen from the list presented by the client. It considers the CipherSuite list in order of client preference. The 2 Bytes represent TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Compression	0x01	Represents the compression method chosen by the server from the list presented by the client. In this case the server has chosen DEFLATE compression.

1910 **Table 6-8 – Server Hello Message**

1911

1912 *Server Hello Extensions*

Field Name	Type Value Assigned	Length Example	List Length (if applicable)	Data Example and Meaning
Renegotiation Info	0xFF 0x01	0x00 0x01	0x00	-- Renegotiation Info Supported
EC Point Format	0x00 0x0B	0x00 0x04	0x03	0x00 Uncompressed 0x01 Compressed Prime 0x02 Compressed Char2
Session Ticket TLS	0x00 0x23	0x00 0x00	--	-- Session Ticket TLS Supported
Extended Master Secret	0x00 0x17	0x00 0x00	--	-- Extended Master Secret Supported

1913 **Table 6-9 – Server Hello Extensions**

1914

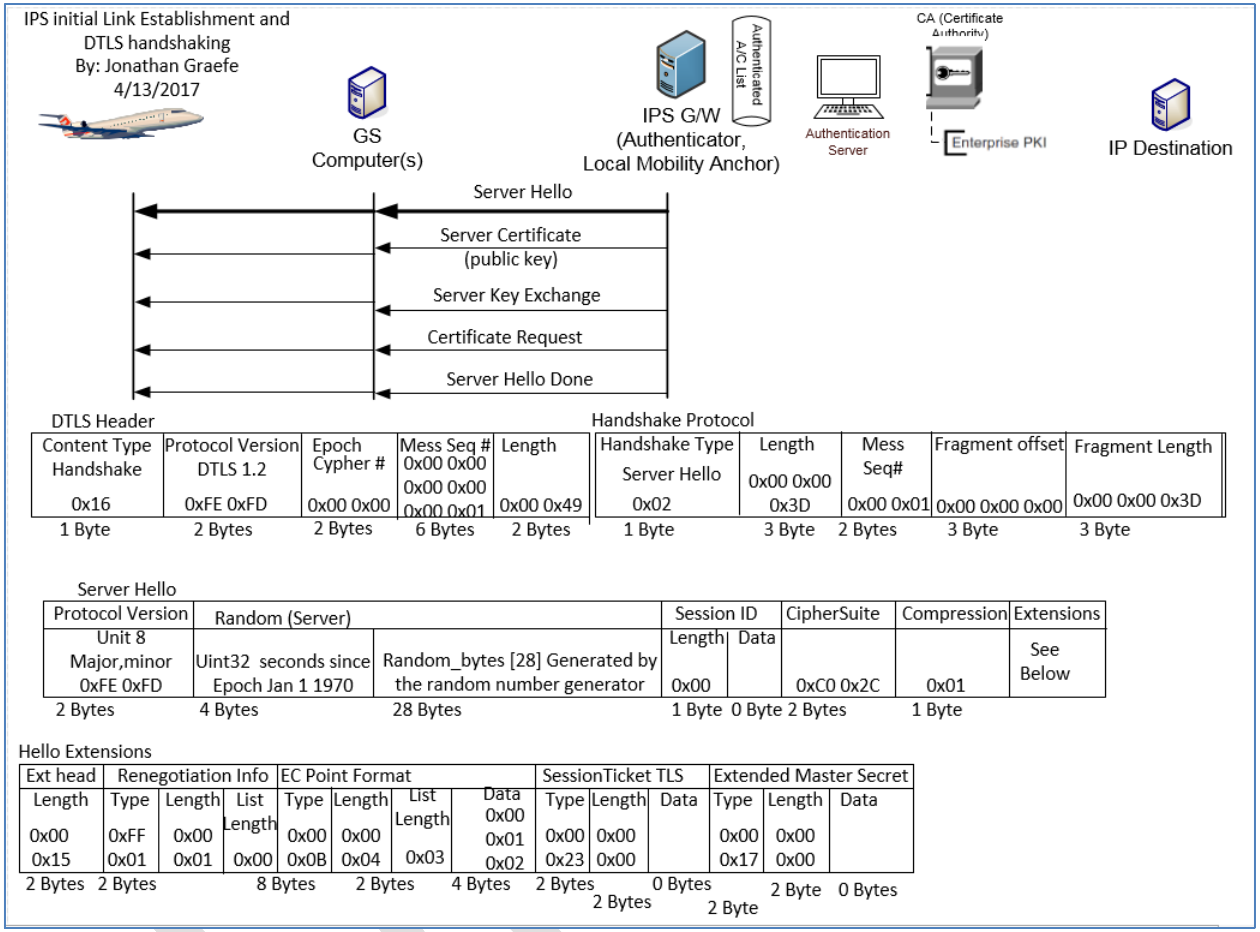


Figure 6-6 – Server Hello

6.1.5.2 Server Certificate

The IPS Gateway will send its own public x.509 certificate, to the IPS Aircraft. The IPS Gateway may also send a root CA certificate to validate the IPS Gateway's server certificate. It is recommended that the first communication of the day with a service provider be a full x.509 certificate handshake. If any keys need to be updated it can be done via this daily full x.509 handshake. The IPS Gateway's public key will be used if as required to encrypt messages from the IPS Gateway with key tag of 0x0A and 0x30 to 0x3F. The RootCA Certificate is used to validate both the IPS Gateway's server key, and if it is the primary service provider, the aircrafts own key. The aircraft will compare the public key with its directory of service provider's keys to validate that the service provider's key is valid. Aircraft are expected to re-authenticate every 8 hours or at the beginning of each flight whichever comes sooner.

6.1.5.2.1 Server Authentication Methods

There are two types of acceptable authentication.

1) Full X.509 certificate exchange. The x.509 certificate and that of the signing root CAs will be exchanged with the aircraft. The aircraft can then perform a decision tree on whether to accept or not the authenticity of the presented certificate. For purposes of this tree the directory certificate is the last known good certificate stored in the aircraft's CMU. It is expected that all aircraft will support full x.509 certificate exchanges.
2) Modified X.509 certificate exchange. The gateway's X.509 Certificate only will be sent to the aircraft. The aircraft can then perform a decision tree on whether to accept or not the authenticity of the presented certificate. The aircraft should have the gateway's certificate preloaded into either the Primary Service Provider's certificate store or one of the Trusted Companion Certificate slots. If not then abort the connection. If so set the appropriate level of permissions (primary vs trusted companion) and continue the authentication process. The aircraft may send its Certificate only or the entire certificate chain. This type of exchange only works if both the aircraft and gateway certificates clearly indicate their signing authority trust anchor (CA Certificate).

6.1.5.2.2 Decision Tree for X.509 key exchanges

Decision Tree for x.509 key exchanges:

1) Directory IPS Gateway certificate and received IPS Gateway certificate match and are not expired. Then proceed with authentication.
2) Directory IPS Gateway certificate and received certificate match but both are expired. Proceed with authentication. The server will likely follow up with a new certificate to be installed.
3) Directory IPS Gateway certificate and received certificate do not match. Abort the connection.
4) RootCA Certificate is expired, but the directory IPS Gateway certificate and the installed certificate match, both are likely expired. Abort Authentication.
5) RootCA Certificate is expired; directory IPS Gateway certificate and installed certificate do not match. Abort the connection, there may be an imposter IPS Gateway.
6) Directory does not contain a certificate and/or rootCA Certificate for this provider. Switch Providers/media.

6.1.5.2.3 Example Certificate Exchange

The certificate exchange is likely to be fragmented over many packets. This example shows the message as one packet.

Certificate Packet

Field Name	Example Value	Meaning
Certificates Length	0x00 0x02 0x7C [3 Bytes]	Represents the total number of bytes that follow in this message, including all keys and key length headers.
Length of this Key (one for each key)	0x00 0x00 0x3E [3 Bytes]	The length of the key to immediately follow this message. There is one 'Length of this key' field for each certificate presented.
RootCA Certificate	Varies [0 – 24 Bytes]	The Key information for the rootCA key.
Length of this Key	0x00 0x00 0x3B [3 Bytes]	The length of the key to immediately follow this message. There is one 'Length of this key' field for each certificate presented.
IPS Gateway Certificate	Varies [0 – 24 Bytes]	The IPS Gateway certificate key information.

Table 6-10 – Certificate Packet

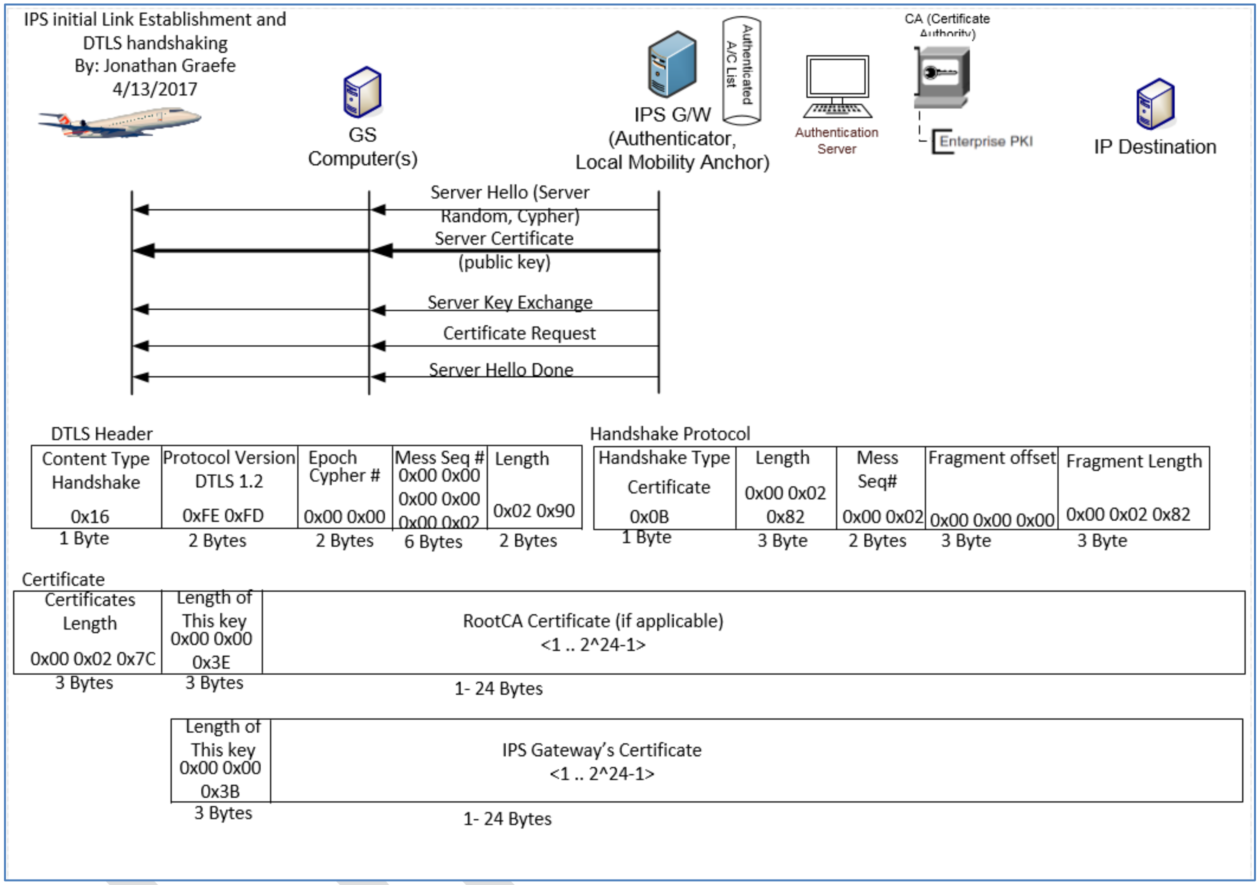


Figure 6-7 – Server Certificate Exchange

6.1.5.3 Server Key Exchange

After the IPS Gateway identifies itself using a public key certificate, an Elliptic Curve Diffie-Hellman ephemeral (ECDHE) key is devised for this session only. The ECDHE key is the pre-master secret negotiated key that will later be used to generate the session key. The DTLS Header field descriptions are the same as recorded in (Initial Client Hello); the only difference is in this case the server (IPS Gateway) is sending a message to the client (Aircraft). The Handshake Protocol Header is similar to the Initial Client Hello with the exception that the Handshake Type is 0x0C Key Exchange.

Field	Example	Meaning
Server EC Params – Curve Type	0x03 [1 Byte]	The ECDHE will use a named Curve to generate the public key
Server EC Params – Named Curve	0x00 0x18 [2 Bytes]	The named Curve will be secp384r1
Key Length	0x65	The Length of the Ephemeral ECDH key that will follow in the next field.
Ephemeral ECDH Public Key	Varies [0-255 Bytes]	This is the public ECDHE key, also called the pre-master secret that the IPS Gateway and Aircraft will use to generate the Master Secret.
Signature Hash	0x02 [1 Byte]	SHA384 will be used for Signature hashes
Signature Algorithm	0x03 [1 Byte]	ECDSA will be used to sign hashes
Signature Length	0x00 0x67 [2 Bytes]	The length of the signed hash of this message
Signature	Varies [1 – 65535 Bytes]	The ECDSA Signed SHA 384 hash of the current (This) message, to ensure authenticity in transit.

Table 6-11 – Server Key Exchange

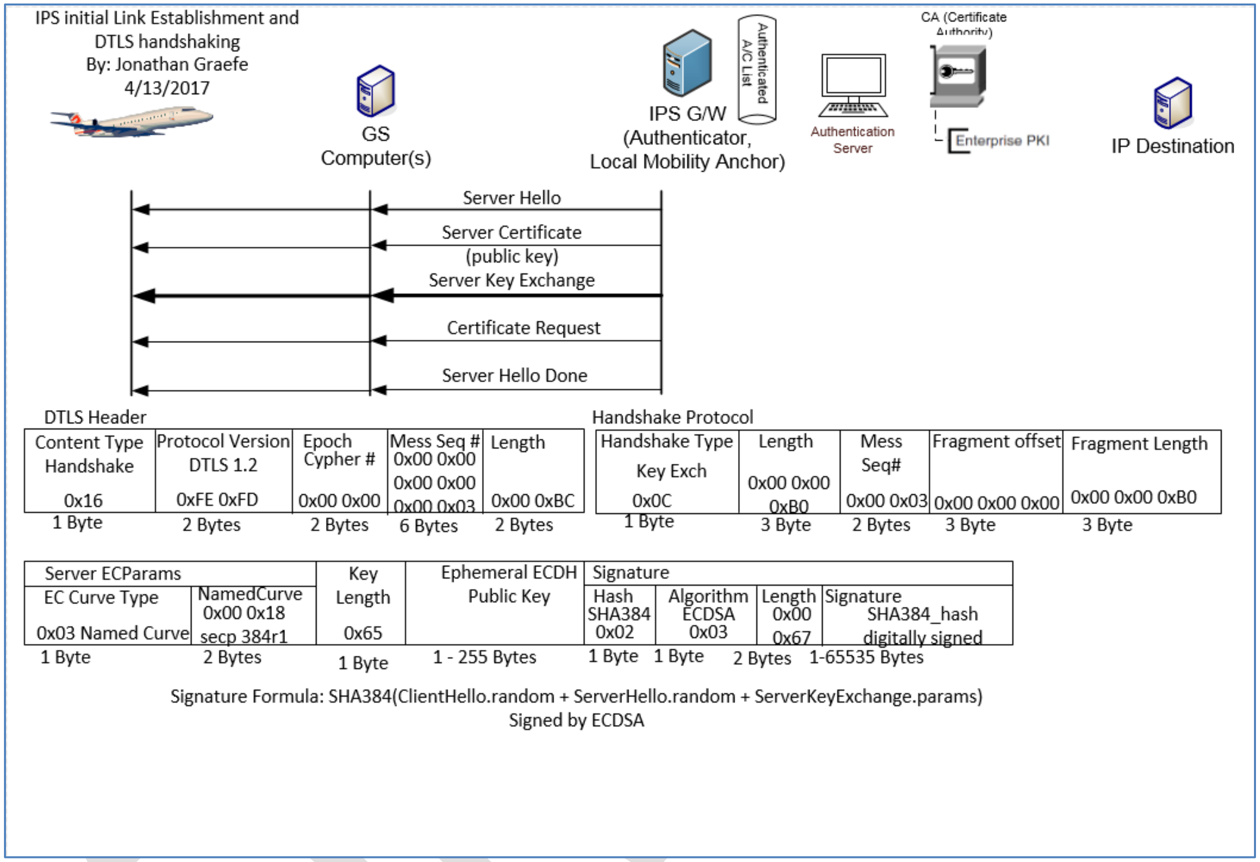


Figure 6-8 - Server Key Exchange (ECDHE)

6.1.5.4 Certificate Request

After sending a Pre-master secret ECDHE key the IPS Gateway begins the process of identifying the aircraft. This message instructs the aircraft what types of authentication keys the IPS Gateway will accept, and the key issuing authorities that are recognized. Similar to previous sections the DTLS Header remains the same, the Handshake Protocol header's only difference is that the Handshake Type is 0x0D Certificate Request.

Field	Example	Meaning
Client Certificate Type(s)	0x01 0x40 [1-256 Bytes]	This is a list of all supported Certificate Types. The first Byte is the length of the list. Each additional Byte represents a different Certificate Type in this case the length is 1 Byte and the accepted Keys are ECDSA.
Signature and Hash Algorithm	0x01 0x05 0x03 [3 – 256 Bytes]	This is a list of all supported Signature and Hash algorithm pairs. The first Byte is the list length in Bytes. The next Byte represents SHA384 hashing and the third Byte represents ECDSA Key signatures.
Distinguished Names (CA's) List Length	0x00 0xEE [2 Bytes]	This is the length in Bytes of all CA Distinguished names that are accepted as authorized key signers for this IPS Gateway.
X.501 DN Length	0x00 0x75	The length of the CA Distinguished Name (DN) to follow. This field only represents the very next DN not the entire packet.
CA DN	Id-at-organizationName==ARINC	The name of a CA who's authority is accepted by this IPS Gateway.

Table 6-12 – Client Certificate Request

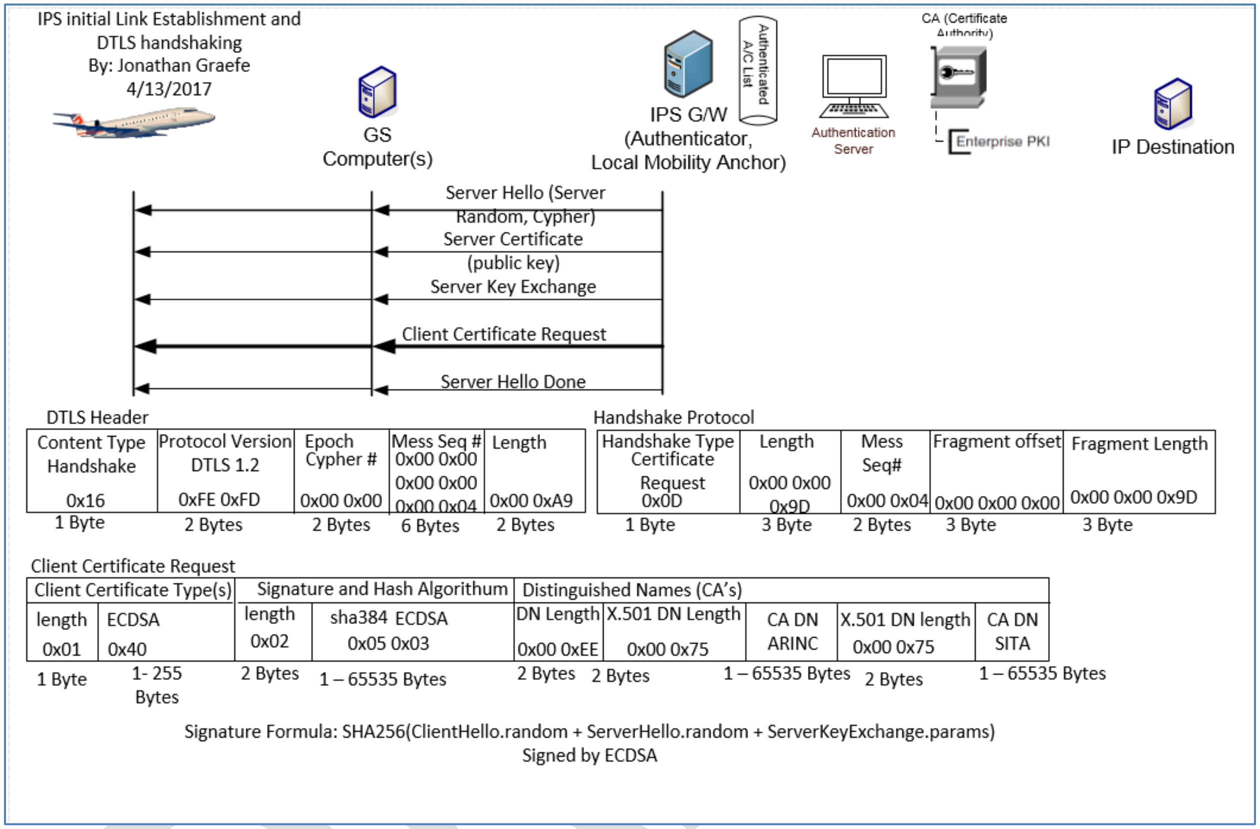


Figure 6-9 – Client Certificate Request

6.1.5.5 Server Hello Done

The IPS Gateway indicates at this point that it has finished transmitting identifying information and the Pre-Master Secret to the client. At this point it waits for the client's identifying information.

The only difference between fields explained in previous sections and this message is the Handshake Protocol header – Handshake Type. The Server Hello Done is 0x0E.

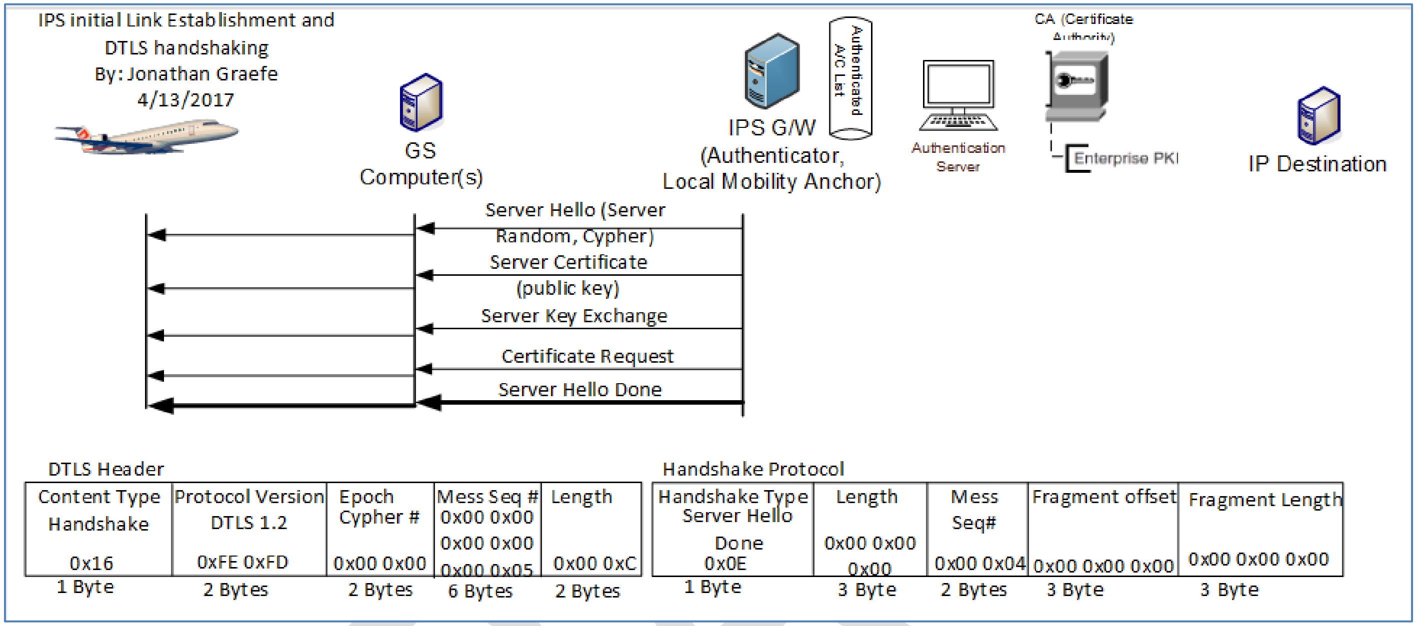


Figure 6-10 – Server Hello Done

6.1.6 Aircraft Authentication Messages

After the server completes identifying itself, sends an ECDHE key and the parameters for authentication types it will accept. It is the client's turn to authenticate itself to the server. This is done by sending an acceptable certificate that matches one of the parameter types accepted by the server and an ECDHE key pre-master secret that the aircraft will use and then starting the encrypted channel process.

6.1.6.1 Client Certificate

The Aircraft will select a certificate that is acceptable to the server. In section 6.1.5.4 it was stated that the Certificate Request that the aircraft received from the server, the server only accepts ECDSA Keys hashed with SHA384 and signed by either ARINC or SITA's private key.. If the aircraft does not have a certificate that matches the requested parameters then the handshake should be aborted. There may not be a roaming agreement in place to support this aircraft. If the aircraft does contain a certificate that matches the parameters the IPS Gateway sent then it can authenticate using that certificate.

The Aircraft can authenticate using a valid public x.509 certificate. It is recommended that the first communication of the day with a service provider be a full x.509 certificate handshake. If any keys need to be updated on the IPS Gateway it can be done via this daily full x.509 handshake. The Aircraft's public key will be used if required to encrypt messages to the IPS Gateway with key tag of 0x0A and 0x30 to 0x3F. The aircraft is expected to re-authenticate every 8 hours or at the beginning of each flight whichever comes sooner.

6.1.6.2 Aircraft Authentication Methods

There are two types of acceptable authentication.

1) Full X.509 certificate exchange. The x.509 certificate and that of the root CA will be exchanged with the IPS Gateway. The IPS Gateway can then perform a decision tree on whether to accept or not the authenticity of the presented keys. For purposes of this tree the directory certificate is the last known good certificate stored on the IPS Gateway. It is expected that all aircraft will support full x.509 certificate exchanges.
2) Modified X.509 certificate exchange. The aircraft's X.509 Certificate only will be sent to the gateway. The gateway can then perform a decision tree on whether to accept or not the authenticity of the presented certificate. The Gateway should have each trusted companion's public certificate preloaded into either the Gateway's certificate store. If not then abort the connection. If so continue the authentication process. The gateway may send its certificate only or the entire certificate chain. This type of exchange only works if both the aircraft and gateway certificates clearly indicate their signing authority trust anchor (CA Certificate).

6.1.6.2.1 Decision Tree for X.509 key exchanges

Decision Tree for x.509 key exchanges:

1) Directory aircraft certificate and received aircraft certificate match and are not expired, nor do they appear in the certificate revocation list. Then proceed with authentication.
2) Aircraft Key appears in a Certificate Revocation List. Abort the connection.
3) Directory aircraft certificate and received certificate match but both are expired. Abort authentication, and send a DTLS certificate expired message. Allow the aircraft to login with its one-time use key.
4) Directory aircraft certificate and received certificate do not match. Validate the received aircraft certificate against the directory rootCA certificate for the aircraft's CA provider.
    a. If the received certificate does validate, install the new aircraft certificate in the directory, deleting the old certificate.
    b. If the received certificate does not validate against the rootCA certificate for this provider, abort the connection. This may be an imposter aircraft or service provider.

5) RootCA Certificate is expired for this aircrafts certificate, abort the connection and send a DTLS alert message indicating bad certificate.
6) RootCA Certificate is expired; directory aircraft certificate and installed certificate do not match. Abort the connection, there may be an imposter aircraft.
7) Directory does not contain a certificate for this aircraft, but does have a rootCA certificate that can authenticate the new key. Validate the key against the rootCA certificate and Certificate revocation lists. If valid install aircraft certificate in the directory and allow authentication.
8) Directory does not contain a certificate or rootCA Certificate for this provider. Abort the connection and flag for follow up.

6.1.6.2.2 Example Certificate Exchange

The certificate exchange is likely to be fragmented over many packets. This example shows the message as one packet.

Field Name	Example Value	Meaning
Certificates Length	0x00 0x02 0x7C [3 Bytes]	Represents the total number of bytes that follow in this message, including all keys and key length headers.
Length of this Key (one for each key)	0x00 0x00 0x3B [3 Bytes]	The length of the key to immediately follow this message. There is one Length of this key field for each certificate presented.
Aircraft Certificate	Varies [0 – 24 Bytes]	Certificate for Aircraft certificate.

Table 6-13 – Certificate Packet

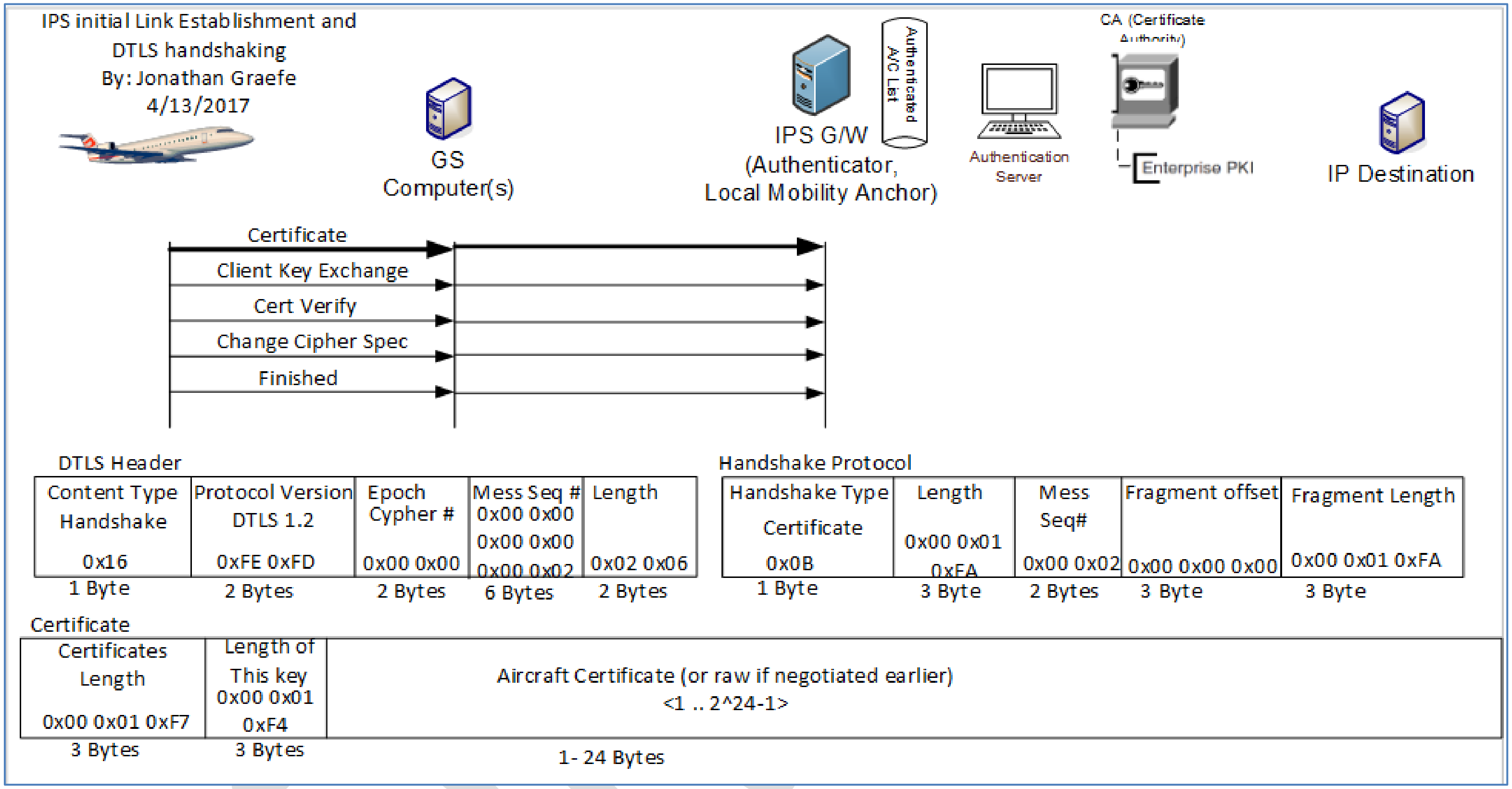


Figure 6-11 – Client Certificate

6.1.6.3 Client Key Exchange

The Aircraft after identifying itself to the server sends an ECDHE key to the IPS Gateway which is also the Pre-Master Secret key. This key with the server key represent some of the information used by both sides to generate the session secret key. The DTLS Header is similar to all other handshake messages. The Handshake protocol Type for Client Key exchange is 0x10.

Field	Example	Meaning

EC Point Key Length	0x65 [1 Bytes]	Represents the length of the ECDHE key in Bytes to follow
ECPoint – Ephemeral ECDH Key	Varies [1-255 Bytes]	The ECDHE Key also known as the Aircraft's Pre-master Secret

Table 6-14 – Client Key Exchange

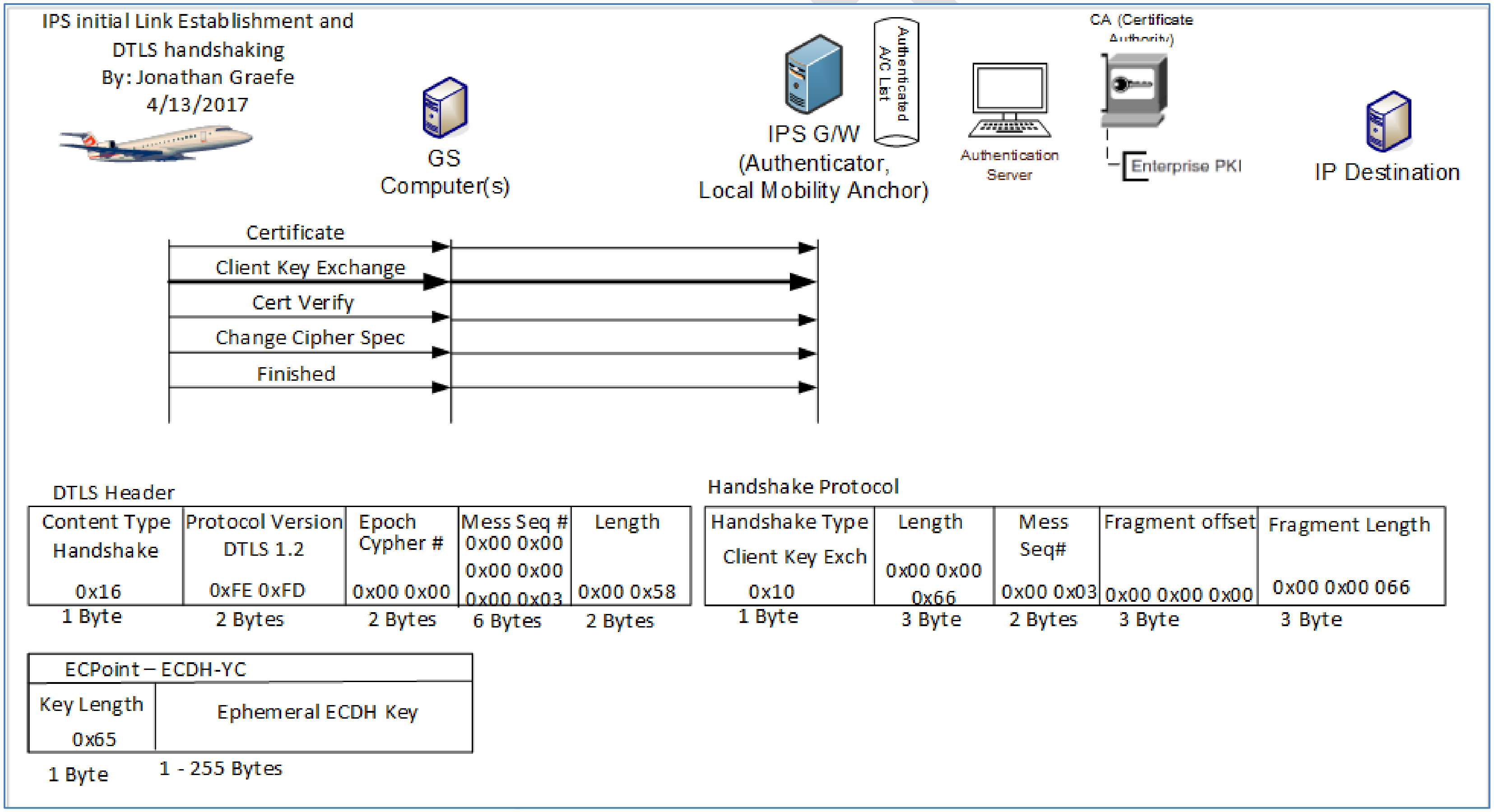


Figure 6-12 – Client Key Exchange

6.1.6.4 Client Certificate Verify

To ensure that the channel is securable, and all messages have been received from the server. The Aircraft now hashes and signs all messages sent and received during the handshake process up to this point. The IPS Gateway can then determine if all messages have been received without modification and determine if the channel is ready for encrypted. After this point both the Aircraft and the server calculate the Session Master Secret Key which is never itself transmitted but is calculated from all messages up to this point and a seed that is well known by both sides.

Similar to all previous handshake messages the DTLS Header is similar. The Handshake Protocol header is also similar; however the Handshake Type of the client Certificate Verify is 0x0F

Field	Example	Meaning
Hash Type	0x02	The Signature field is using a SHA384 hash of all the handshake messages sent and received thus far.
Signature Type	0x03	The Signature field hash is signed with an ECDSA Private Key, the public certificate was sent earlier via the certificate exchange
Length	0x00 0x66	Represents the length in Bytes of the Signature.
Signature	Varies [1-65535] Bytes	The SHA 384 hash of all handshake messages signed by the ECDSA private key of the aircraft.

Table 6-15 - Certificate Verify Message

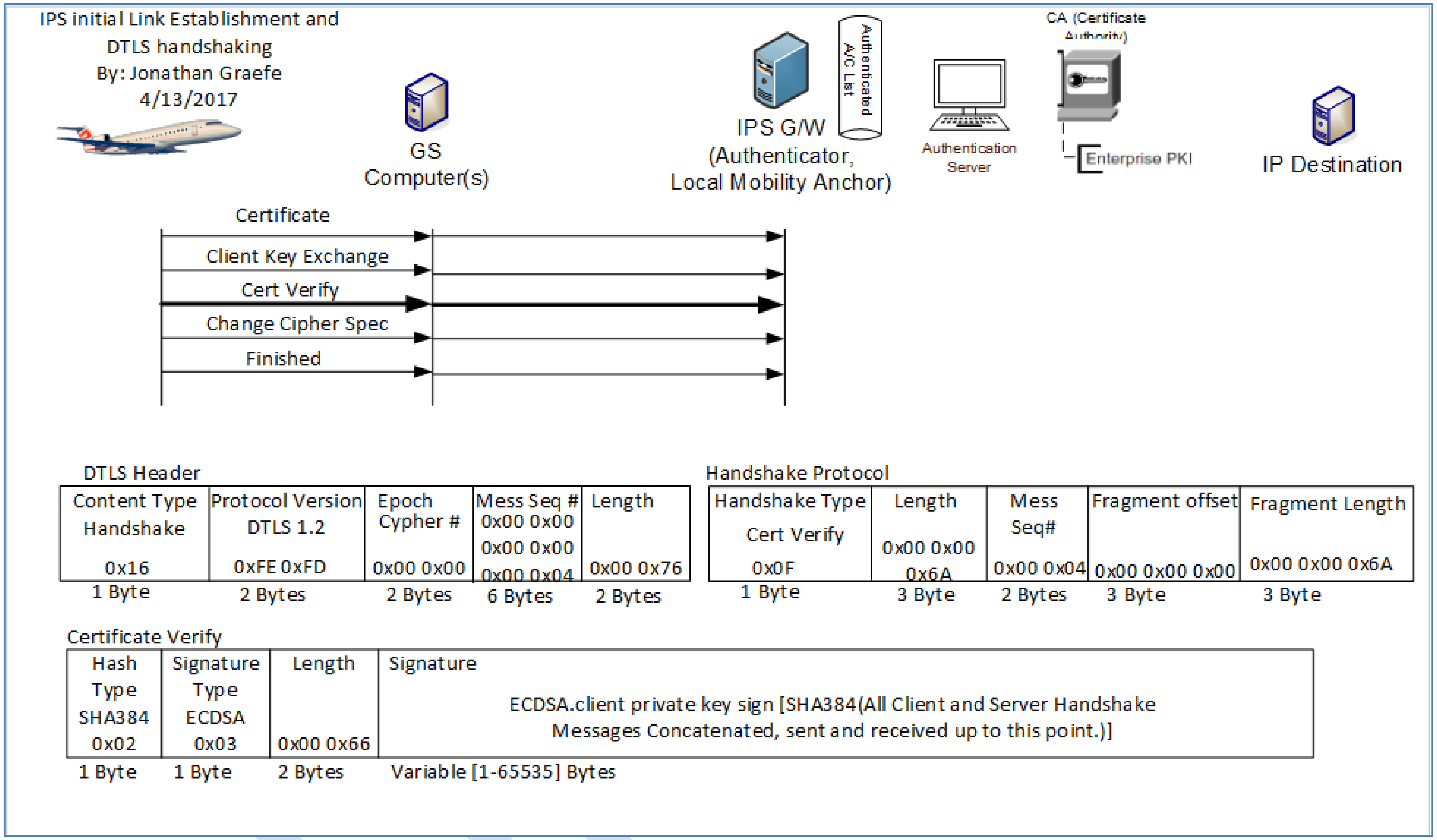


Figure 6-13 – Certificate Verify Message

6.1.6.5 Client Change Cipher Spec

This message indicates that the aircraft will now encrypt all messages sent towards the IPS Gateway using the parameters negotiated earlier. All messages from the aircraft after the change cipher spec will have SHA 384 Message integrity hashes using the Aircrafts Private Key for signing. In addition all Messages to the IPS Gateway UDP port 5908 with key tag of 0x0A will be encrypted using the IPS Gateway's Public Key.

The DTLS Header is different for this message. The Content type is 0x14 for Change Cipher Spec message. The Change Cipher Spec message only contains the type 0x01.

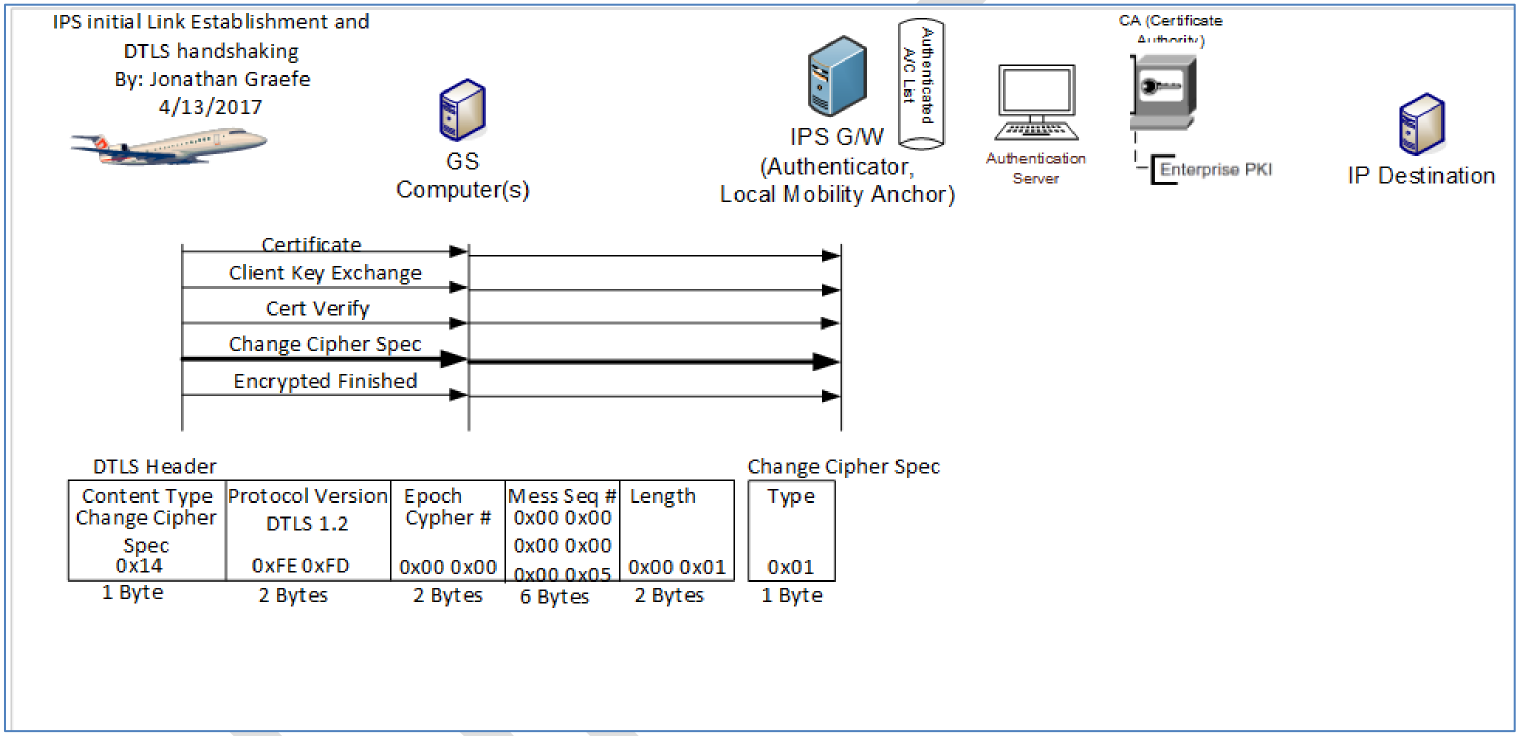


Figure 6-14 – Aircraft Change Cipher Spec

6.1.6.6 Client Finished (Encrypted)

Once the Change Cipher Spec is sent all new messages (not retries of previous messages) are encrypted with the just negotiated cipher, hash and signature methods. The aircraft is now sending a message to the IPS Gateway that it is finished identifying itself to the server and is ready to begin normal traffic. The DTLS header is the standard handshake header. The Handshake Protocol header's Type is 0x14. This message is encrypted. The DTLS header is sent in the clear but the Handshake protocol header and all following materials are encrypted.

The Client Finished message is detailed below:

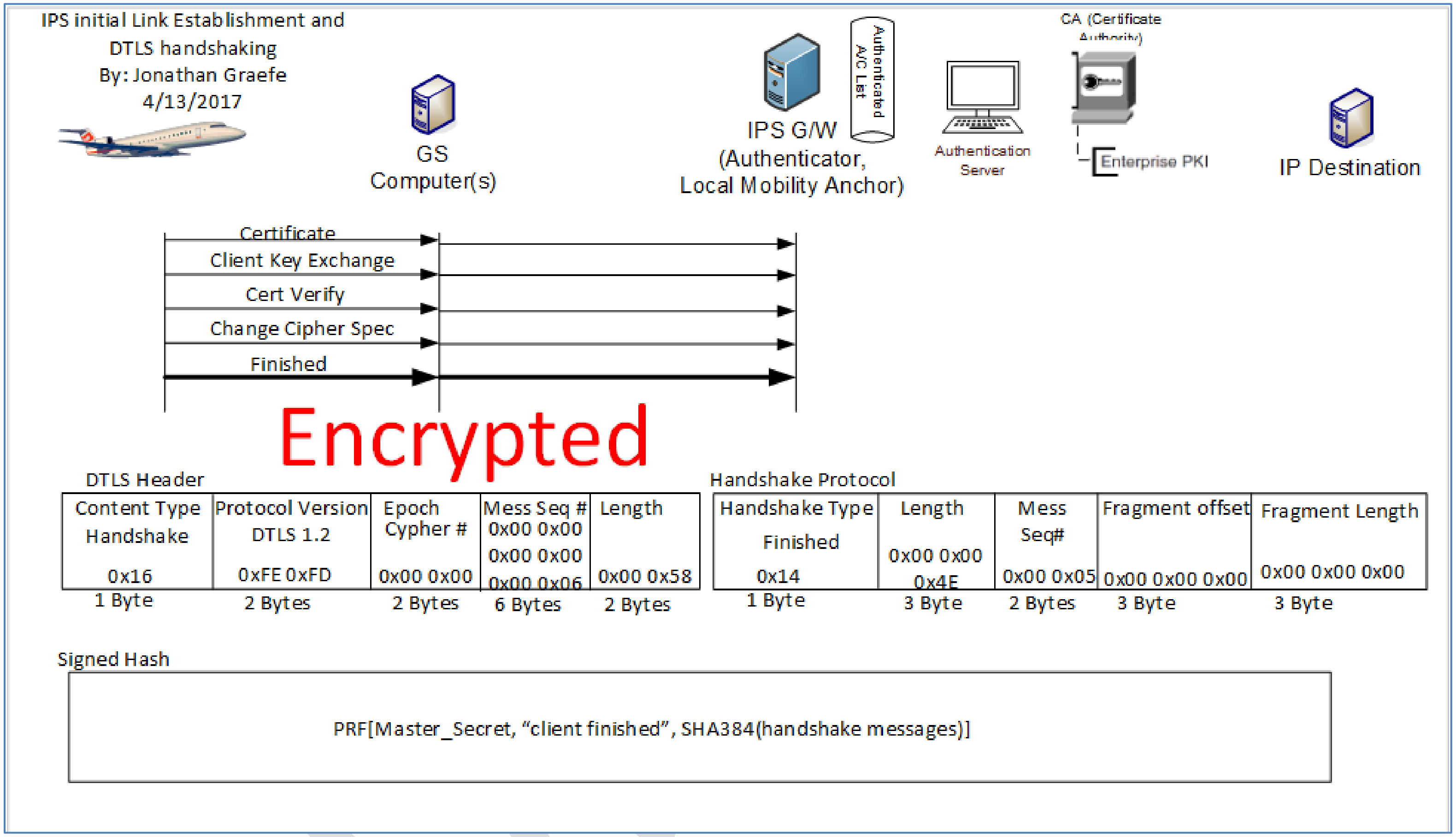


Figure 6-15 – Client Finished (Encrypted)

6.1.7 Server Authentication completion

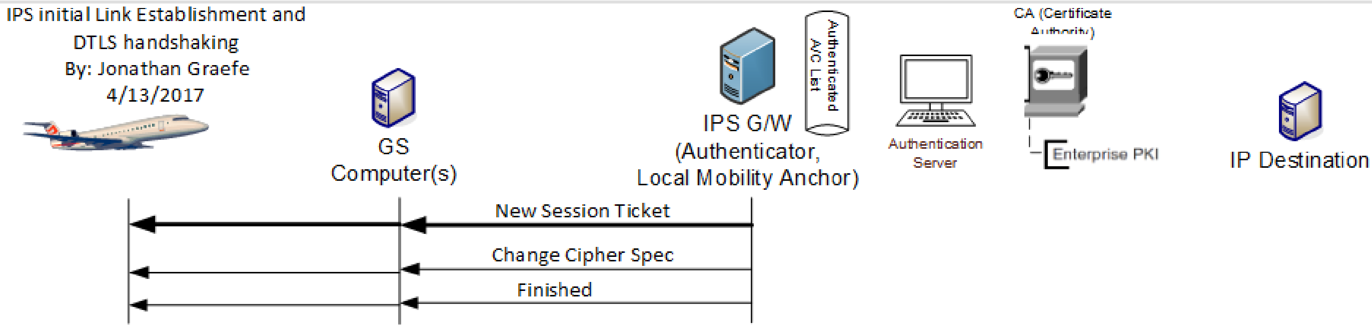
The IPS Gateway completes the DTLS authentication process by providing the aircraft with a session Ticket whereby it can resume a previously lost session as long as the ticket has not yet expired. Then the server starts its side of the encrypted tunnel and finally marks the authentication process as complete.

6.1.7.1 Session Ticket Message

The IPS Gateway issues a Session Ticket so that the aircraft can resume a session as long as the ticket is still valid. Each ticket has an expiration clock that once expired invalidates the ticket. Similar to all handshake messages above the DTLS header is similar. The Handshake Protocol Handshake Type field is 0x04 for Session Ticket.

Field	Example	Meaning
Lifetime Hint	0x00 0x00 0x70 0x80 [4 Bytes]	The number of seconds that this ticket is valid from the point sent. The IPS gateway will keep the ticket and a countdown clock in memory and allow the ticket to be used as long as there is time on the clock. At the point of 0 seconds left the ticket is removed as a valid ticket. The aircraft should use a similar process.
Length	0x02 0xA0 [2 Bytes]	The total length of the session ticket
Ticket	Varies [1 – 65535 Bytes]	The Session Ticket

Table 6-16 – Session Ticket Message



DTLS Header

Content Type	Protocol Version	Epoch Cypher #	Mess Seq #	Length
Handshake 0x16	DTLS 1.2 0xFE 0xFD	0x00 0x00	0x00 0x00 0x00 0x00 0x00 0x06	0x02 0xB2
1 Byte	2 Bytes	2 Bytes	6 Bytes	2 Bytes

Handshake Protocol

Handshake Type	Length	Mess Seq#	Fragment offset	Fragment Length
Session Ticket 0x04	0x00 0x02 0xA6	0x00 0x06	0x00 0x00 0x00	0x00 0x02 0xA6
1 Byte	3 Byte	2 Bytes	3 Byte	3 Byte

Session Ticket Message

Lifetime Hint	Length	Ticket
8 Hours (28800 sec) 0x00 0x00 0x70 0x80	0x02 0xA0	Varies
4 Bytes	2 Bytes	1-65535 Bytes

Figure 6-16 – Session Ticket

6.1.7.2 Server Change Cipher Spec

This message indicates that the IPS Gateway will now encrypt all messages sent towards the aircraft using the parameters negotiated earlier. All messages from the IPS Gateway after the change cipher spec will have SHA 384 Message integrity hashes using the IPS Gateway's Private Key for signing. In addition all further Messages from UDP 5908 with key tag of 0x0A will be encrypted using the Aircraft's Public Key.

The DTLS Header is different for this message. The Content type is 0x14 for Change Cipher Spec message. The Change Cipher Spec message only contains the type 0x01.

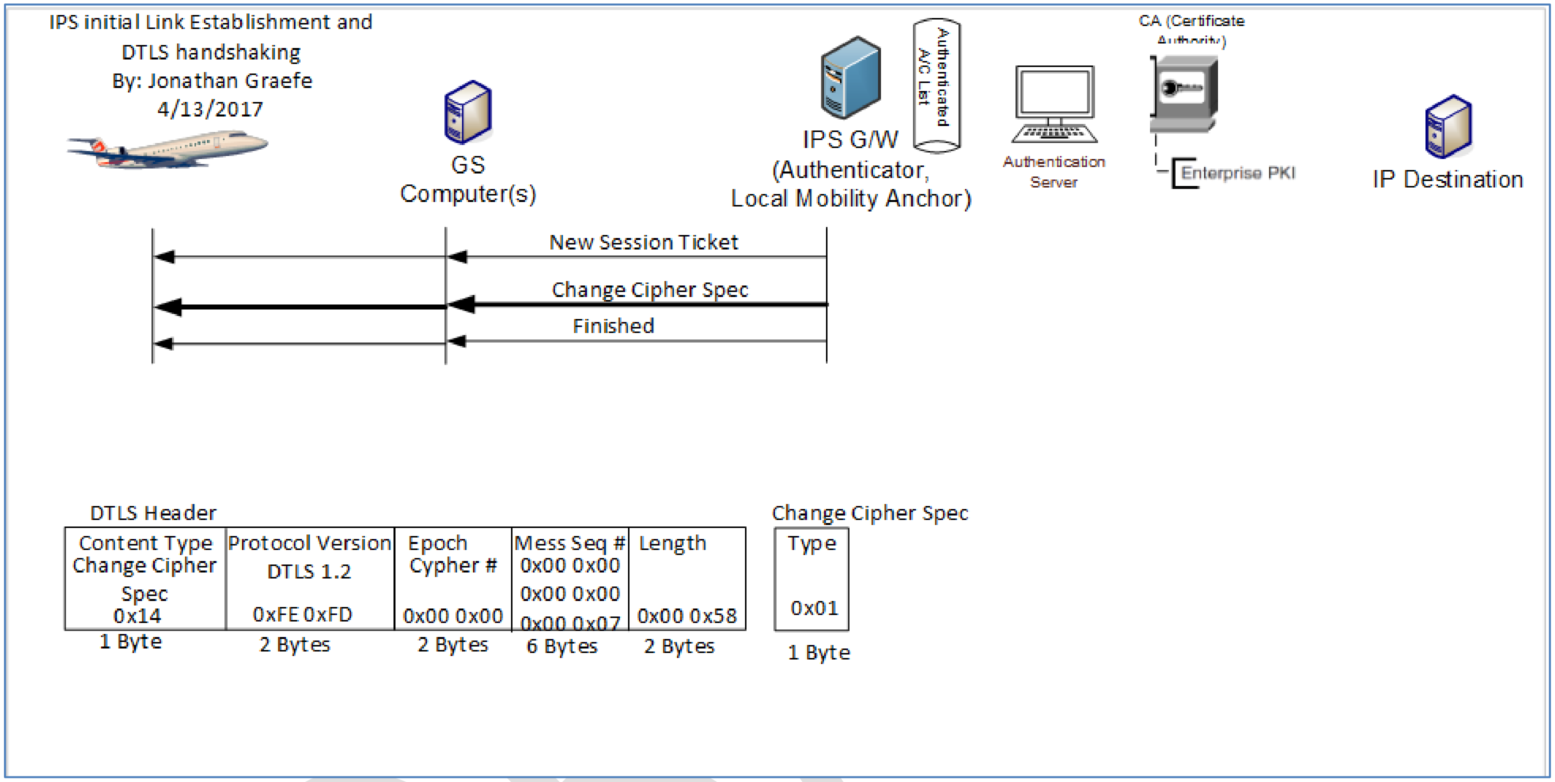


Figure 6-17 – Server Change Cipher Spec

6.1.7.3 Server Finished (Encrypted)

Once the Change Cipher Spec is sent all new messages (not retries of previous messages) are encrypted with the just negotiated cipher, hash and signature methods. The IPS Gateway is now sending a message to the aircraft that it is finished with the identification process and is ready to begin normal traffic. The DTLS header is the standard handshake header. The Handshake Protocol header's Type is 0x14. The DTLS header is sent in the clear but the Handshake protocol header and all following materials are encrypted.

The Server Finished message is detailed below:

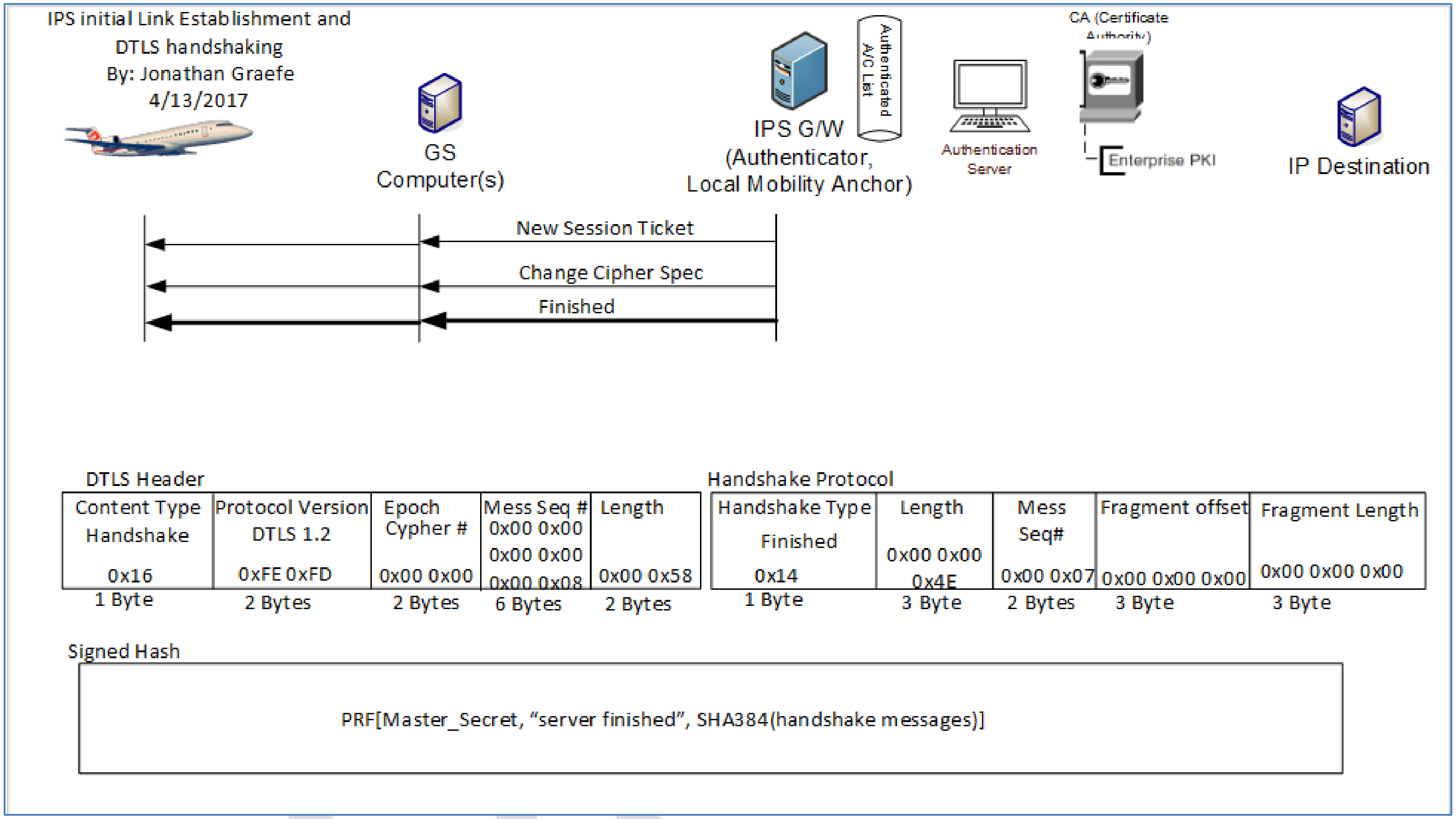


Figure 6-18 – Server Finished

6.1.8 Login information messages

Once the DTLS logon is complete, the gateway and aircraft need a few additional pieces of information to maintain the connection. These Logon Information messages will be encrypted and compressed using the methods already agreed to in the DTLS logon. It should be noted that both the gateway and aircraft will need to decrypt these messages and use their contents to determine the correct MIC. If the MIC fails then the entire message and its contents should be discarded from memory and the DTLS session torn down.

The Aircraft to ground Login Information Message is expected by the gateway first. This way the gateway knows that the aircraft has otherwise accepted all of the servers DTLS parameters.

Aircraft to Gateway Finalized login information Message		
Field	**Value**	**Example**
Aircraft IPv6 Address	The Global Fixed Mobility address of the avionics.	00FF:0A98:2354:9222:5464:3893:2398:D4A9
Tail # Length	The total length in Bytes of the Tail Number used for ACARS translations	0x00 07
Aircraft Tail Number	The Aircraft's Tail Number used for ACARS Translations	N123456
ATN address	The Aircraft's ATN address. Used for ATN translations	0xA5F098
Random Message Number	A random number that will be the beginning message number for downlinks. This random number will be used for the MIC calculation of this very message.	0x00 00 00 00 55 16
Flight ID Length	The Total Length in Bytes of the Flight ID	0x00 06
Flight ID	The Flight ID	AB1234
MIC	The Message Integrity code generated via the function in section 5.4.3 MIC Generation Function	0x FF 87 12 85

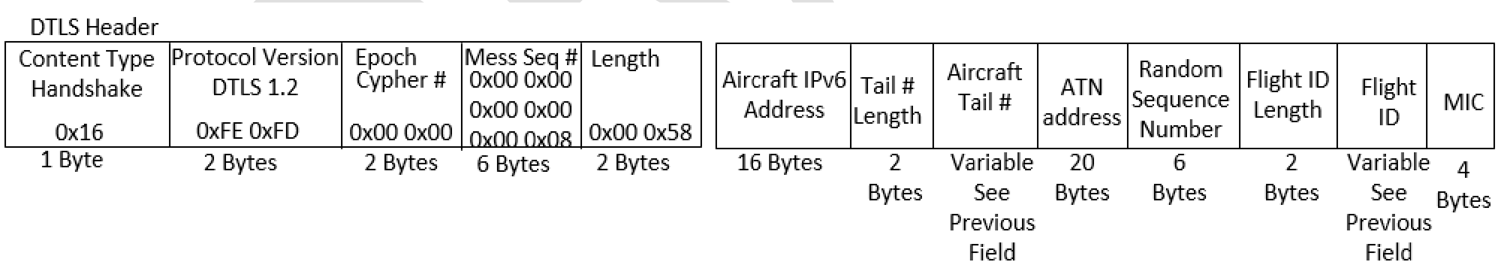


Figure 6-19 – Finalized logon Information Exchange message Aircraft to local gateway

After the login information message from the aircraft is received decoded and MIC checked the gateway will respond with its own logon information message. Informing the aircraft of the random sequence number used for uplink MIC calculations.

Gateway to Aircraft finalized logon information Message		
Field	**Value**	**Example**
Random Message Number	A random number that will be the beginning message number for uplinks. This random number will be used for the MIC calculation of this very message.	0x00 00 00 88 55 16
MIC	The Message Integrity code generated via the function in section 5.4.3 MIC Generation Function	0x F0 82 13 45

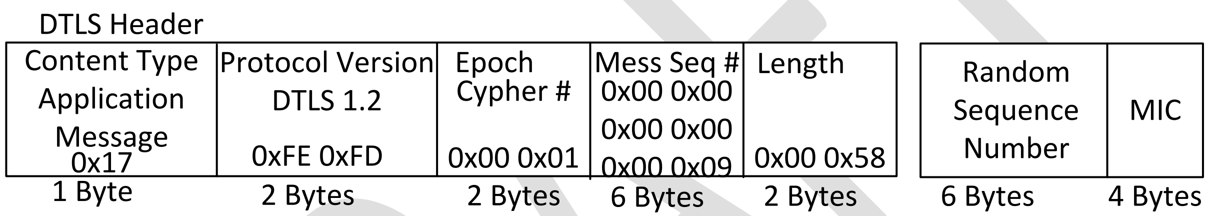


Figure 6-20 - Additional Information Message Gateway to Aircraft

6.2 IPS Aircraft – IPS Ground System

For IPS Aircraft to IPS Ground System Messaging, illustrated in Figure 3-4, the IPS Gateway is used to manage the message flow without interpreting or reformatting the message data. The general requirements for the IPS Gateway are:

- Maintaining key aircraft information (tail number, flight id) for each authentication event
- Maintain session key for MIC computation and encryption
- Maintaining a Session Record for the specific "connection", defined by:
  - Source Port – Destination Port Pair, and
  - Source IP Address – Destination IP Address Pair
- Managing, for each established Session, the sequence mapping between the IPS Aircraft – IPS Gateway messages and the IPS Gateway – IPS Ground System messages
- Supporting Compression, ATNPKT Generation, Segmentation and Reassembly:
  - Downlink –
    - Support ATNPKT segmentation and reassembly as required
    - Support acknowledgement of downlink blocks based on the "More" bit setting
      - "More" bit set – Gateway can acknowledge blocks based on internal Acknowledgement timer
      - "More" bit not set – Gateway must forward to IPS Ground System, and only acknowledge block upon receipt of corresponding IPS Ground System Acknowledgement
    - Support uncompressing downlink messages
    - Creation and routing of message copies based on airline preference
  - Uplink –
    - Support ATNPKT segmentation and reassembly as required
    - Acknowledge IPS Ground System upon IPS Aircraft Acknowledgement of all corresponding message segments
    - Support compressing uplink messages
- Supporting key-based message integrity calculations to include with uplink messages and to use for validating integrity of downlink messages
- Supporting determination of optimal ground station for VDL Mode 2 uplink delivery

There are three distinct phases in the transport of the downlink and uplink messages:

Transmission Leg	Mechanism	Notes
Downlink Messages		
IPS Aircraft (Avionics) → GS	SNPDU / AVLC Packet	
GS → IPS Gateway	IPv6 Packet	
IPS Gateway → IPS Ground System	Native IPv6	Depends on the connection type to ground system
Uplink Messages		
IPS Ground System → IPS Gateway	Native IPv6	Depends on the connection type to ground system

IPS Gateway → GS	IPv6 Packet	
GS → IPS Aircraft (Avionics)	SNPDU / AVLC Packet	

Table 6-17 – IPS Transmission Legs for IPS Ground System

The details of the different packaging of the IPv6 data have been provided in previous sections. The following sections provide details of the ATNPKT for the applicable DS primitives.

6.2.1 ATNPKT Message Set

This section describes the ATNPKT message set used for communication between the IPS Aircraft and the IPv6 Host. Each message type is defined by the DS Primitive Value. The Presence Flags and related Field contents applicable to the message are specified in Table 5-18.

6.2.1.1 D-Start

To establish a communication session an initial D-START/D-Start(confirm) exchange is required. Figure 6-21 shows an example of D-Start.

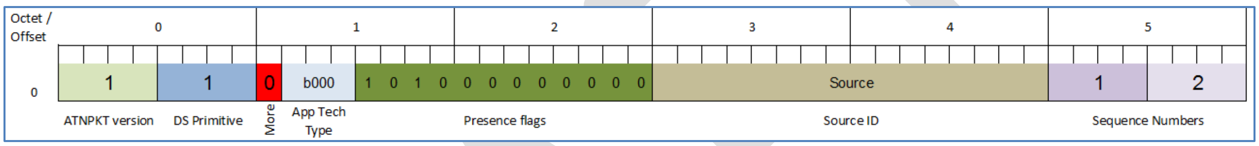


Figure 6-21 – D-Start Example

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 1 (defines the message as a D-Start)
- More bit set to 0 (short message)
- App Tech Type is set to b000 for ATN/IPS DS
- The first and third presence field flags set (indicating source ID and sequence number fields present)
- Source ID is a communication identifier used by the IPS aircraft or IPS Ground System (D-Start source ID is not used by the IPS Gateway)
- Sequence numbers (number sent is 1 and next expect to be received is 1)

Note that D-Start can optionally carry user data; therefore the example provided here could look more like the example shown for D-Data.

6.2.1.2 D-Start cnf

A D-Start confirm (cnf) is generated in response to D-Start being received.

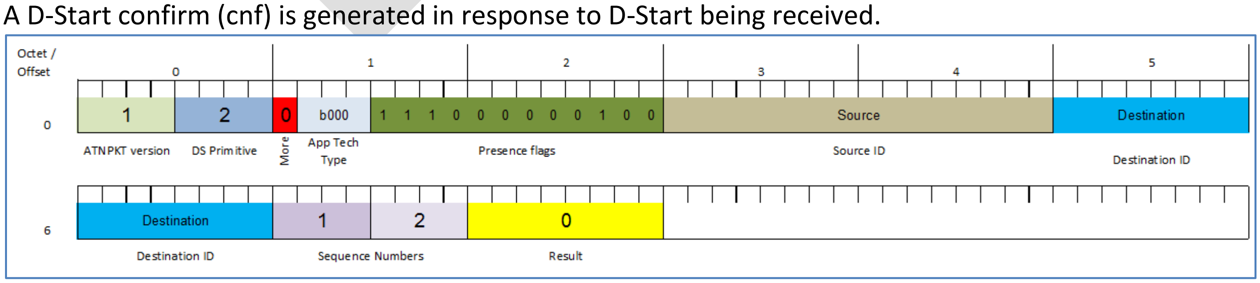


Figure 6-22 – D-Start cnf example

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 2 (defines the message as a D-Start cnf)
- More bit set to 0 (short message)
- App Tech Type is set to b000 for ATN/IPS DS
- The first, second, third, and tenth presence field flags are set (indicating source ID, destination ID, sequence number, and result fields present)
- Source ID is the identification of the source peer
- Destination ID is the identification of the destination peer
- Result value of 0 indicates acceptance of the D-Start (1 and 2 are rejects)
- Sequence numbers (number sent is 1 and next expect to be received is 2)

6.2.1.3 D-Data

The D-Data packet contains either IPS data, or ATN/OSI data or A620 data. It consists of the ATNPKT fixed and variable parts. The variable part content is dependent on the type of data and whether it is the first or a subsequent fragment in a fragmented message using the More bit.

The D-Data DS will be used for all of the authentication message exchange.

The following example (Figure 6-23 and Figure 6-24) shows the layout of the ATNPKT for a two segment IPS message. The first segment shows the More bit set to '1', the first 2 bytes of the data contain the length of the data and the 3rd byte of the data contains the compression flag. The second segment has the More bit set to '0' indicating the end of the data.

Octet / Offset	0	1	2	3	4	5
0	1 ATNKT ver / 5 DS primitive	more 1 / b000 AppTechType / 0 1 1 0	0 0 0 0 0 0 0 1 Presence flags	Destination Destination ID		1 N(S) / 2 N(R)
6	9712 Data length		1 Compression Flag	Data		
12						
.....						
1020						
1026						

Figure 6-23 – D-Data, 1st of 2 segments (IPS data)

Octet / Offset	0	1	2	3	4	5
0	1 ATNKT ver / 5 DS primitive	more 0 / b000 AppTechType / 0 1 1 0	0 0 0 0 0 0 0 1 Presence flags	Destination Destination ID		2 N(S) / 2 N(R)
6	data					
12						
.....						
186						
192						

Figure 6-24 – D-Data, 2nd of 2 segments (IPS data)

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 5 (defines the message as a D-Data)
- More bit as described in the example
- App Tech Type is set to b000 for ATN/IPS DS
- Three presence bits set (2nd – for destination id, 3rd – for sequence number field, 12th – for user data)
- Destination ID is the identification of the destination peer
- Sequence numbers (number sent are sequential 1-2 and next expected to be received is 2)
- User data (first 2 bytes containing the length, 3rd byte containing compression flag)

6.2.1.4 D-ACK

The D-Ack primitive provides acknowledgement for one or more D-Data messages received. The example in Figure 6-25 shows the acknowledgement of messages received up to sequence number 4 by having a value of 5 for the next expected message to be received. The first number in the sequence number field (N(S)) is not incremented by D-Ack and should be the same as the previous messages Ns (to allow for the increment on the next message with an applicable Ns).

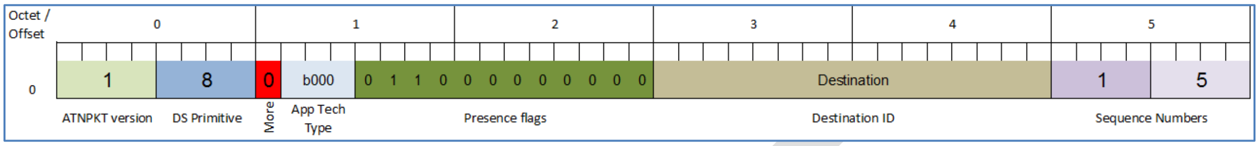


Figure 6-25 – D-ACK example

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 8 (defines the message as a D-ACK)
- More bit set to '0'
- App Tech Type is set to b000 for ATN/IPS DS
- The second and third presence field flags are set (indicating destination ID and sequence number fields present)
- Destination ID is the identification of the destination peer
- Sequence numbers (number sent is shown as 1 but should be the same as the last one sent, and next expect to be received is 5)

6.2.1.5 D-END

The D-End primitive is used to unbind the communication between DS-uses in an orderly manner such that any data that is in transit is delivered before the unbinding is completed. Figure 6-26 provides an example of the D-End primitive.

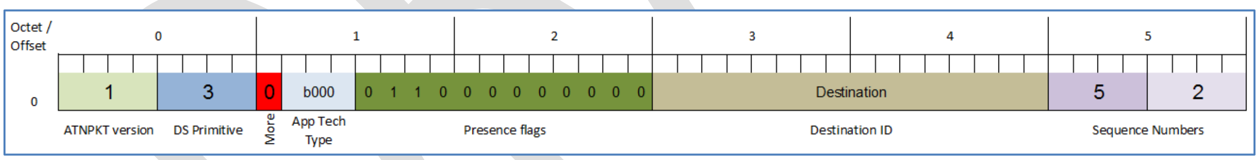


Figure 6-26 – D-END example

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 3 (defines the message as a D-END)
- More bit set to '0'
- App Tech Type is set to b000 for ATN/IPS DS
- The second and third presence field flags are set (indicating destination ID and sequence number fields present)
- Destination ID is the identification of the destination peer
- Sequence numbers (number sent is 5 and next expect to be received is 2)

6.2.1.6 D-END cnf

The D-End cnf primitive informs the DS-user with a positive or negative response from the peer DS-user about the completion of the dialogue termination. Figure 6-27 provides an example of the D-End cnf primitive. The ‘0’ in the result field indicates a positive confirmation to the D-End request.

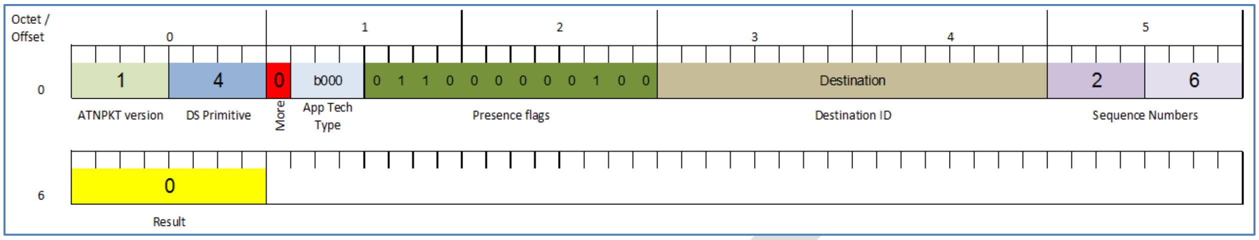


Figure 6-27 – D-END cnf example

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 4 (defines the message as a D-END cnf)
- More bit set to ‘0’
- App Tech Type is set to b000 for ATN/IPS DS
- The second, third, and tenth presence field flags are set (indicating destination ID, sequence number, and result fields present)
- Destination ID is the identification of the destination peer
- Sequence numbers (number sent is 2 and next expect to be received is 6)
- Result value of 0 indicates acceptance of the D-END (1 and 2 are rejects)

6.2.1.7 D-Abort

The D-Abort primitive can be invoked to abort the relationship between communicating DS-users. Any data in transit may be lost.

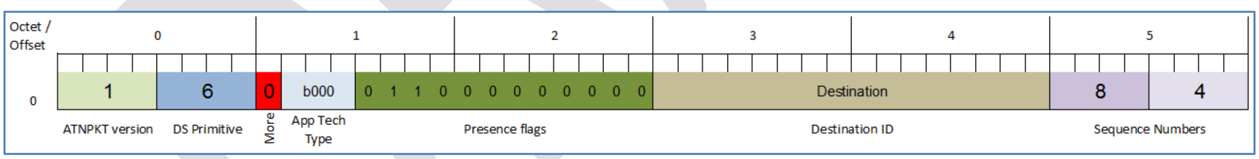


Figure 6-28 – D-Abort example

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 6 (defines the message as a D-Abort)
- More bit set to ‘0’
- App Tech Type is set to b000 for ATN/IPS DS
- The second and third presence field flags are set (indicating destination ID and sequence number fields present)
- Destination ID is the identification of the destination peer
- Sequence numbers (number sent is 8 and next expect to be received is 4)

6.2.2 Message Segmentation

The downlink / uplink data between IPS Aircraft and IPS Gateway has to fit within the maximum IPv6 packet size of 1280 bytes. The maximum size ATNPKT will fit within this limit, so no additional segmentation considerations are required at this level.

Segmentation may be required at the link layer, but this is subnetwork specific. For example the limit of the AVLC packet (max 251 bytes) means that a maximum sized IPv6 packet will need to be sent in 5 segments. This segmentation will be handled by the VDL mode 2 'orange' protocol. The IPS Gateway is responsible for supporting this segmentation. The IPS Gateway is responsible for:

- Segmentation of uplink messages using the ATNPKT More bit for user data exceeding 1024
- Reassembly of downlink messages received from an IPS Aircraft using the ATNPKT More bit
- Segmentation using the orange protocol for AVLC packet size limit
- Reassembly of the orange protocol segmentation
- Management of acknowledgements to both IPS Ground System and to IPS Aircraft
- Management of sequence numbers for message exchange both with IPS Ground System and with IPS Aircraft. This includes properly correlating the sequence numbers used with the IPS Ground System and with the IPS Aircraft.

Figure 6-29 provides an example of the segmentation that the IPS Gateway is involved with. In this example:

- A 2000 byte message needs to be delivered to an IPS Aircraft
- The IPS Ground System has to send this message in two segments to limit segments to 1024 bytes. Segment 1 will have the More bit set to '1'
- The IPS Gateway receives this 2 segment message and performs the following processing:
  - reassembles the message in order to process the message efficiently
  - compresses the user data (reduces the message content size to 890 bytes, a representative example), and compresses the IPv6 and UDP headers
  - uses the orange protocol to segment the data for VDL (AVLC packet limit of 251 bytes). This segmentation results in 4 uplink segment being generated
  - compute the MIC and append at end of the packet
  - Forward to Ground Station which adds the AVLC frame for transmission to the IPS Aircraft

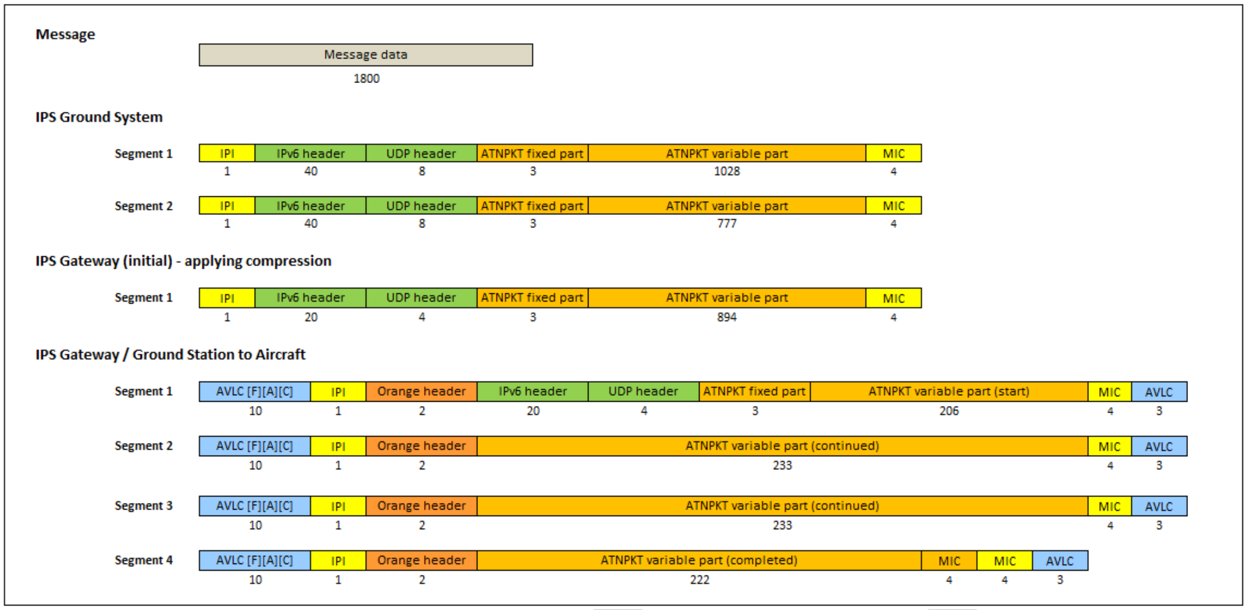


Figure 6-29 – Message segmentation example

6.2.2.1 Sequence number and acknowledgment management

Since the message segmentation can be different for messages going between the IPS Gateway and IPS Aircraft and for messages going between the IPS Gateway and IPS Ground System, the IPS Gateway is responsible for managing the correlation of sequence numbers and managing acknowledgements. This difference in segmentation can be a result of the IPS Gateway compressing data for efficient transmission. There are a number of requirements which impact the IPS Aircraft – IPS Ground System sequencing and acknowledgement processing, including:

- Maximum ATNPKT size
- Maximum number (16) of unacknowledged ATNPKTs
- Acknowledgement to aircraft after ack timer expiry when more bit set, acknowledgement to aircraft only if ack received from IPS Ground System when more bit not sent
- Acknowledgement to IPS Ground System when all segments acknowledged by IPS Aircraft

Sequencing Example

There are two sequence numbers in the ATNPKT, described in 5.10.2.3, with N(S) describing the sequence number sent and N(R) describing the next expected number to be received. Table 6-18 shows an example of the N(S) sequence number that the IPS Gateway receives from an IPS Ground System and the corresponding N(S) that it sends to an IPS Aircraft.

N(S) sequence #	
Received from IPS Ground System	Sent to IPS Aircraft
1	
2	
	1
3	
	2

Table 6-18 – Sequence number correlation

In this example, a two segment message with sequence numbers 1 & 2 is received by the IPS Gateway, compression by the Gateway results in a single segment message going to the IPS Aircraft with sequence number 1. Next a single segment messages is received by the IPS Gateway with sequence number 3, this results in a single segment message going to the IPS Aircraft with sequence numbers of 2.

<u>Acknowledgement Example</u>

The IPS Gateway is responsible for acknowledging messages received from both the IPS Ground Systems and from IPS Aircraft. N(R) is used to acknowledge the receipt of messages. Acknowledgement is most commonly done using the D-Ack message, however an acknowledgement can piggy back on other messages such as D-Data by updating N(R).

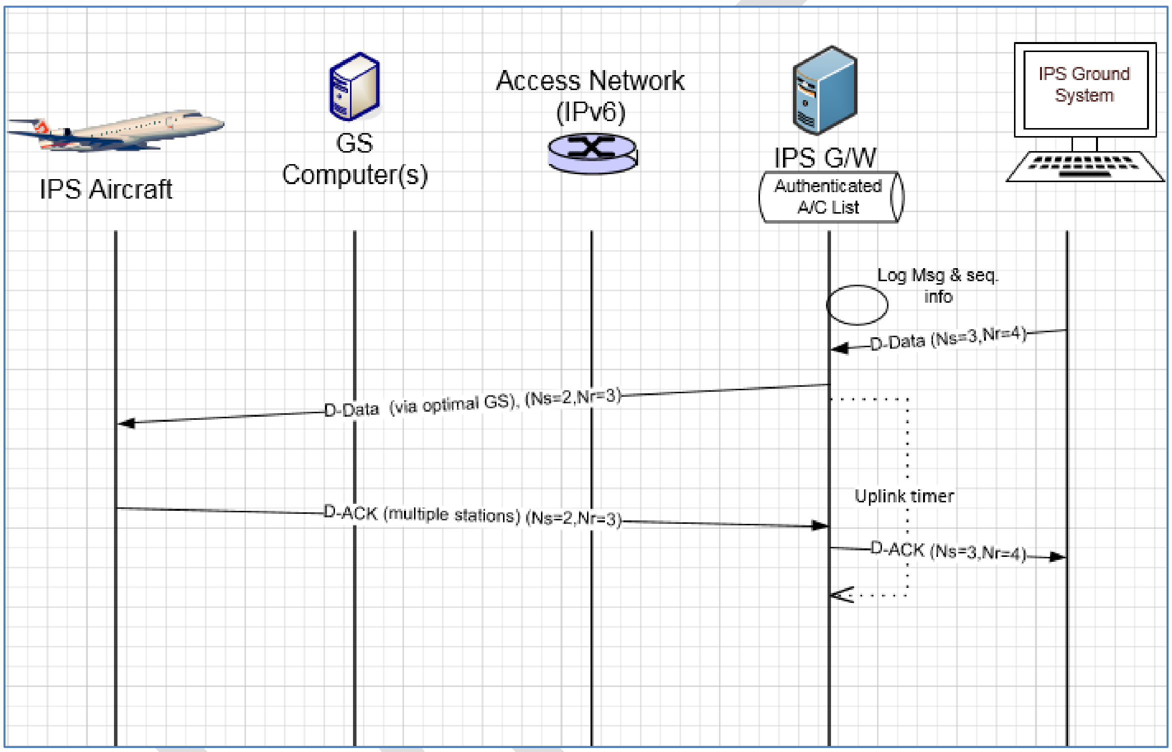


Figure 6-30 – Simple uplink scenario (from IPS Ground System)

Figure 6-30 shows an example of a D-Data uplink and corresponding D-Ack downlink response. The IPS Gateway receives a single block D-Data uplink from IPS Ground System (with N(S) sequence number of 3, and with N(R) of 4 indicating the next sequence number that it expects to see. Due to previous segmented messages, the IPS Gateway sets the sequence number (N(S)) to 2 with N(R) being 3 for sending to the IPS aircraft. The IPS aircraft acknowledges the message by generating a D-Ack message with N(R) set to 3 indicating the next sequence number that it expects to see. The value in the N(S) field is not incremented and reflects the last message sent. The IPS Gateway receives this acknowledgement and generates a corresponding D-Ack message to the IPS Ground System with N(R) of 4 and N(S) of 3.

6.2.3 Order of operations: Compression and MIC Generation / Verification

Data compression / decompression and MIC generation / verification are done by both the IPS Aircraft and the IPS Gateway. Data is compressed in two iterations in order to support efficient segmentation, first the ATNPKT user data is compressed, then the IPv6 and UDP header are compressed. Compression of the user data will only be done when it results in a size reduction and will be denoted through the compression flag.

After generating the IPv6 uplink packet, the IPS Gateway will calculate the MIC and put the last 4 bytes of the computed MIC at the end of the IPv6 uplink packet. Other than the authentication exchange, all messages will have MIC computed and included.

When receiving a downlink, the IPS Gateway will compute MIC and compare the MIC with the MIC at the end of the downlink packet. If the MICs do not compare the message shall be discarded after being logged.

The processing steps for downlinks and uplinks are detailed below (using VDLm2 as the transmission media). Note that a MIC is also computed for each VDLm2 segment, which is independent of the IPv6 MIC.

<u>Downlink (IPS Aircraft generating message that will go to IPS End System)</u>

A. From IPS Aircraft to Ground Station

1. If the user data is reduced in size by compression, set compression bit and compress the user data using Deflate
2. Determine the number of ATNPKTs to handle the user data (max user data size is 1024 bytes)
3. Put together the IPv6 packet
    a. Add ATNPKT fixed and variable parts for each segment
    b. Add UDP header
    c. Add IPv6 header
4. Compress the IPv6 header +UDP header using ROHC
5. Compute the MIC (see Figure 5-18), add the last 4 bytes of the MIC at the end of the IPv6 packet
6. Utilize ‘orange’ protocol for link layer segmentation
7. Compute MIC over the downlinkVDLm2 packet (see Figure 5-20) and add the last 4 bytes of the MIC at the end of the packet
8. Add IPI at front of the packet
9. Add the AVLC UI frame

B. From Ground Station to IPS Gateway

10. The Ground Station, based on the IPI, determines the message is an IPS message
11. The Ground Station deliver message for delivery to the IPS Gateway

C. From IPS Gateway to IPS End System

12. The IPS Gateway computes the MIC on the VDL downlink packet and compares the last 4 bytes against the MIC appended to the downlink packet, if they don’t match the message and the MIC status are logged and a TLS error message is sent
13. The link layer segments (orange protocol) are reassembled

14. Compute the IPv6 MIC and compare with the last 4 bytes of the MIC with the MIC included at the end of the received IPv6 packet, if they don't match log the status and generate a TLS error message
15. The IPS Gateway decompresses the IPv6 & UDP headers, extracts the ATNPKT segments and rebuilds the user data
16. The IPS Gateway checks the compression bit and decompresses the user data if it was compressed
17. The IPS Gateway segments the ATNPKT data if needed
18. The IPS Gateway puts together the IPv6 packet destined for the IPS Ground System
    a. Add ATNPKT fixed and variable parts for each segment
    b. Add UDP header
    c. Add IPv6 header

Uplink (message from IPS End System that will go to IPS Aircraft)

A. From IPS Gateway to Ground Station

1. If the user data is reduced in size by compression, set compression bit and compress the user data (this is data from IPS Ground System) using Deflate
2. Determine the number of ATNPKTs to handle the user data (max user data size is 1024 bytes)
3. Put together the IPv6 packet
    a. Add ATNPKT fixed and variable parts for each segment
    b. Add UDP header
    c. Add IPv6 header
4. Compress the entire IPv6 header +UDP header using ROHC
5. Compute the MIC (see Figure 5-18), add the last 4 bytes of the MIC at the end of the IPv6 packet
6. Utilize 'orange' protocol for link layer segmentation
7. Add the AVLC address and link control fields
8. Compute MIC over the downlinkVDLm2 packet (see Figure 5-20) and add the last 4 bytes of the MIC at the end of the packet
9. Add IPI at front of the packet
10. The IPS Gateway delivers message to the Ground Station

B. From Ground Station to IPS Aircraft

11. Completes the AVLC UI frame and sends to aircraft

6.2.4 IPS Aircraft (Avionics) Initiated Downlink Messages

The IPS Aircraft can initiate the following ATNPKT messages for downlink to an IPS Ground System:

- D-Start
- D-Data
- D-End
- D-Abort

This section provides details on these ATNPKT messages in downlinks addressed to IPS Ground Systems and the role of the IPS Gateway as a "middle man". The format of these messages has already been described in 6.2.1; the focus here is their usage.

6.2.4.1 IPS Aircraft Initiated D-Start Session

The IPS Aircraft will initiate a communication session with an IPS Ground System using the D-Start message, with the IPS Ground System completing the start with a D-Start(cnf) response.

Figure 6-31 shows an example of a D-Start exchange and Figure 6-32 shows a failure of the D-Start.

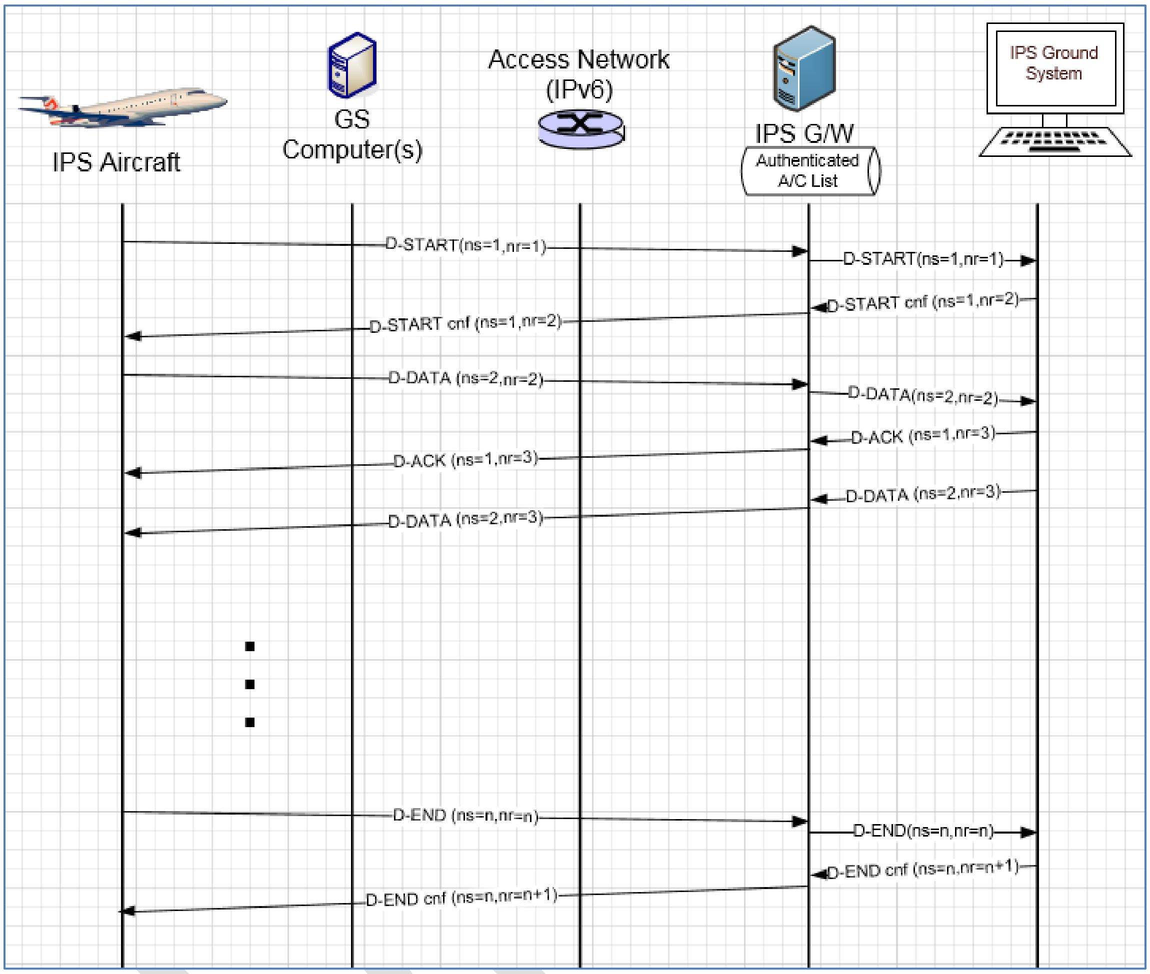


Figure 6-31 – D-Start Scenario

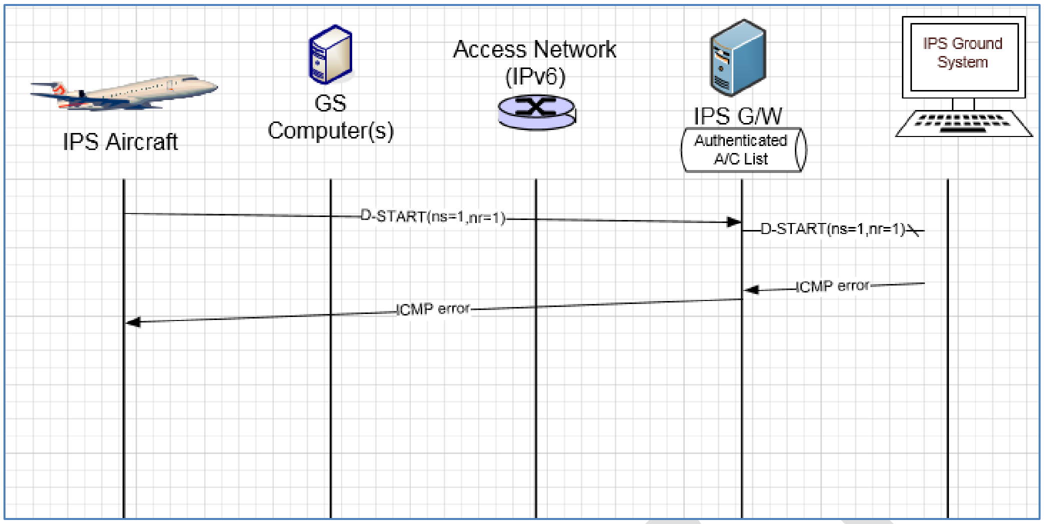


Figure 6-32 – D-Start failure scenario

6.2.4.2 IPS Aircraft Initiated D-Data Message (via Satcom)

IPS Aircraft sends data to an IPS Ground System through the D-Data message. The D-Data message is acknowledged by the IPS Gateway via a D-Ack response (indicating the next expected sequence number) or through an imbedded acknowledgement (by incrementing the next expected sequence number) in another message such as uplink D-Data or a D-End. The D-Data message is segmented as needed by the IPS Aircraft to fit within the IPv6 MTU size. The IPS Aircraft maintains timers waiting for acknowledgement and retransmits as needed.

Figure 6-33 shows an example of a 2 segment downlink for an IPS Ground System. The message is sent via Satcom. In this example (starts below the dashed line, the part above the dashed line is just to illustrate previous data exchange to show how sequence numbers get incremented):

- Avionics generates message for transmission to an IPS Ground System, the message with ATNPKT user data greater than 1024 bytes, requires breaking down into 2 segments
- The two segments are transmitted one after another with sequence numbers 2 and 3
- received by the Satcom ground earth station (GES) and sent to IPS Gateway
- IPS Gateway receives segments, computes and compares MIC, expands IPv6 and UDP header, creates 2 segments for transmission to IPS Ground System
- IPS Gateway acknowledges receipt of the first segment (Ns 2) to IPS Aircraft after expiry of acknowledgement timer
- IPS Gateway waits to receive an acknowledgement from the IPS Ground System before acknowledging the final segment (upon receipt of the acknowledgement N(R)=4, the IPS Gateway generates an acknowledgement N(R)=4 to the IPS Aircraft)

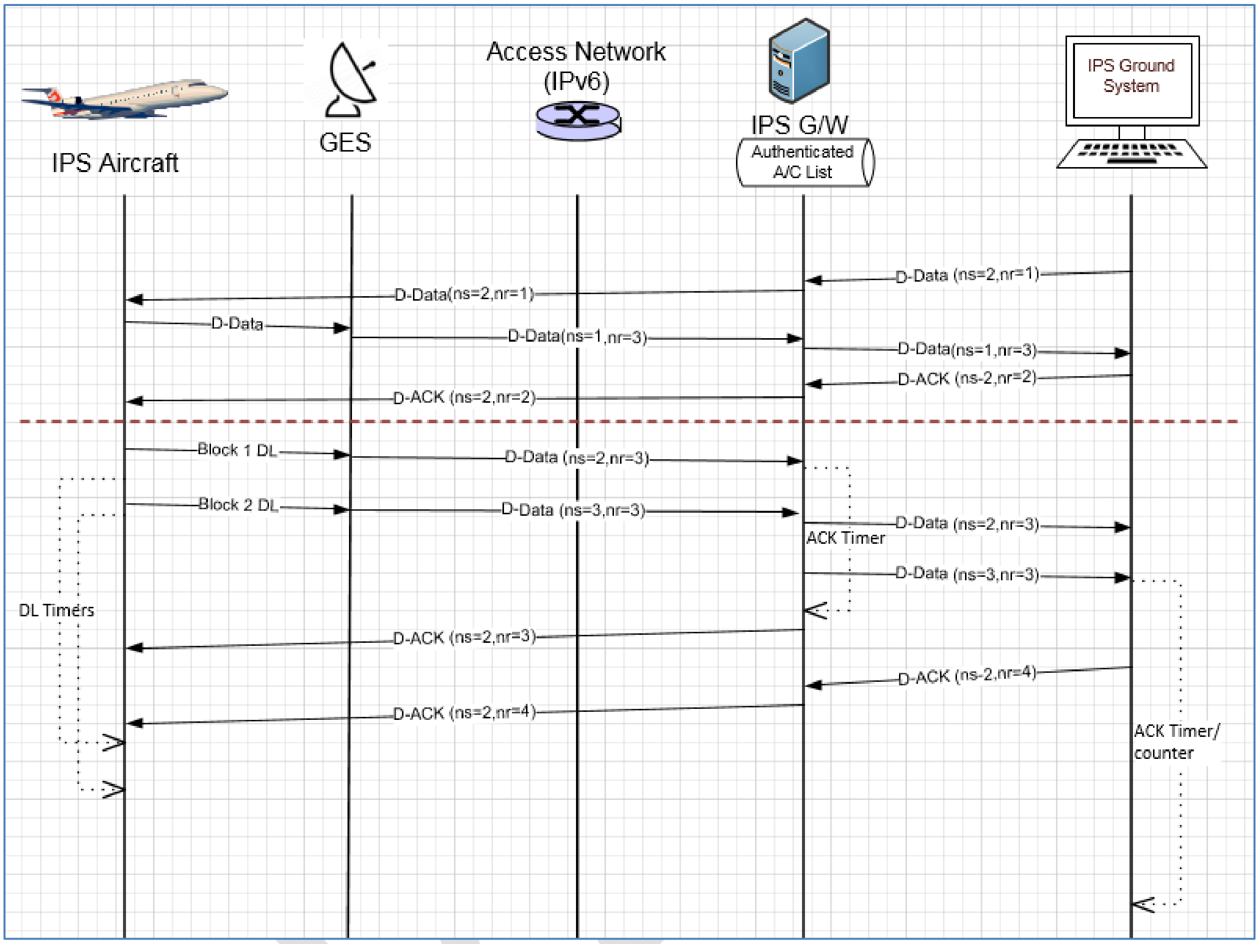


Figure 6-33– Five segment DL to IPS Ground System

6.2.4.3 IPS Aircraft Initiated D-Data Message (via VLDm2)

D-Data messages sent via VDL mode 2 are subject to the 'orange' protocol which provides the link layer segmentation. Because the VDLm2 MTU size is smaller than the IPv6 MTU size, the link layer needs to provide the segmentation.

Figure 6-34 shows an example of a single (ATNPKT) segment downlink to an IPS Ground System that has to be segmented by the 'orange' protocol to fit within the VDL mode 2 MTU size. In this example:

- Avionics generates message for transmission to an IPS Ground System, the message with ATNPKT user data of 600 bytes fits within one ATNPKT (and therefore one IPv6 packet), however it is too large for one AVLC frame
- The segmentation for the link layer is done by the 'orange' protocol and results in three segments.
- The three segments are transmitted one after another with message number 1 and sequence numbers 1, 2 and 3
- The messages are received by multiple ground stations, each prepends signal strength value (SSV) and sends to IPS Gateway
- IPS Gateway provides link layer acknowledgement for the three segments

- IPS Gateway computes and compares MIC for each segment
- IPS Gateway reassembles the segments, expands IPv6 and UDP header, creates 1 segment for transmission to IPS Ground System
- IPS Gateway waits to receive an acknowledgement from the IPS Ground System before acknowledging the ATNPKT D-Data with a D-Ack (this is sent a single segment orange protocol message since it fits within the AVLC MTU)

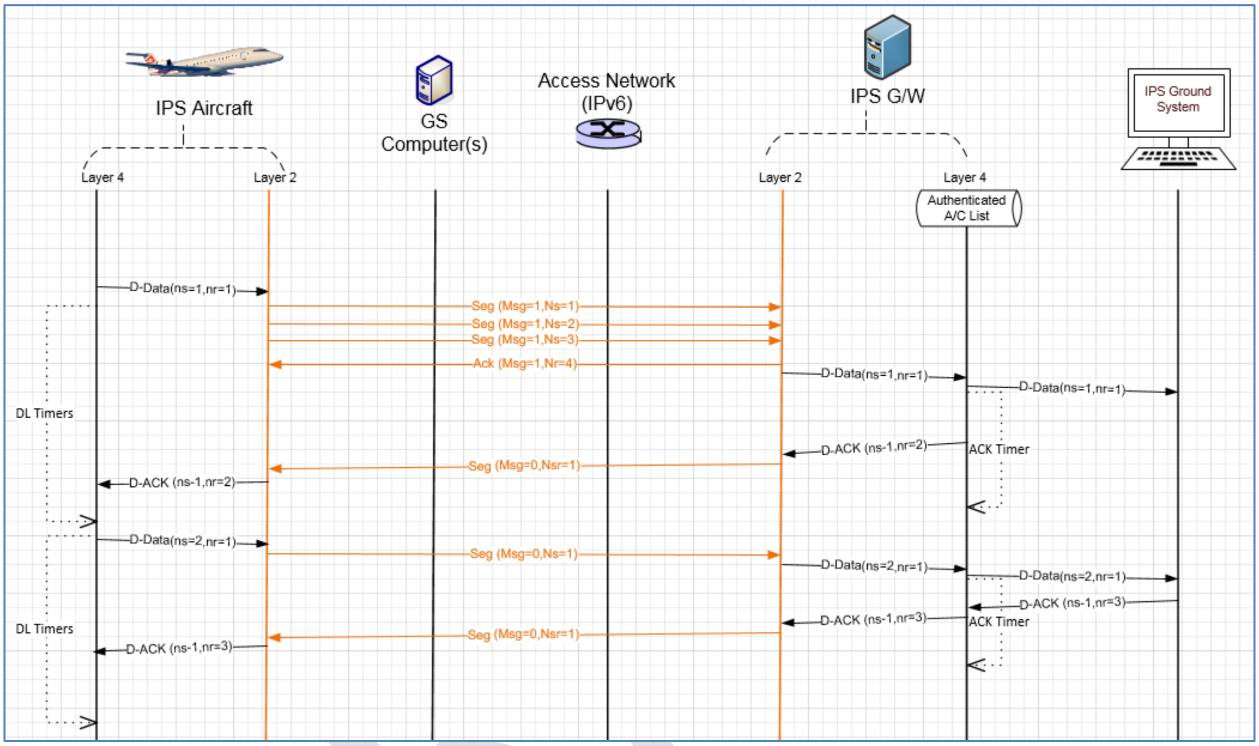


Figure 6-34 - Segmentation using Orange protocol

6.2.4.4 IPS Aircraft Initiated D-End

D-End can be initiated by the IPS Aircraft to terminate a dialogue with a peer DS-user in an orderly manner such that any data in transit between the DS-peers is delivered before the unbinding is completed.

Figure 6-35 shows an example of a D-End sequence. In this example a D-End is generated by the aircraft at the same time that a D-Data is sent by the IPS Ground System. The IPS Ground System waits for acknowledgement of the D-Data before sending the confirmation to the D-End.

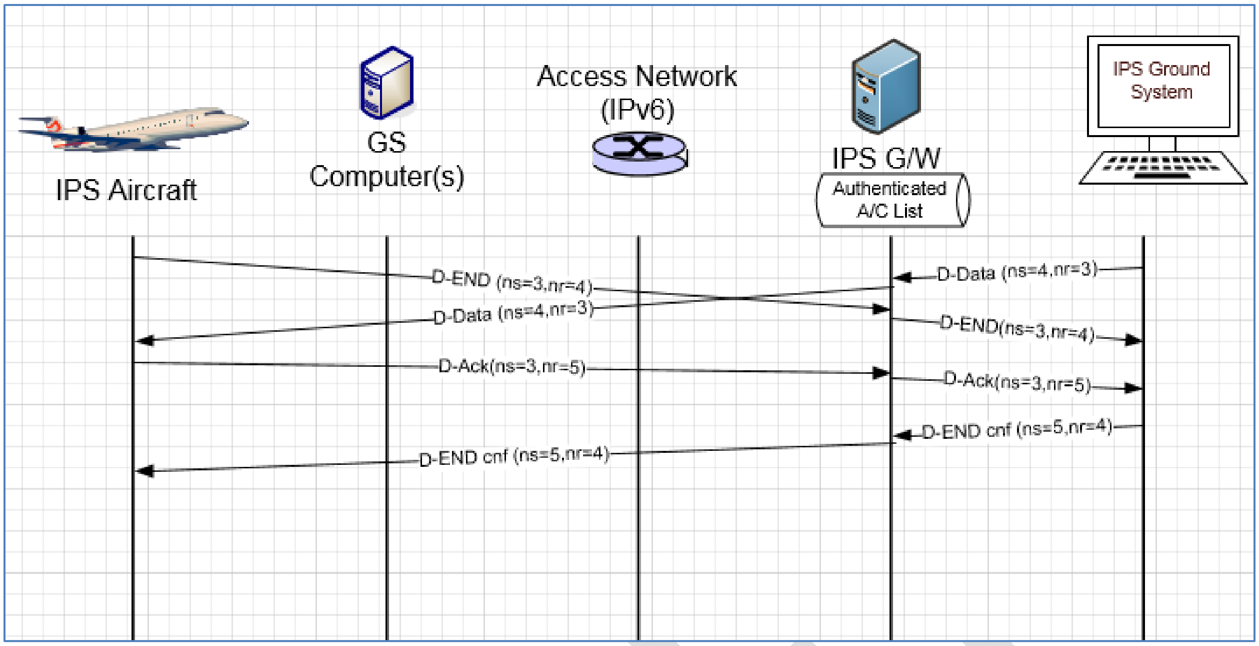


Figure 6-35 – D-End Scenario

Figure 6-36 shows an example of a D-End cnf - reject sequence. In this example a D-End is generated by the aircraft at the same time that a D-Data is sent by the IPS Ground System. The IPS Ground System waits for acknowledgement of the D-Data but this is not received within a time parameter so it generates a D-End confirm with a reject status.

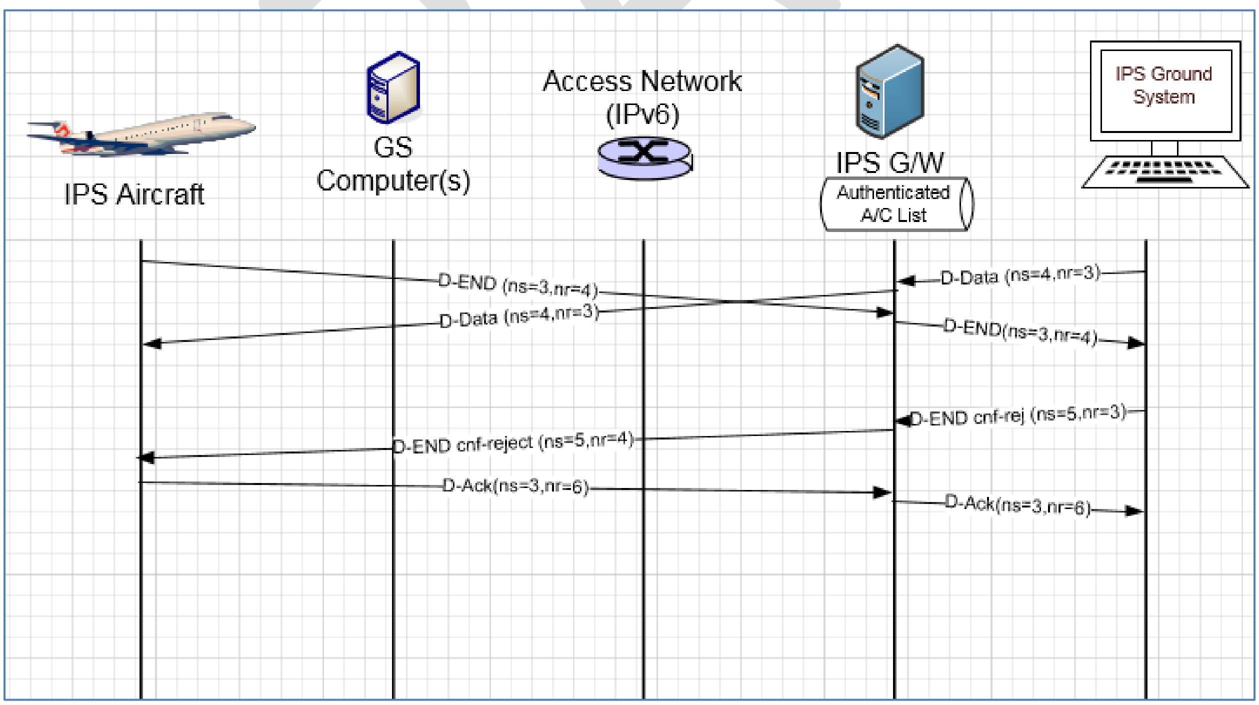


Figure 6-36 – D-End Cnf (reject) Scenario

6.2.4.5 IPS Aircraft Initiated D-Abort

D-Abort can be initiated by the aircraft to terminate communicating with a peer DS-user. Any data in transit may be lost.

Figure 6-37 shows an example of a D-Abort scenario with a D-Data coming from the IPS Ground System that will not be acknowledged.

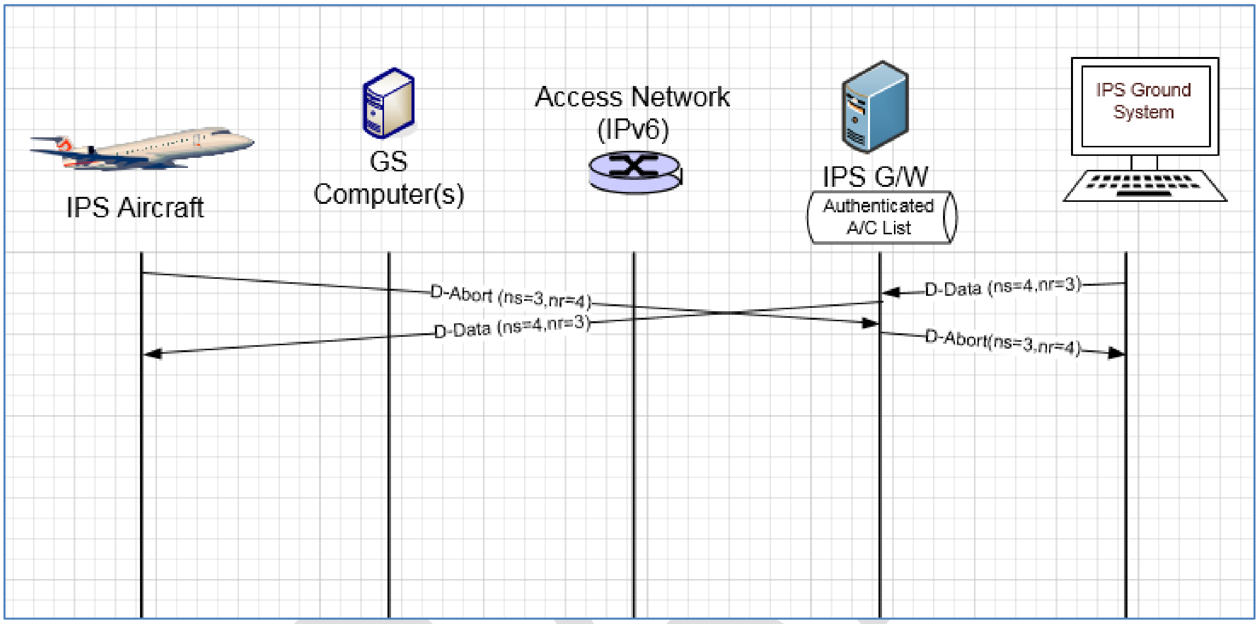


Figure 6-37 – D-Abort Scenario

6.2.5 IPS Ground System Initiated Uplink Messages

The IPS Ground System can initiate the following ATNPKT messages for uplink:

- D-Start
- D-Data
- D-End
- D-Abort

This section provides details on these ATNPKT messages in uplinks addressed to IPS Aircraft and the role of the IPS Gateway as a "middle man". The format of these messages has already been described in 6.2.1; the focus here is their usage.

6.2.5.1 IPS Ground System Initiated D-Start Session

The IPS Ground System initiated communication session with an IPS Aircraft is through the D-Start message. The IPS Aircraft responds with a D-Start(cnf). The scenario is the reverse of that shown in Figure 6-31.

6.2.5.2 IPS Ground System Initiated D-Data Message

IPS Ground System sends data to an IPS Aircraft through the D-Data message. The D-Data message from the IPS Ground System is received by the IPS Gateway, which logs the message and notes the sequence number. The IPS Gateway prepares and transmits the message to the aircraft. The D-Data is acknowledged by the IPS Aircraft via a D-Ack response (indicating the next expected sequence number) or through an imbedded acknowledgement (by incrementing the next expected sequence number) in another message such as a downlink D-Data or a D-End. The IPS Gateway does not acknowledge the IPS

Ground System until an acknowledgement has been received from the IPS Aircraft. The IPS Gateway maintains timers waiting for acknowledgement and retransmits as needed. The Gateway processing for D-Data uplink is described below for IP and non-IP based datalink.

6.2.5.2.1 IP based data link D-Data uplink

Figure 6-38 shows an example of an uplink for an IPS Ground System transmitted via Satcom. In this example:

- IPS Ground System generate a two block message (ATNPKT user data > 1024) with sequence numbers 1 and 2 for transmission to an IPS Aircraft, the message is sent to the IPS Gateway
- The message is logged, sequence numbers are noted, the user data and IPv6 / UDP headers are compressed. Compression in this example does not change that two ATNPKTs need to be transmitted
- The two blocks are sent to the IPS Aircraft (via Satcom), however the second segment gets lost in transmission. The aircraft acknowledges the first segment by sending a D-Ack with next expected sequence number of 2 (acknowledgement is based on the high watermark).
- IPS Gateway waits for the expiry of the uplink timer before resending segment sequence number 2
- IPS Aircraft immediately acknowledges this segment, since it is the last segment in the message (More bit set to '0') and all segments have been received correctly, with a D-Ack with the next expected sequence number set to 3)
- IPS Gateway receives the acknowledgement and immediately generates an acknowledgement (next expected sequence number 3) to the IPS Ground System

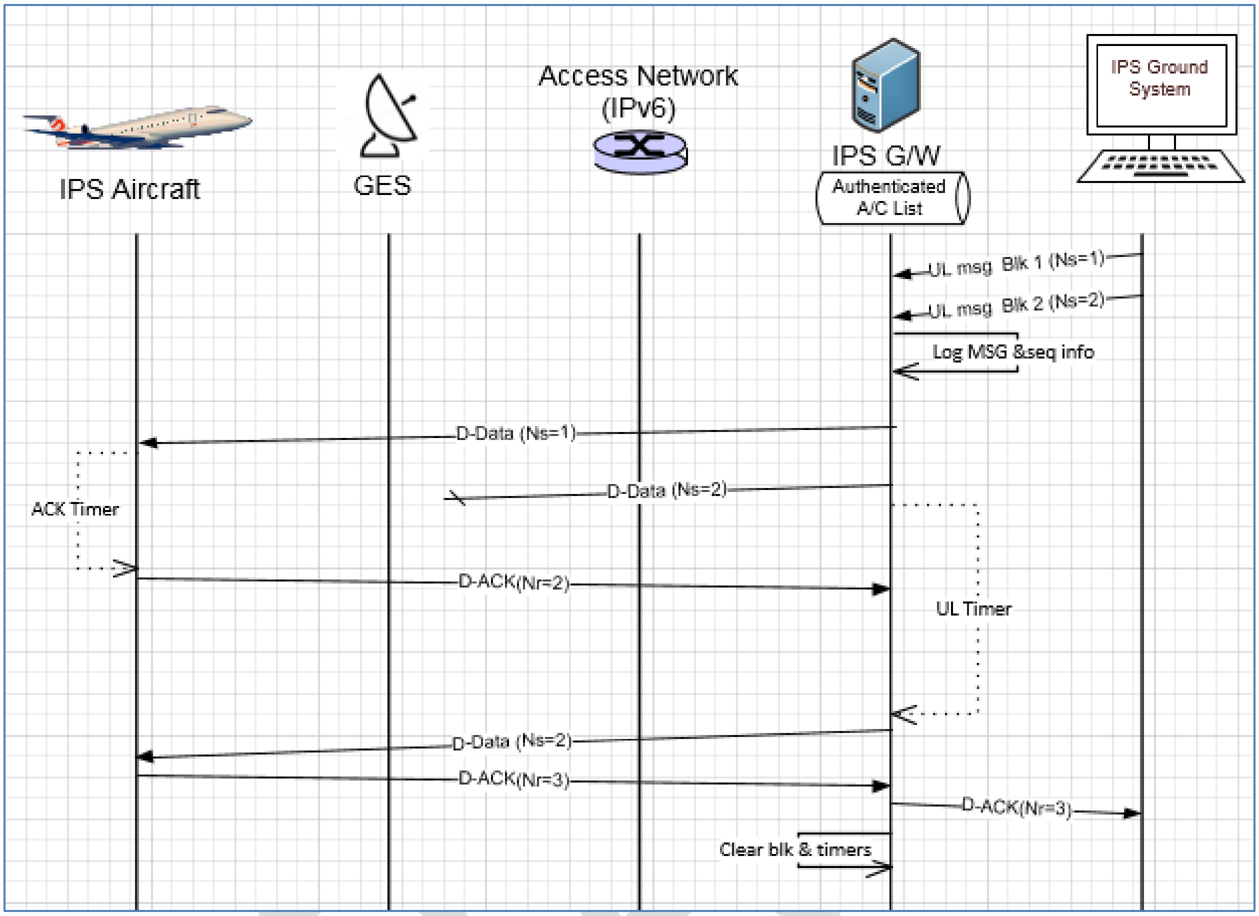


Figure 6-38 – Uplink from IPS Ground System (via Satcom)

6.2.5.2.2 Non-IP based datalink D-Data uplink

Figure 6-39 shows an example of an uplink for an IPS Ground System transmitted via VDL mode 2. In this example:

- IPS Ground System generate a message (sequence number 1) for transmission to an IPS Aircraft, the message is sent to the IPS Gateway
- The message is logged, sequence numbers are noted, the user data and IPv6 / UDP headers are compressed. Even with compression, the message is too large to fit within on AVLC frame.
- The segmentation for the link layer is done by the ‘orange’ protocol and results in three segments.
- The three segments are transmitted one after another with message number 1 and sequence numbers 0, 1, and 2 via the optimal ground station
- Link layer acknowledgement is received for the first two segments but not the third. After the ack timer expires, the third segment is retransmitted.
- The MIC is computed for each segment and compared with the MIC in the segment
- The IPS aircraft link layer reassembles the message and sends to upper layer for processing
- The IPS aircraft generates a D-ACK for the D-Data and passes message to the link layer for transmission. Since the message is small only one segment is required (message number 0,

which indicates a single segment message, sequence number 0 because it is irrelevant) which does not get a link layer ack

- The IPS Gateway receives the single segment link layer message containing the D-Ack, after checking the MIC the message is passed to the upper layer.
- As soon as the IPS Gateway receives the D-Ack from the aircraft, it generates a D-Ack to the IPS Ground System.

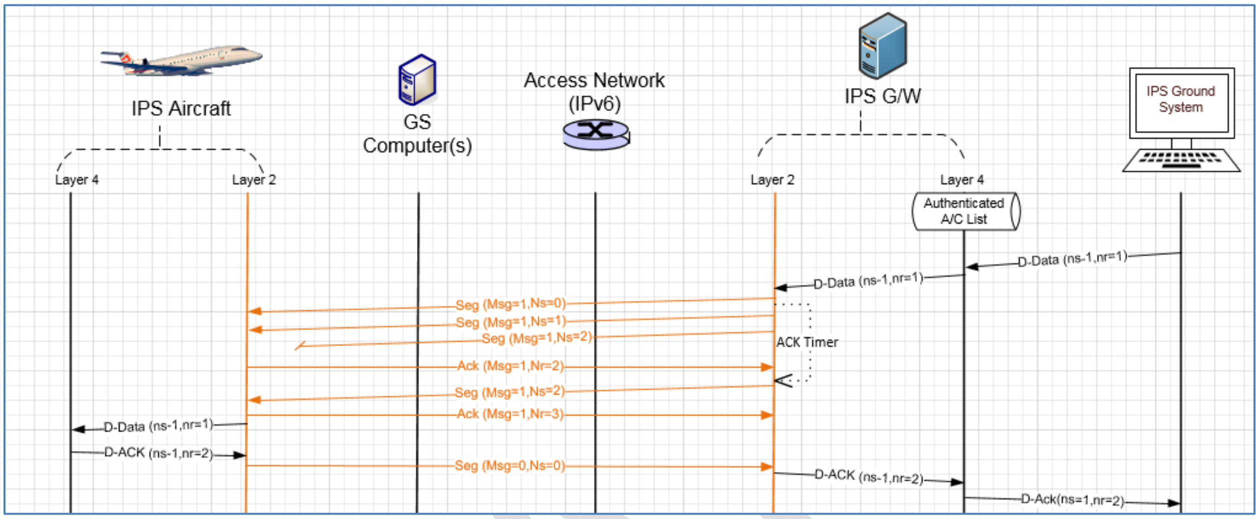


Figure 6-39 - Uplink from IPS Ground System (via VDLm2)

6.2.5.3 IPS Ground System Initiated D-End

D-End can be initiated by the IPS Ground System to terminate a dialogue with an IPS Aircraft in an orderly manner such that any data in transit between the DS-peers is delivered before the unbinding is completed.

Figure 6-35 shows an example of a D-End sequence in the reverse direction.

6.2.5.4 IPS System Initiated D-Abort

D-Abort can be initiated by an IPS Ground System to terminate communicating with an IPS Aircraft. Any data in transit may be lost. The scenario in Figure 6-37 is the reverse of the case described here. D-Abort IPS Ground System initiated

6.2.6 Additional Scenarios (IPS Aircraft – IPS Ground System)

Additional scenarios are provided to further illustrate the flow between IPS Aircraft and IPS Ground System, through the IPS Gateway.

Combined uplink & downlink scenario (IPS Aircraft – IPS Ground System)

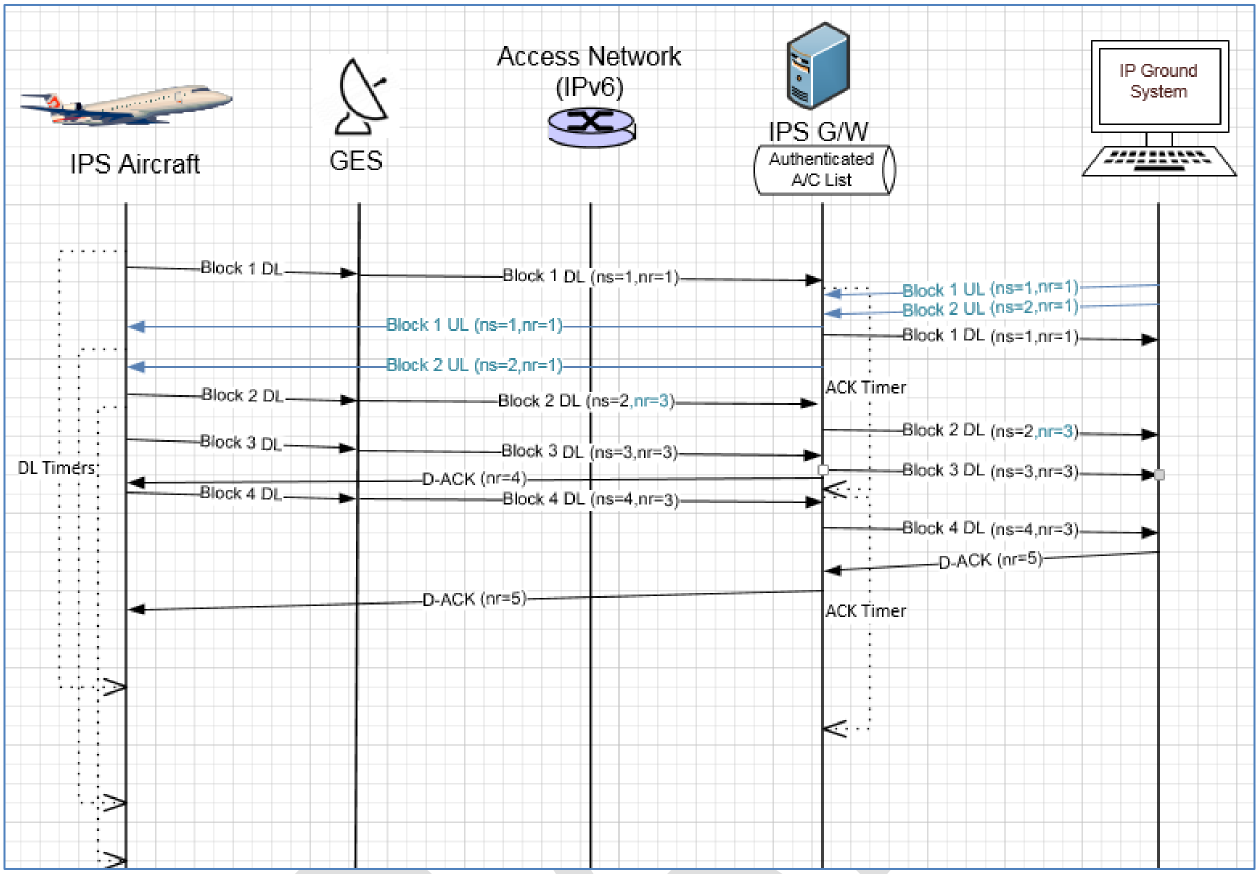


Figure 6-40 – Combined Uplink / Downlink Scenario

In this example (Figure 6-40) a downlink is being sent down at the same time as an uplink is going to an IPS Aircraft. For the uplink:

- IPS Ground System generates a two block uplink message which gets routed to the IPS Gateway
- IPS Gateway receives the 2 segments and sends it to the IPS Aircraft via Satcom
- The IPS aircraft receives the 2 segment message and acknowledges the receipt by imbedding the acknowledgement [N(R)=3] in a downlink that is in process
- IPS Gateway receives the acknowledgement and generates an acknowledgment [N(R)=3] to the IPS Ground System

For the downlink:

- IPS Aircraft generates a 4 segment downlink (sequence numbers [N(S)] 1 through 4) and sends the segments sequentially (embedding the acknowledgement to the uplink in the 2nd segment)
- The downlinked segments are routed from the ground earth station to the IPS Gateway
- IPS Gateway acknowledges receipt of the segments 1-3 to IPS Aircraft after expiry of acknowledgement timer with a D-Ack [N(R)=4]
- IPS Gateway sends the segments to the IPS Ground System
- IPS Gateway waits to receive an acknowledgement from the IPS Ground System before acknowledging the final segment (upon receipt of the acknowledgement N(R)=5, the IPS Gateway generates an acknowledgement N(R)=5 to the IPS Aircraft)

This scenario highlights the management of the sequence numbers.

Uplinks from two IPS Ground Systems to one IPS Aircraft

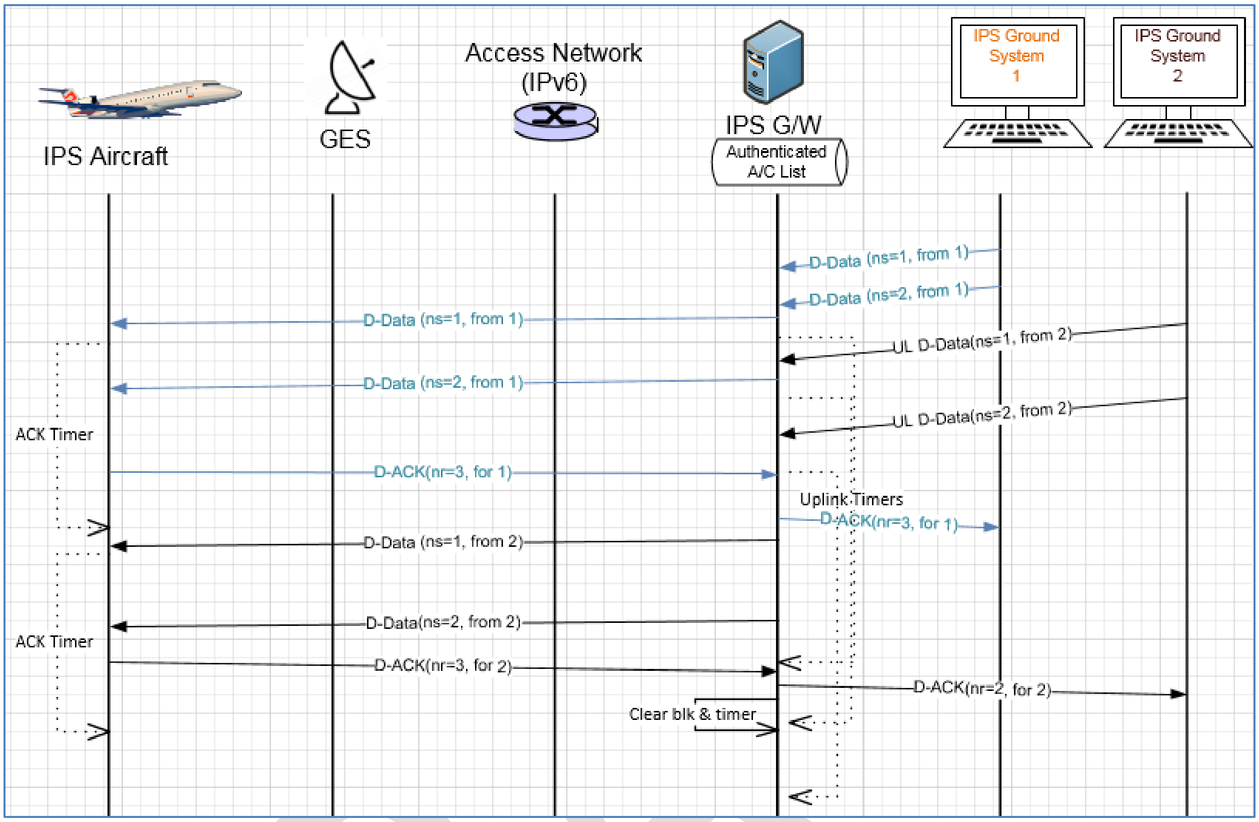


Figure 6-41 – Uplinks from two IPS Ground Systems Scenario

This scenario (Figure 6-41) shows an example of uplinks going to one IPS Aircraft from two different IPS Ground Systems. The key point to note is that the sequence numbers are independent for each source address / port – destination address / port pair.

Unsuccessful uplink

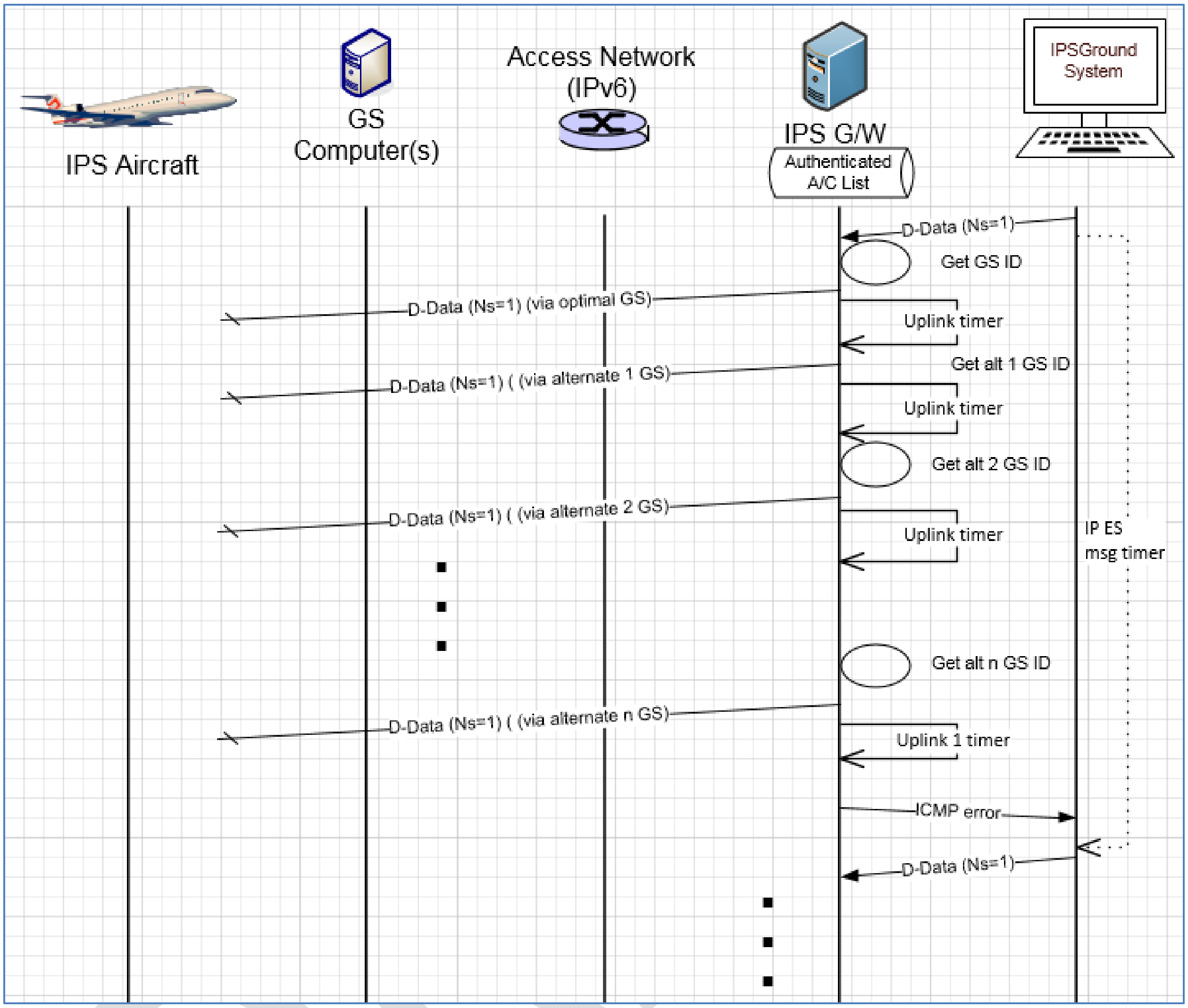


Figure 6-42 – Unsuccessful uplink

This scenario (Figure 6-42) shows the sequence for an unsuccessful uplink. In this scenario:

- Uplink input is destined for an IPS Aircraft is routed to the IPS Gateway from IPS Ground System
- IPS Gateway identifies the optimal ground station from the tail scorecard and sends to that ground station for delivery to the aircraft
- The grounds station does not do any retries if there is no acknowledgement from the aircraft, retries are handled by the IPS Gateway
- IPS Gateway selects the best alternate ground station and sends the message to it for retransmission to the aircraft
- The IPS Gateway goes through its scorecard within parameter time before it has to respond back to the IPS Ground System
- With no acknowledgement received, an ICMP error is sent to the IPS Ground System
- The IPS Ground System will try resending the message which starts a new sequence of attempts to deliver

<u>Uplink with missing Acknowledgements scenario</u>

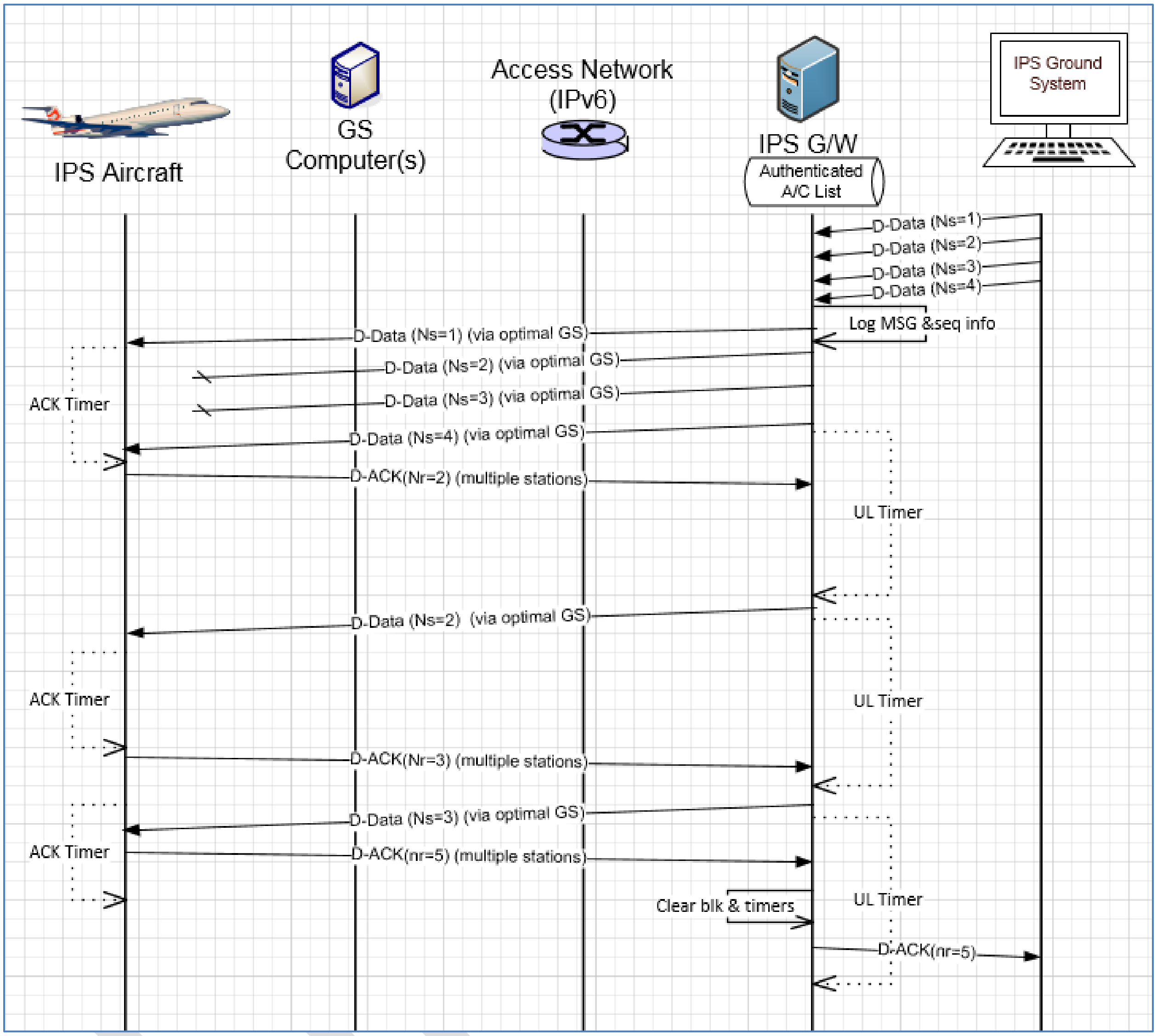


Figure 6-43 – Uplink with missing Acknowledgements scenario

This scenario (Figure 6-43) shows the sequence when acknowledgement is missing for a couple of segments in a 5 segment uplink. . In this scenario:

- A input from IPS Ground System is a 4 segment message and they are sent via the optimal ground station to the IPS Aircraft (layer 2 segmentation is not shown in this example)
- Acknowledgement is received for the first segment
- After the timer waiting for acknowledgement expires, the IPS Gateway retransmits the oldest unacknowledged segment (Ns=2)
- The message is sent to the optimal ground station for delivery (this may be a different ground station then previously tried as the optimal station could have been updated by the receipt of the last acknowledgement)
- Acknowledgement is received for the resent segment, indicating that there are one or more segments that need to be resent
- Segment Ns=3 is then retransmitted via the optimal ground station (again may be different then original due to update from D-Ack receipt)

- IPS aircraft receives this segment and this completes the receipt of the message so it generate an acknowledgement (Nr=5) for the last 2 segments of the uplink
- Upon receipt of this acknowledgement, a D-Ack is generated back to the IPS Ground System

6.3 IPS Aircraft – A620 Host

Figure 3-5 shows the communications path between the IPS Aircraft and the ARINC 620 (A620) Host. The DS peers are the IPS Aircraft (avionics) and the IPS Gateway. For IPS Aircraft to A620 Host data exchange the IPS Gateway provides an IP termination point and supports the IP - A620 conversion for messages to/from the A620 Host System.

The following are the general requirements for the IPS Gateway for IPS Aircraft to A620 Host communications which are similar to the general requirements for IPS Aircraft to IPS Ground System:

- Maintaining key aircraft information (tail number, flight id) for each authentication event
- Maintain session key for MIC computation and encryption
- Maintaining a Session Record for the specific "connection", defined by:
    - Source Port – Destination Port Pair, and
    - Source IP Address – Destination IP Address Pair
- Managing, for each established Session, the sequence numbers
- For Downlink, supporting:
    - Uncompressing downlink messages
    - Support ATNPKT segmentation and reassembly as required
    - Acknowledgement of downlink blocks based on the "More" bit setting
        - "More" bit set – Gateway can acknowledge blocks based on internal Acknowledgement timer
        - "More" bit not set – Gateway acknowledges message immediately
    - Generating A620 message from the downlink message and sending to A620 Host
- For Uplink, supporting:
    - Generation of ATNPKT from A620 message, ATNPKT segmentation of larger messages for IPS Aircraft delivery
    - For large message, perform ATNPKT segmentation
    - Compressing messages
    - Message Assurance response (if requested) or appropriate reject response is provided to A620 Host in the same manner as done currently
- Supporting key based include key-based message integrity calculations to include with uplink messages and to use for validating integrity of downlink messages
- Supporting determination of optimal ground station for uplink delivery (for VDL)
- Supporting the IPv4 interface to/from the Ground Stations

There are three distinct phases in the transport of the downlink and uplink messages:

Transmission Leg	Mechanism	Notes
Downlink Messages		
IPS Aircraft (Avionics) → GS	SNPDU / AVLC Packet	
GS → IPS Gateway	IPv6 Packet	
IPS Gateway → A620 Host	A620	
Uplink Messages		
A620 Host → IPS Gateway	A620	
IPS Gateway → GS	IPv6 Packet	

GS → IPS Aircraft (Avionics)	SNPDU / AVLC Packet	

Table 5-20 – IPS Transmission Legs for A620 Host

The details of the different packaging of the IPv6 data have been provided in previous sections. The following sections provide details of the ATNPKT for the applicable DS primitives.

6.3.1 ATNPKT Message Set

The following sections identify the format of the ATNPKT message part used for IPS Aircraft – A620 Host communications. Note that for the A620 communication, only the D-Data and D-Ack primitives are applicable.

6.3.1.1 D-Data

The D-Data packet contains A620 data. It consists of the ATNPKT fixed and variable parts, with the variable portion carrying payload data. The variable part content will be dependent on the type of data and whether it is the first or a subsequent fragment in a fragmented message using the More bit.

The following example (Figure 6-44, and Figure 6-45) shows the layout of the ATNPKT for a two segment FANS 1/A downlink message. The presence flag is set for Destination ID, Sequence numbers, Called Peer ID (containing the center name) and User Data. The first segment shows the More bit set to ‘1’, and the first 2 bytes of the data contain the length of the data. The 2nd segment does not repeat the Called Peer ID field. The second segment has the More bit set to ‘0’ indicating the end of the message.

Octet / Offset	0	1	2	3	4	5
0	1 ATNKT ver | 5 DS primitive	more 1 | b011 AppTechType | 0 1 1 0	1 0 0 0 0 0 0 1 Presence flags	Destination Destination ID		1 N(S) | 1 N(R)
6	4 Called Peer ID length	CenterName Called Peer ID				9712 Data length
12	Data length (cont)	Compression Flag	Data			
.....						
1026						
1032						
1038						

Figure 6-44 – D-Data, 1st of 2 segments (FANS 1/A data)

Octet / Offset	0	1	2	3	4	5
0	1 ATNKT ver | 5 DS primitive	more 0 | b011 AppTechType | 0 1 1 0	0 0 0 0 0 0 0 1 Presence flags	Destination Destination ID		2 N(S) | 1 N(R)
6	data					
12						
.....						
186						
192						

Figure 6-45 – D-Data, 2nd of 2 segments (FANS 1/A data)

The example shows:

- ATNPKT version as 1 (always set to 1)
- DS Primitive set to 5 (defines the message as a D-Data)
- More bit as described in the example
- App Tech Type is set to b011 indicating FANS/IPS DS
- The second, third, fifth and last presence field flags are set (indicating destination ID, sequence number, called Peer ID and User Data fields are present)
- Called Peer ID field is only present in the first segment
- Sequence numbers (number sent are sequential 1-2 and next expected to be received is 1)

6.3.1.2 D-ACK

The D-Ack message for A620 data is identical as the D-Ack described in section 6.2.1.4

6.3.2 Message Segmentation

The same constraints for downlink / uplink data exchange between IPS Aircraft and IPS Gateway described in section 6.2.2 apply, that require the message to be broken down into segments utilizing the ATNPKT More bit when the user data size exceeds 1024 bytes. Additionally subnetwork segmentation may be required, for example for VDL if the 251 byte AVLC packet size is exceeded. The IPS Aircraft, since it knows the AVLC packet size, will segment the message appropriately. On the other hand, A620 messages can be large; therefore a message received from an A620 Host that exceeds the 1024 byte user data maximum will be segmented at the ATNPKT level, while segmentation for the AVLC packet limitations will be done using the orange protocol. Both segmentations will be managed by the IPS Gateway. Management of the message segmentation by the IPS Gateway for A620 messages includes the following functionality:

- Segmentation of uplink messages using the ATNPKT More bit for user data exceeding 1024
- Reassembly of downlink messages received from an IPS Aircraft using the ATNPKT More bit
- Segmentation using the orange protocol for AVLC packet size limit
- Reassembly of the orange protocol segmentation
- Building of the A620 message using data from the ATNPKT and information from the flight authentication record
- Management of acknowledgements to the IPS Aircraft and message assurance to A620 Host

6.3.2.1 Sequence number and acknowledgment management

For data destined for A620 Host, the IPS Gateway is acting as the IPS Ground System, only sequence numbers and acknowledgements between the IPS Gateway and the IPS Aircraft are relevant. There are a number of requirements which impact the IPS Aircraft to A620 Host related sequencing and acknowledgement processing, including:

- Maximum ATNPKT user data size (1024 bytes)
- AVLC packet size (251 bytes)
- Maximum number (16) of unacknowledged ATNPKTs
- Acknowledgement to aircraft after ack timer expiry when more bit set, acknowledgement to aircraft immediately when more bit not sent

6.3.3 Compression and MIC Generation / Verification

The compression and MIC generation / verification for IPS Aircraft – A620 Host messages is consistent with the approach described in 6.2.3.

The processing steps for downlinks and uplinks are detailed below using VDL Mode 2 as the media.

<u>Downlink (IPS Aircraft generating message that will go to A620 Host)</u>

A. From IPS Aircraft to Ground Station

1. Compress the user data using Deflate
2. Determine the number of ATNPKTs to handle the user data (max user data size is 1024 bytes)
3. Put together the IPv6 packet

   a. Add ATNPKT fixed and variable parts for each segment
   b. Add UDP header
   c. Add IPv6 header
4. Compress the entire IPv6 packet (IPv6 header +UDP header + ATNPKT) using ROHC
5. Compute MIC over the IPv6 packet (see Figure 5-18) and add the last 4 bytes of the MIC at the end of the IPv6 packet
6. Utilize 'orange' protocol for link layer segmentation
7. Compute MIC over the downlinkVDLm2 packet (see Figure 5-20) and add the last 4 bytes of the MIC at the end of the packet
8. Add IPI at front of the packet
9. Add the AVLC UI frame

B. From Ground Station to IPS Gateway

10. The Ground Station, based on the IPI, determines the message is an IPS message
11. The Ground Station delivers message to the IPS Gateway

C. From IPS Gateway to A620 Host

12. The IPS Gateway computes the MIC on the VDL downlink packet and compares the last 4 bytes against the MIC appended to the downlink packet, if they don't match the message and the MIC status are logged and a TLS error message is sent
13. The link layer segments (orange protocol) are reassembled
14. Compute the IPv6 MIC and compare with the last 4 bytes of the MIC with the MIC included at the end of the received IPv6 packet, if they don't match log the status and generate a TLS error message
15. The IPS Gateway decompresses the IPv6 & UDP headers, extracts the ATNPKT segments and rebuilds the user data
16. The IPS Gateway checks the compression bit and decompresses the user data if it was compressed
17. The IPS Gateway builds the A620 message from the user data and header contents

<u>Uplink (message from A620 Host that will go to IPS Aircraft)</u>

A. From IPS Gateway to Ground Station

1. Extract header information from the A620 data and the aircraft authentication record
2. If the user data is reduced in size by compression, set compression bit and compress the user data (this is data from IPS Ground System) using Deflate
3. Determine the number of ATNPKTs to handle the user data (max user data size is 1024 bytes)
4. Put together the IPv6 packet
   a. Add ATNPKT fixed and variable parts for each segment
   b. Add UDP header
   c. Add IPv6 header
5. Compress the entire IPv6 Packet (IPv6 header +UDP header) using ROHC
6. Compute the MIC (see Figure 5-18), add the last 4 bytes of the MIC at the end of the IPv6 packet
7. Utilize 'orange' protocol for link layer segmentation
8. Add the AVLC address and link control fields

9. Compute MIC over the downlinkVDLm2 packet (see Figure 5-20) and add the last 4 bytes of the MIC at the end of the packet
10. Add IPI at front of the packet
11. The IPS Gateway delivers message to the Ground Station

B. From Ground Station to IPS Aircraft

12. Completes the AVLC UI frame and sends to aircraft

6.3.4 IPS Aircraft (Avionics) Initiated A620 Downlink Messages

The only A620 message initiated by the IPS Aircraft is the D-Data message. The IPS Aircraft also sends D-Ack messages in response to D-Data uplinks.

6.3.4.1 IPS Aircraft Initiated D-Data Message

The D-Data message is used to send A620 data to an A620 Host. The type of data (AOC, AFN, FANS CPDLC or FANS ADS-C) that is being sent is dependent on the port number.

Figure 6-46 shows an example of a 3 segment downlink intended for an A620 Host. The message is generated by the avionics and:

- 3 blocks are sent one after another
- received by the Satcom ground earth station and sent to IPS Gateway
- IPS Gateway acknowledges receipt of the segments to IPS Aircraft
- IPS Gateway extracts payload from IPv6
- IPS Gateway converts data from binary
- IPS Gateway builds the A620 message and sends to AMQS for delivery to the A620 Host

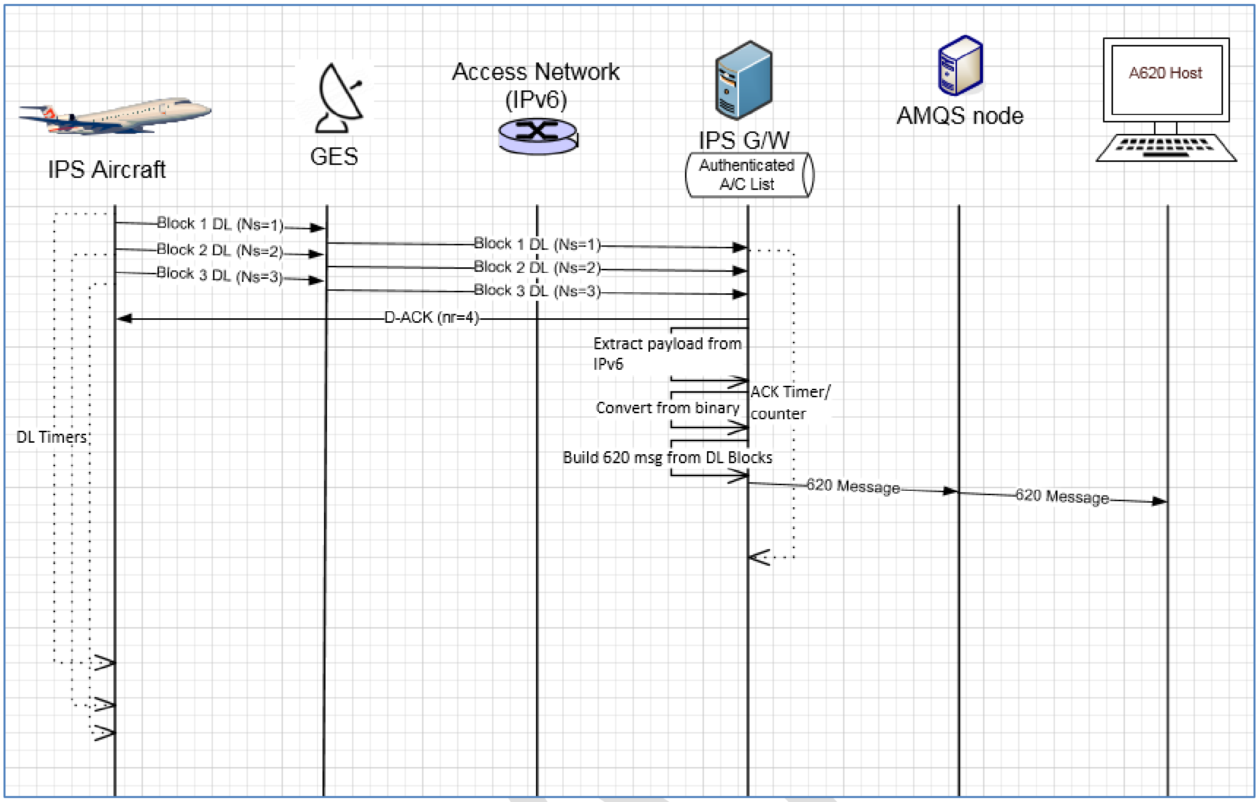


Figure 6-46 – 3 Segment downlink to A620 Host

6.3.4.2 Generating the A620 Message

The IPS Gateway builds the A620 message for sending to the A620 Host from data contained in the ATNPKT (in the variable part including the user data field), and the authentication record for the flight. The following example shows how the content from the IPS message is converted to an A620 message. In this example the downlink message is a CPDLC response of 'ROGER' to a 'EXPECT 20000FT' CPDLC uplink. The example shows the three pieces of data that are the input to building the message and the resultant output message.

CPDLC response of 'ROGER' to a 'EXPECT 20000FT' CPDLC uplink

Inputs

contents of ATNPKT user data

H1#M1/BA OAKXGXA.AT1.N87CR6104F51203116C

contents of relevant ATNPKT header fields

Called Peer (Center Name)	OAKXGXA
Calling Peer (Flight ID)	*

* the flight ID would only be present if the ID had changed from when flight was authenticated

relevant data in flight authentication record

Flight ID	NW1234
Tail number	N87CR

Output

Generated A620 Message

```
QU OAKXGXA
.DDLXXXX 312145
ATC
FI NW1234/AN N87CR
DT DDL XXF 312145 F37A
-  AT1.N87CR6104F51203116C
```

where XXXX is for the IPS Gateway

Figure 6-47 – A620 message construction

6.3.5 A620 Host Initiated Uplink Messages

The initiation of an uplink by an A620 Host is unchanged from current operation and is effectively transparent to the A620 Host. The A620 Host will generate an A620 message for delivery to the aircraft. Functionality on the network will recognize the message is for an IPS Aircraft and route the message to the IPS Gateway for delivery to the IPS Aircraft.

6.3.5.1 A620 Initiated Data Message

Figure 6-48 shows an example of A620 Host initiated uplink to an IPS Aircraft.

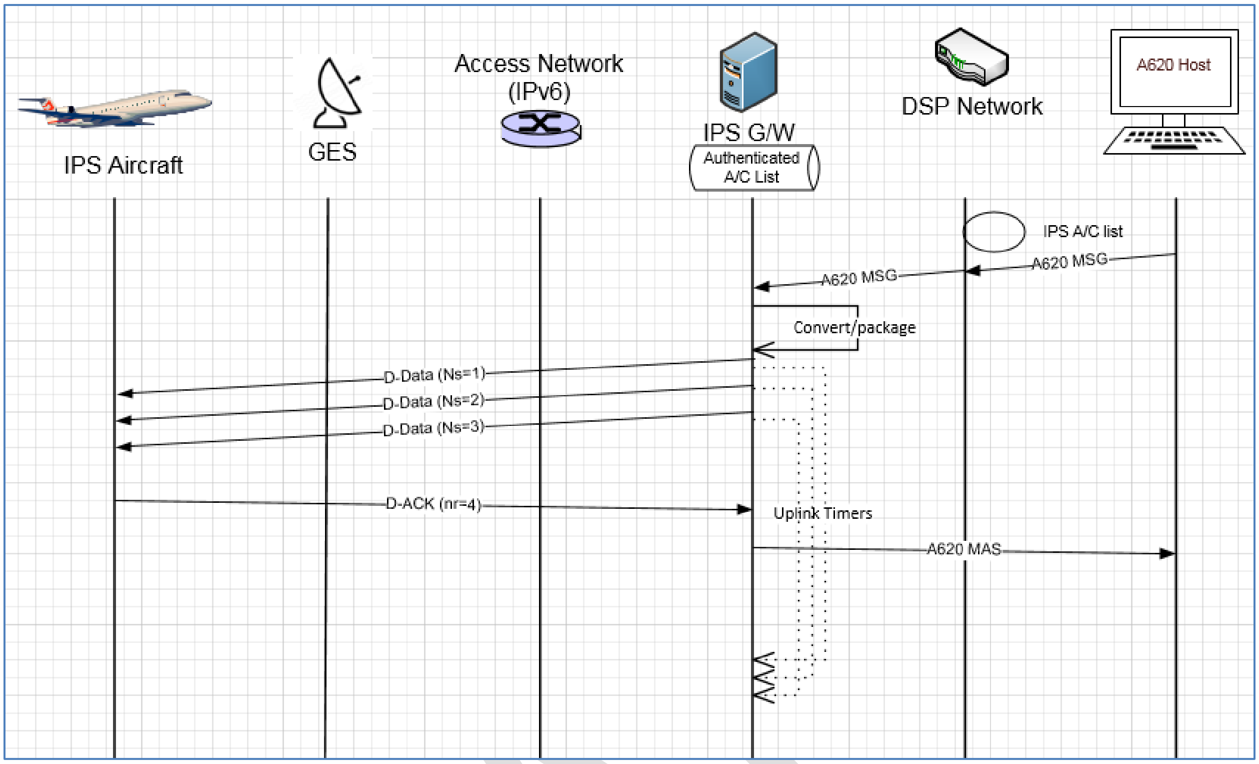


Figure 6-48 – A620 Host initiated uplink scenario

In this example:

- A620 message is generated by a A620 Host and sent to the DSP for delivery to the aircraft
- Functionality within the network determines the message is destined for a flight that is in the IPS A/C list and routes it to the IPS Gateway
- IPS Gateway converts message to binary, segments (sequence number 1-3) and packages in ATNPKT in IPv6, adds IPI in front of the IPv6 packet and sends to Satcom for delivery
- IPS Aircraft generates an acknowledgement to the three segments
- IPS Gateway sends message assurance for the A620 message if it was requested

6.4 IPS Aircraft – ATN/OSI End System

Figure 3-6 shows the communications path between the IPS Aircraft and an ATN/OSI End System. The DS peers are the IPS Aircraft (avionics) and the IPS Gateway. For IPS Aircraft to ATN/OSI End System data exchange the IPS Gateway:

- provides an IP termination point
- provides the ATNPKT - CLNP conversion for messages to/from the ATN/OSI End System
- manages the ATN/OSI connection with the ATN/OSI End System

The following are the general requirements for the IPS Gateway for IPS Aircraft to ATN/OSI End System communications which are similar to the general requirements for IPS Aircraft to A620 Host:

- Maintaining key aircraft information (tail number, flight id) for each authentication event
- Maintaining a Session Record for the specific "connection", defined by:
    - Source Port – Destination Port Pair, and
    - Source IP Address – Destination DTE Address Pair
- Managing, for each established Session, the sequence numbers
- For Downlink, supporting:
    - Uncompressing downlink messages
    - Support ATNPKT segmentation and reassembly as required
    - Acknowledgement of downlink blocks based on the "More" bit setting
        - "More" bit set – Gateway can acknowledge blocks based on internal Acknowledgement timer
        - "More" bit not set – Gateway acknowledges message immediately
    - Generating ATN/OSI message from the downlink message and sending to ATN/OSI End System
- For Uplink, supporting:
    - Generation of ATNPKT from ATN/OSI message, ATNPKT segmentation of larger messages for IPS Aircraft delivery
    - For large message, perform ATNPKT segmentation
    - Compressing messages
- Supporting key-based message integrity calculations to include with uplink messages and to use for validating integrity of downlink messages
- Supporting determination of optimal ground station for uplink delivery

There are three distinct phases in the transport of the downlink and uplink messages:

Transmission Leg	Mechanism	Notes
Downlink Messages		
IPS Aircraft (Avionics) → GS	SNPDU / AVLC Packet	
GS → IPS Gateway	IPv6 Packet	
IPS Gateway → ATN/OSI ES	CLNP	
Uplink Messages		
ATN/OSI ES → IPS Gateway	CLNP	
IPS Gateway → GS	IPv6 Packet	
GS → IPS Aircraft (Avionics)	SNPDU /	

	AVLC Packet	

Table 5-21 - IPS Transmission Legs for ATN/OSI End System

The details of the different packaging of the IPv6 data have been provided in previous sections. The following sections provide details of the ATNPKT for the applicable DS primitives.

6.4.1 ATNPKT Message Set

The ATNPKT message set for IPS – ATN/OSI communications is the same set as defined for IPS – IPS communications defined in section 6.2.1.

6.4.2 Message Segmentation

The same constraints for downlink / uplink data exchange between IPS Aircraft and IPS Gateway described in section 6.2.2 apply, that require the message to be broken down into segments utilizing the ATNPKT More bit when the user data size exceeds 1024 bytes. Additionally subnetwork segmentation may be required, for example for VDL if the 251 byte AVLC packet size is exceeded. The IPS Aircraft, since it knows the AVLC packet size, will segment the message appropriately. On the other hand, ATN/OSI messages can be large; therefore a message received from an ATN/OSI Host that exceeds the 1024 byte user data maximum will be segmented at the ATNPKT level, while segmentation for the AVLC packet limitations will be done using the orange protocol. Both segmentations will be managed by the IPS Gateway. . Management of the message segmentation by the IPS Gateway for ATN/OSI messages includes the following functionality:

- Segmentation of uplink messages using the ATNPKT More bit for user data exceeding 1024
- Reassembly of downlink messages received from an IPS Aircraft using the ATNPKT More bit
- Segmentation using the orange protocol for AVLC packet size limit
- Reassembly of the orange protocol segmentation
- Building of the ATN/OSI message using data from the ATNPKT and information from the flight authentication record
- Management of acknowledgements to the IPS Aircraft

6.4.2.1 Sequence number and acknowledgment management

For data destined to an ATN/OSI End System, the IPS Gateway is acting as the IPS Ground System in relationship to the IPS Aircraft, only sequence numbers and acknowledgements between the IPS Gateway and the IPS Aircraft are relevant. There are a number of requirements which impact the IPS Aircraft to ATN/OSI End System related sequencing and acknowledgement processing, including:

- Maximum ATNPKT user data size (1024 bytes)
- AVLC packet size (251 bytes)
- Maximum number (16) of unacknowledged ATNPKTs
- Acknowledgement to aircraft after ack timer expiry when more bit set, acknowledgement to aircraft immediately when more bit not sent

To the ATN/OSI End System, the IPS Gateway is acting as the ATN/OSI DTE.

6.4.3 Compression and MIC Generation / Verification

The compression and MIC generation / verification for IPS Aircraft – ATN/OSI End System messages is consistent with the approach described in 6.2.3.

The processing steps for downlinks and uplinks are detailed below.

<u>Downlink (IPS Aircraft generating message that will go to ATN/OSI End System)</u>

A. From IPS Aircraft to Ground Station

1. Compress the user data using Deflate
2. Determine the number of ATNPKTs to handle the user data (max user data size is 1024 bytes)
3. Put together the IPv6 packet
    a. Add ATNPKT fixed and variable parts for each segment
    b. Add UDP header
    c. Add IPv6 header
4. Compress the entire IPv6 packet (IPv6 header +UDP header) using ROHC
5. Compute MIC over the IPv6 packet (see Figure 3 9) and add the last 4 bytes of the MIC at the end of the IPv6 packet
6. Utilize 'orange' protocol for link layer segmentation
7. Compute MIC over the downlinkVDLm2 packet (see Figure 3 11) and add the last 4 bytes of the MIC at the end of the packet
8. Add IPI at front of the packet
9. Add the AVLC UI frame

B. From Ground Station to IPS Gateway

10. The Ground Station, based on the IPI, determines the message is an IPS message
11. The Ground Station delivers to the IPS Gateway

C. From IPS Gateway to ATN/OSI End System

12. The IPS Gateway computes the MIC on the VDL downlink packet and compares the last 4 bytes against the MIC appended to the downlink packet, if they don't match the message and the MIC status are logged and a TLS error message is sent
13. The link layer segments (orange protocol) are reassembled
14. Compute the IPv6 MIC and compare with the last 4 bytes of the MIC with the MIC included at the end of the received IPv6 packet, if they don't match log the status and generate a TLS error message
15. The IPS Gateway decompresses the IPv6 & UDP headers, extracts the ATNPKT segments and rebuilds the user data
16. The IPS Gateway checks the compression bit and decompresses the user data if it was compressed
17. The IPS gateway manages the connection to the OSI ground system, it provides a COTP4 link up to session/presentation protocols awaited by the ground OSI systems
18. The IPS Gateway builds the ATN/OSI (CLNP) message from the user data and header contents
19. The IPS Gateway sends the message via the ATN/OSI connection

<u>Uplink (message from ATN/OSI that will go to IPS Aircraft)</u>

A. From IPS Gateway to Ground Station

1. Extract header information from the ATN/OSI data and the aircraft authentication record
2. If the user data is reduced in size by compression, set compression bit and compress the user data (this is data from IPS Ground System) using Deflate
3. Determine the number of ATNPKTs to handle the user data (max user data size is 1024 bytes)
4. Put together the IPv6 packet
    a. Add ATNPKT fixed and variable parts for each segment
    b. Add UDP header
    c. Add IPv6 header
5. Compress the entire IPv6 Packet (IPv6 header +UDP header) using ROHC
6. Compute the MIC (see Figure 3 9), add the last 4 bytes of the MIC at the end of the IPv6 packet
7. Utilize 'orange' protocol for link layer segmentation
8. Add the AVLC address and link control fields
9. Compute MIC over the downlinkVDLm2 packet (see Figure 3 11) and add the last 4 bytes of the MIC at the end of the packet
10. Add IPI at front of the packet
11. The IPS Gateway delivers message to the Ground Station

B. From Ground Station to IPS Aircraft

12. Completes the AVLC UI frame and sends to aircraft

6.4.4 IPS Aircraft (Avionics) Initiated Downlink Messages

The IPS Aircraft can initiate the following ATNPKT messages for downlink destined to an ATN/OSI End System:

- D-Start
- D-Data
- D-End
- D-Abort

This section provides details on these ATNPKT messages in downlinks addressed to the IPS Gateway destined for an ATN/OSI End System. The format of these messages has already been described in 6.2.1; the focus here is their usage.

6.4.4.1 IPS Aircraft Initiated D-Start Session

The IPS Aircraft will initiate a communication session with an ATN/OSI End System using the D-Start message, with the IPS Gateway completing the start with a D-Start(cnf) response after the IPS Gateway initiates the connection with the ATN/OSI End System.

Figure 6-49 shows an example of a D-Start exchange and Figure 6-50 shows a failure of the D-Start. The key point in both examples is that the IPS Gateway immediately acknowledges the message to avoid a timeout while the connection is being established. The IPS Gateway performs the NSAP lookup to obtain the address of the destination facility and initiates a connection with the facility via the ATN/OSI network. The IPS Gateway acts as an ATN DTE. Once the connection is established (or if the connection cannot be established), the IPS Gateway sends a D-Start cnf response (accepted or rejected) back to the aircraft.

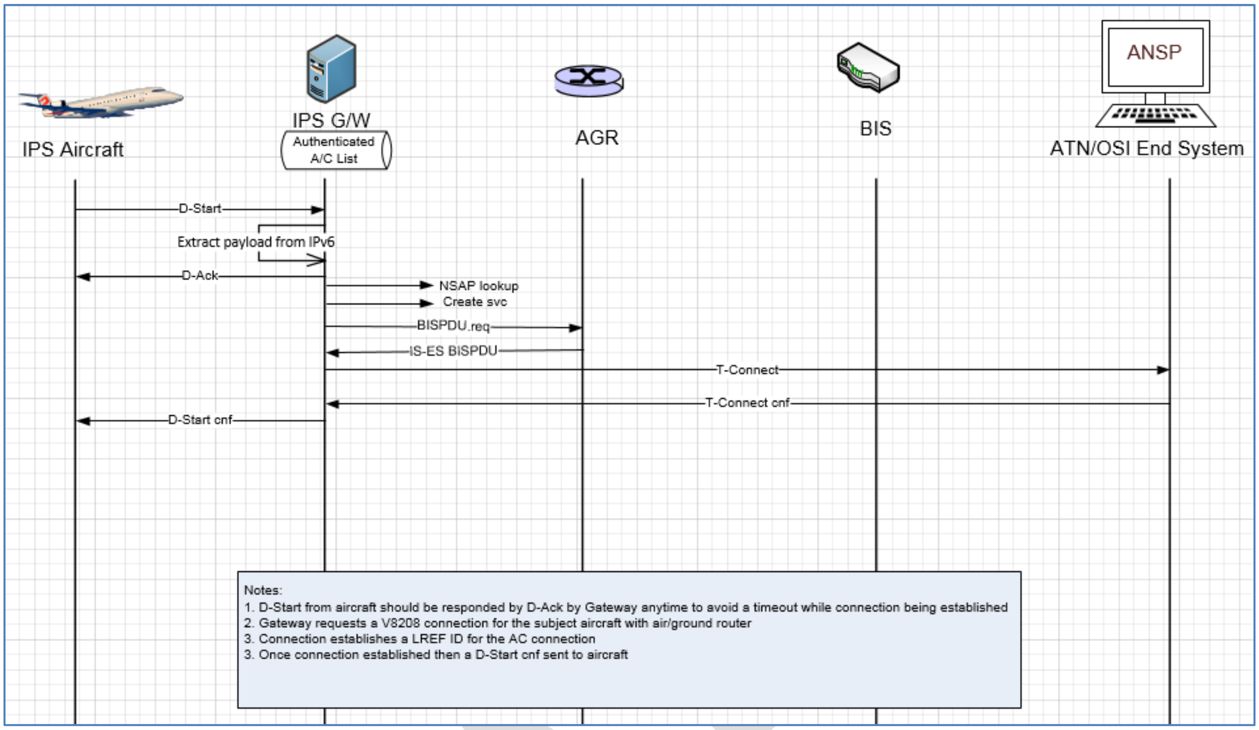


Figure 6-49 - D-Start scenario with ATN/OSI End System

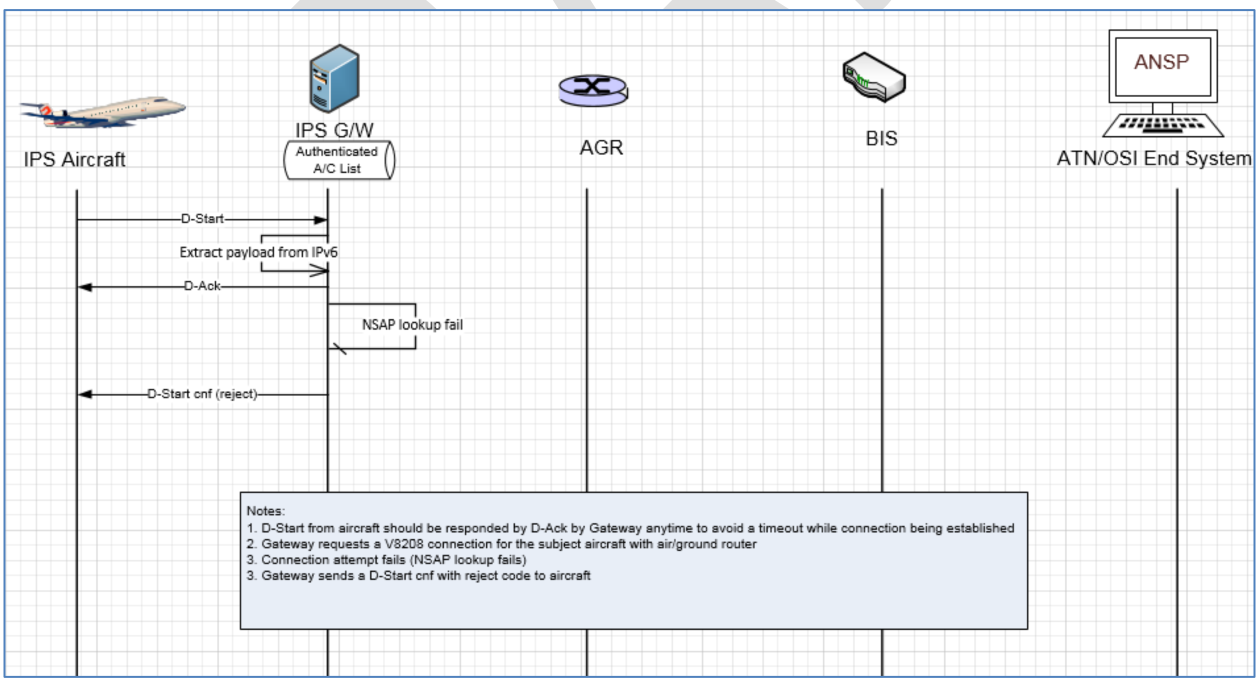


Figure 6-50 - D-Start failure scenario with ATN/OSI End System

6.4.4.2 IPS Aircraft Initiated D-Data Message

The D-Data message is used to send ATN application data to an ATN/OSI End System. The type of data (CM, CPDLC or ADS-C) that is being sent is dependent on the port number.

Figure 6-51 shows an example of a single segment downlink intended for an ATN/OSI End System. The message is generated by the avionics and:

- received by multiple ground stations, message sent to IPS Gateway
- IPS Gateway de-duplicates
- IPS Gateway extracts payload from IPv6
- IPS Gateway expands compressed data
- IPS Gateway get LREF ID from established connection
- IPS Gateway builds the ATN/OSI message and puts it on the ATN/OSI network for delivery to the ATN/OSI End System
- IPS Gateway receives acknowledgement from ATN/OSI End System and based this an acknowledgement to the IPS Aircraft

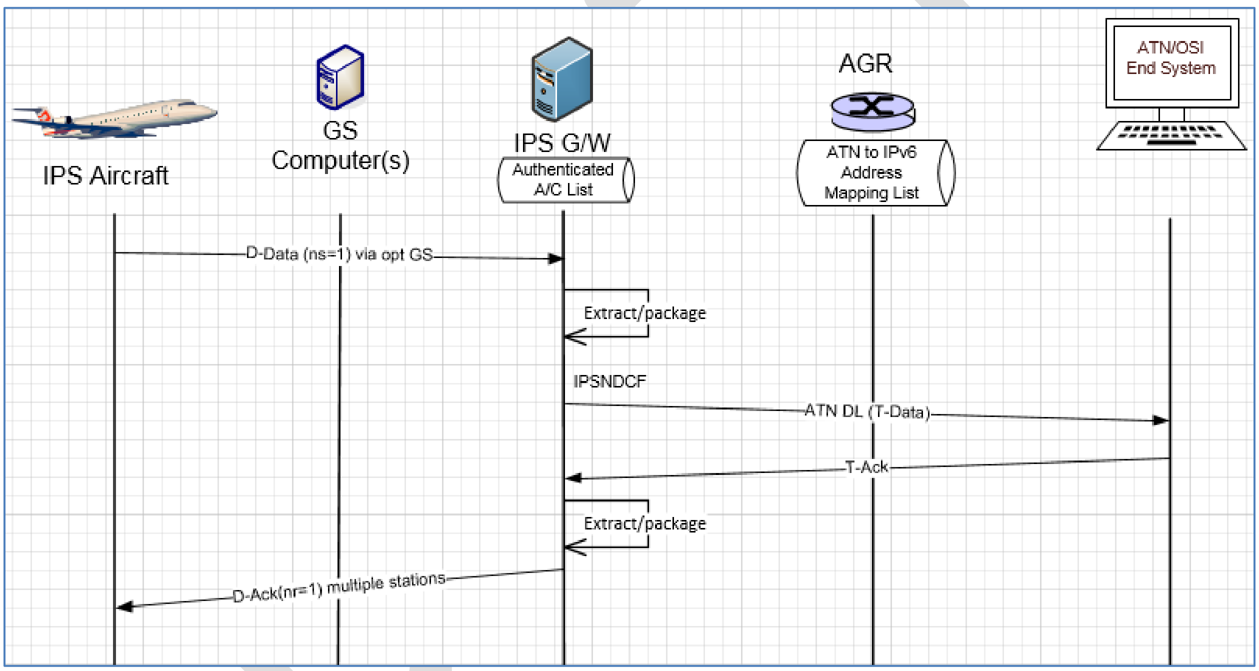


Figure 6-51 - 1 Segment downlink to ATN/OSI End System

6.4.5 ATN/OSI End System Initiated Uplink Messages

The initiation of an uplink by an ATN/OSI End System to an IPS Aircraft is unchanged from current operation and is effectively transparent to the ATN/OSI End System. The ATN/OSI End System will generate an ATN/OSI message for delivery to the aircraft. Based on the aircraft address, the ATN routers will route the message to the IPS Gateway. The IPS Gateway will package the message for delivery to the IPS Aircraft.

6.4.5.1 ATN/OSI End System Initiated Data Message

Figure 6-52 shows an example of A620 Host initiated uplink to an IPS Aircraft.

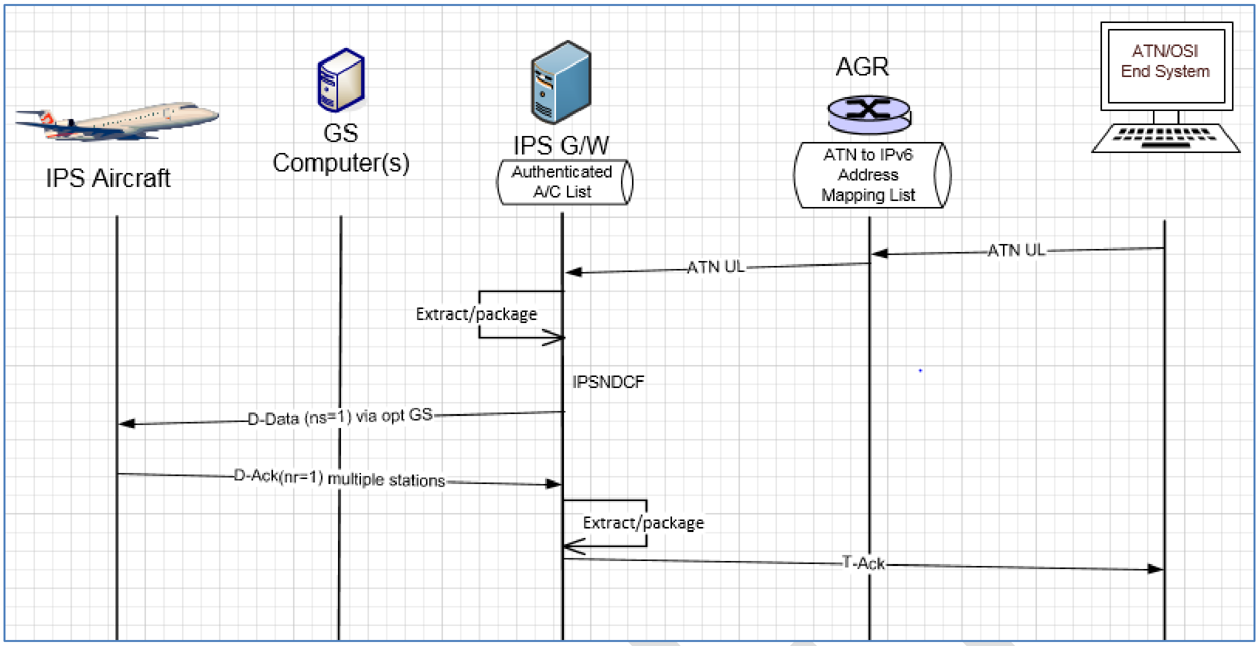


Figure 6-52 – ATN/OSI End System initiated uplink scenario

In this example:

- An ATN message is generated by a ATN/OSI End System and addressed for delivery to the aircraft via the ATN network
- Based on the address, the ATN ground router will send message to the IPS Gateway because the address is in a list of IPS aircraft
- IPS Gateway compresses the message, single segment is sufficient and packages in ATNPKT in IPv6 and sends to the optimal ground station
- the ground station puts it into a AVLC frame and adds IPI and sends to IPS Aircraft
- IPS Aircraft generates an acknowledgement
- IPS Gateway sends acknowledgement to the ATN/OSI End System

6.5 IPS Mobility

IPS mobility will be primarily handled through IPS Gateway internetworking. Each IPS aircraft will receive a stable IPv6 Mobile Network Prefix (MNP) that that travels with the aircraft through all mobility events. The MNP will identify the mobility service provider (the 'home' IPS Gateway). The mobility concept is consistent with IPv6 mobility defined in RFC 6275. The IPS mobility concept is consistent with the multilink concept. The IPS gateway supports multilink, the IPS gateway will use all IPS media available, and prioritizing based on airline or ANSP preference (usually cost-based). The IPS gateway will interconnect with other CSPs. The IPS gateway can also translate an IP message to ARINC 620 and send it to the legacy ACARS message processing system and for uplinking on ACARS if the aircraft has no IPS access (i.e. non-SATCOM equipped flying in non-IPS region).

The IPS Gateway internetworking is based on the trusted companion service provider model. A primary service provider will have a trusted relationship (contractual relationship and exchange of public CA certificates). An airline will choose which trusted companions their aircraft can roam onto. Figure 6-53 shows the concept of the trusted companions using a key trust tree.

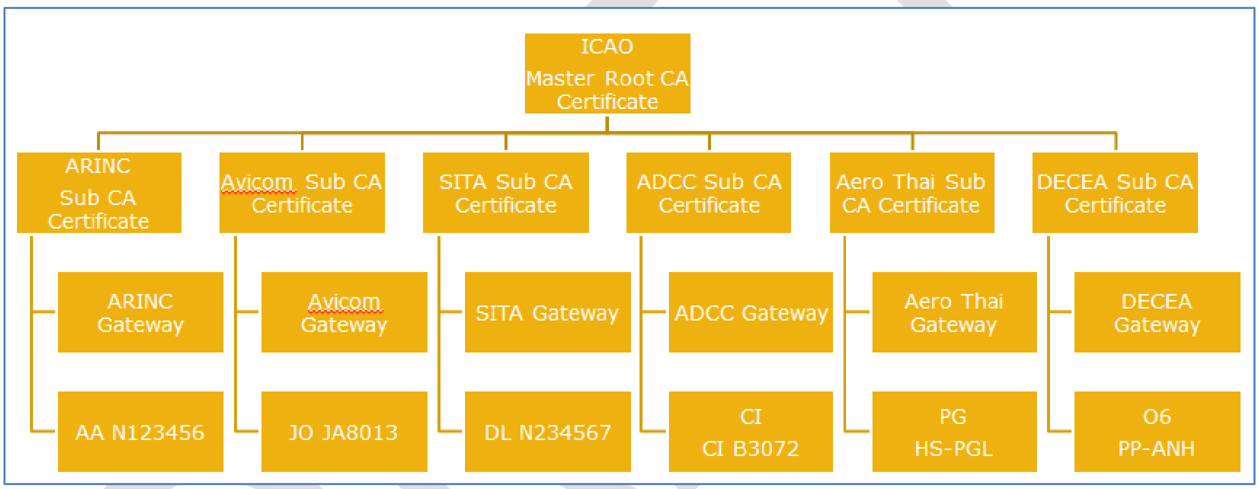


Figure 6-53 – Key Trust Tree

The IPS aircraft, when out of its home IPS Gateway region, will be able to communicate through a local IPS Gateway. The IPS aircraft will hear GSIFs from the local IPS Gateway service provider and initiate authentication. The basic concept is illustrated in Figure 6-54, which shows an IPS aircraft hearing a GSIF from a local IPS Gateway, authenticating with the local IPS Gateway. The local IPS Gateway will provide the route information (binding update) to the home IPS Gateway. The home IPS Gateway will use this information to route messages for the aircraft to the local IPS Gateway. If the aircraft leaves the local IPS Gateway coverage area, the local IPS Gateway will notify the home IPS Gateway that it no longer has the aircraft (a binding update with lifetime set to 0).

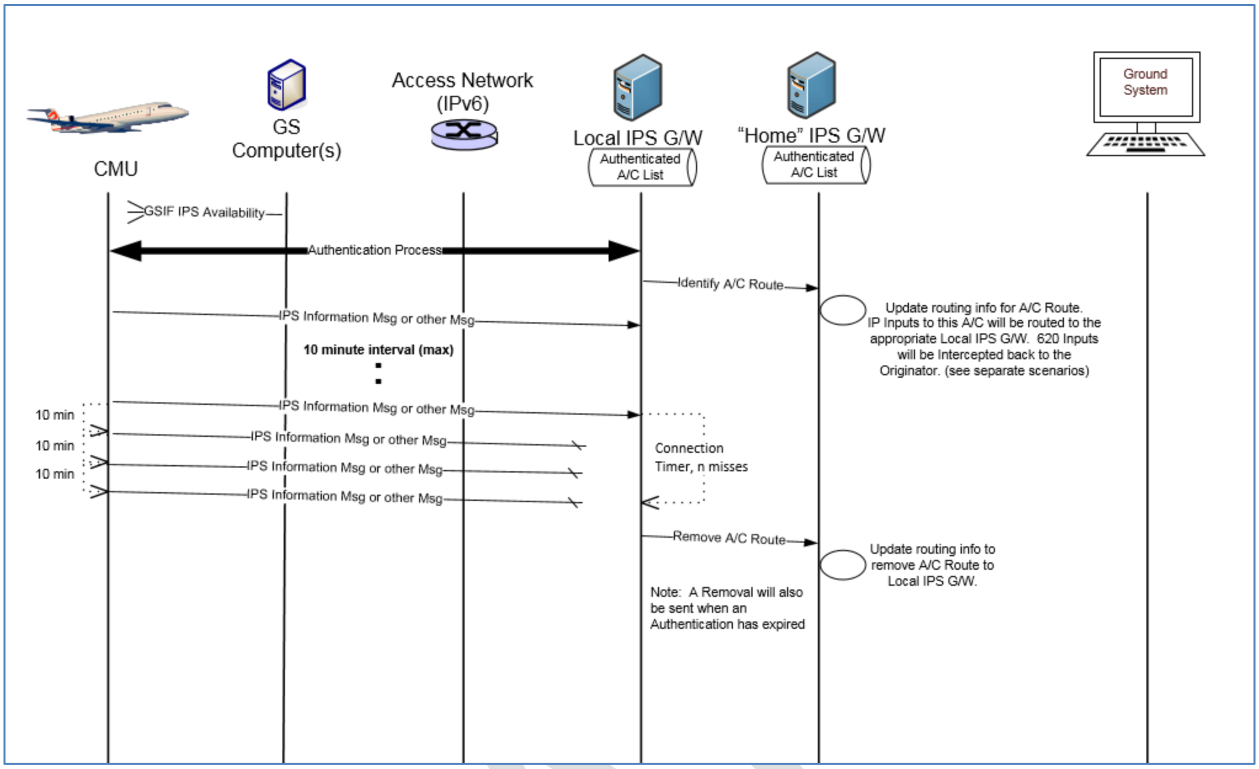


Figure 6-54 – Mobility scenario

With the home IPS Gateway knowing the routing to an IPS aircraft, the scenario in Figure 6-55 shows an example of how messages would be delivered from an IPS Ground System to an IPS aircraft:

- The home IPS Gateway receives an IPS message from an IPS Ground System destined for an IPS aircraft. The home IPS Gateway knows the routing to the aircraft through a local IPS Gateway.
- The home IPS Gateway encapsulates the message to the local IPS Gateway
- The local IPS Gateway strips the encapsulation and send the IPS message to the aircraft through the preferred media
- The downlink response from the IPS aircraft goes to the local IPS Gateway
- The local IPS Gateway routes the message directly to the IPS Ground System

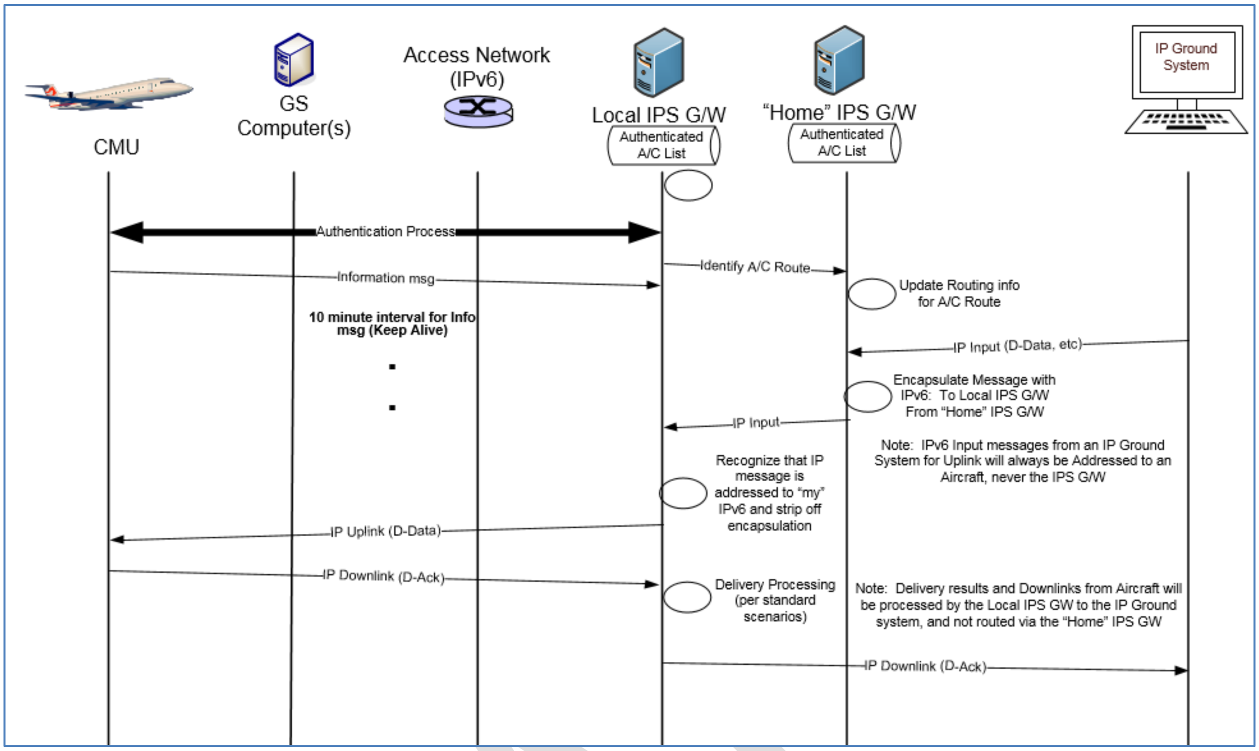


Figure 6-55 – Mobility scenario – IPS Ground System

The scenario in Figure 6-56 shows an example of how messages would be delivered from a 620 Host facility to an IPS aircraft:

- A620 message is generated by a A620 Host and sent to the DSP for delivery to aircraft
- Functionality within the DSP network determines the message is destined for a flight that is in the IPS A/C list and routes it to the IPS Gateway
- The home IPS Gateway receives the 620 input knows the routing to the aircraft is through a local IPS Gateway.
- The home IPS Gateway encapsulates the message to the local IPS Gateway
- The local IPS Gateway strips the encapsulation, converts the 620 message to an IPS message and send the IPS message to the aircraft through the preferred media
- The downlink response from the IPS aircraft goes to the local IPS Gateway
- The local IPS Gateway generates Message Assurance (if requested) and routes the 620 MAS message directly to the 620 Host

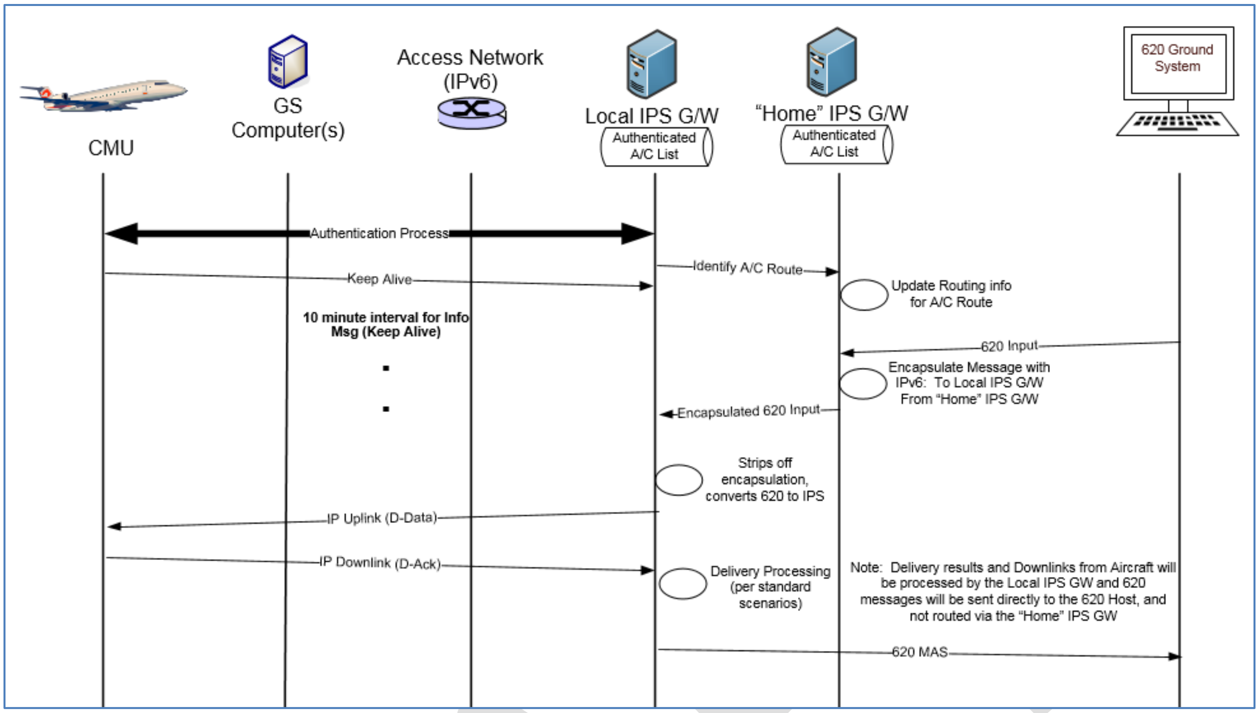


Figure 6-56 – Mobility Scenario – 620 Host

The scenario in Figure 6-57 shows an example of how messages would be delivered from a ATN/OSI facility to an IPS aircraft:

- ATN/OSI message is generated by a ATN/OSI End System and addressed for delivery to the aircraft (NSAP address) via the ATN network
- Based on the address, the ATN ground router will send message to the IPS Gateway because the address is in a list of IPS aircraft
- The home IPS Gateway receives the ATN/OSI input, knows the routing to the aircraft is through a local IPS Gateway.
- IPS Gateway extract the message data and packages in ATNPKT in IPv6
- The home IPS Gateway encapsulates the message and sends to the local IPS Gateway
- The local IPS Gateway strips the encapsulation and send the IPS message to the aircraft through the preferred media
- IPS Aircraft generates an acknowledgement which goes to the local IPS Gateway
- The local IPS Gateway encapsulates the acknowledgement and sends to the home IPS Gateway
- The home IPS Gateway strips the encapsulation, extracts data, checks connection (gets LREF) to ATN/OSI end system, generates ATN/OSI message (T-Ack) and send to the ATN/OSI end system.

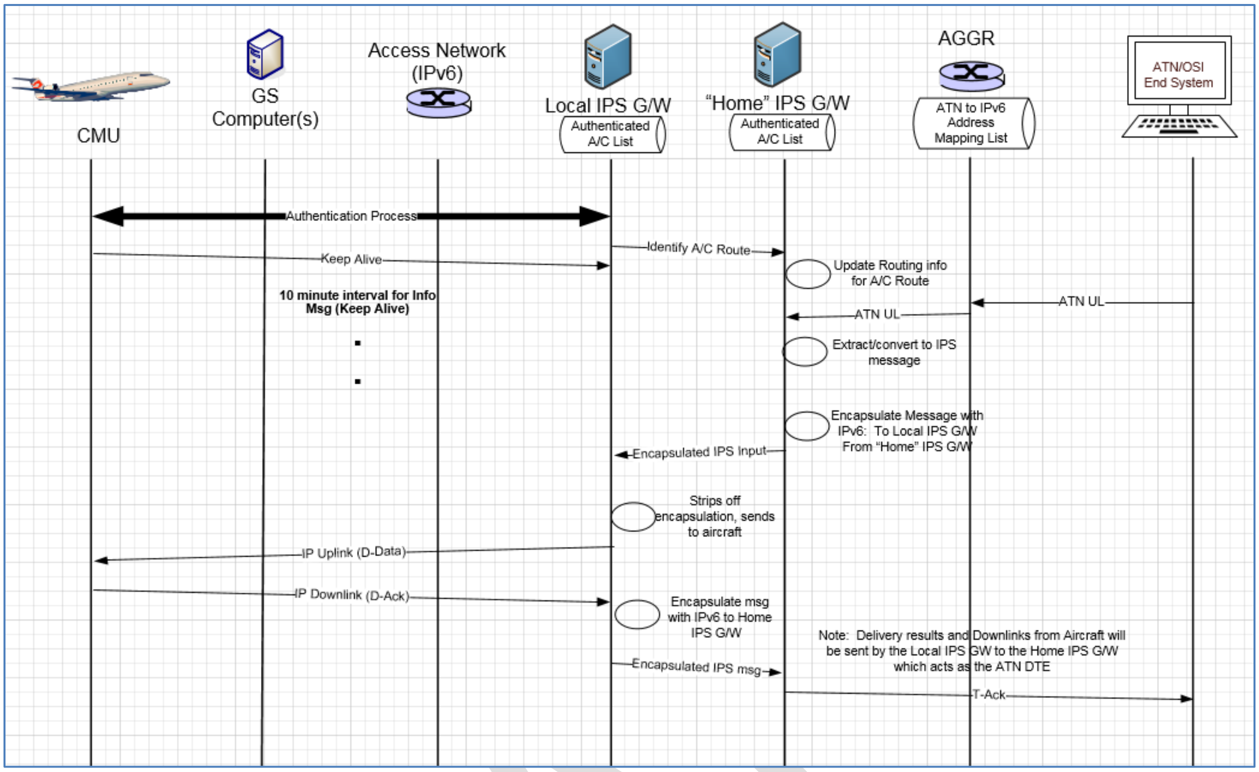


Figure 6-57 – Mobility Scenario – ATN/OSI End System

6.6 Performance Requirements

The IPS Gateway will need to have the capacity to support all aircraft that the DSP is supporting.
content to be developed – the following table may be taken into consideration

Performance Parameter	ATN B1 ED120 SPR Standard published Based on Eurocontrol Generic ACSP Requirements doc.	ATN B2 ED228 SPR Standard published Based on most stringent RCP130/RSP160	ATN B3 SESAR 15.2.4 predicted (no standards started) Based on most stringent RCP60/RSP60
Transaction Time One way (sec)	4 - 95% of messages 12 – 99.9% of messages	5 - 95% of messages 12– 99.9% of messages	2 - 95% of messages 5 – 99.9% of messages
Transaction Time Two way (sec)		10 - 95% of messages 18– 99.9% of messages	4 - 95% of messages 8 – 99.9% of messages
Availability -CSP	0.999	0.9995	0.999995 (maybe reduced by multi-link)
Availability - Aircraft		0.99	0.999
Integrity	$1-10^{-5}$	Not specified Must be good enough to meet RCP/RSP	Not specified Must be good enough to meet RCP/RSP

7 Appendix A - Ground Station Requirements for IPS

7.1 GS Uplink Requirements

7.1.1 GSIF For IPS

Support for IPv6 will be indicated in the GSIF by incorporating two additional parameters:

- the UI frames support parameter
- the IPS availability parameter

Both of these parameters need to be included in the GSIF for IPS operation.

7.1.1.1 UI Frames Support Parameter

This parameter indicates whether the ground station supports exchanging data (AOA packets, VDL 8208 packets, and/or VDL IPS packets) using UI frames. It shall be encoded as shown in Table 7-1 and Table 7-2.

Parameter ID	0	0	0	0	0	1	1	1
Parameter length	n_8	n_7	n_6	n_5	n_4	n_3	n_2	n_1
Parameter value	0	0	0	0	0	u_i	u_8	u_a

Table 7-1 - UI Frames Support Parameter Format

Bit	Name	Value	Description
1	u_a	$u_a = 0$	AOA packets in UI frames not supported and/or requested
		$u_a = 1$	AOA packets in UI frames supported and/or requested
2	u_8	$u_8 = 0$	VDL 8208 packets in UI frames not supported and/or requested
		$u_8 = 1$	VDL 8208 packets in UI frames not supported and/or requested
3	u_i	$u_i = 0$	VDL IP packets in UI frames not supported and/or requested
		$u_i = 1$	VDL IP packets in UI frames supported and/or requested
4	Reserved	0	Reserved for future use
5	Reserved	0	Reserved for future use
6	Reserved	0	Reserved for future use
7	Reserved	0	Reserved for future use
8	Reserved	0	Reserved for future use

Table 7-2- UI Frames Support Parameter Values

7.1.1.2 IPS Availability Parameter

This parameter indicates IPS availability and provides the IPv6 address of the IPS Gateway / Router. It shall be encoded as shown in Table 7-3.

Parameter ID	0	0	0	0	1	0	0	0
Parameter length	0	0	0	1	0	0	0	0
Parameter value	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1
Parameter value	a_{16}	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9
Parameter value	a_{24}	a_{23}	a_{22}	a_{21}	a_{20}	a_{19}	a_{18}	a_{17}
. . . .								
Parameter value	a_{120}	a_{119}	a_{118}	a_{117}	a_{116}	a_{115}	a_{114}	a_{113}
Parameter value	a_{128}	a_{127}	a_{126}	a_{125}	a_{124}	a_{123}	a_{122}	a_{121}

Table 7-3 – IPS Availability Parameter Format

The parameter value contains the 128 bit address of the IPS Gateway associated with this ground station.

7.1.2 AVLC Downlink Destination Address for IPS

Destination address for the AVLC ground station from the aircraft for IPS is described in Table 7-4.

Bit	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Field	Type			SPC				RID		RaID		CID (C Identifier)								DID (D Identifier)							
Value	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Ground Station Specific Address, Allocated and Assigned by an ICAO-Delegated Organization = 101			Service Provider Code ARINC= 0001						Radio																	

Table 7-4 – AVLC downlink destination address

The address is a 24-bit address and corresponds to the allocation of ground station addresses defined in ARINC 631. The following table shows the assignments:

Organization	Prefix
Reserved	0000 ---- ---- ---- ---- ----
ARINC	0001 ---- ---- ---- ---- ----
SITA	0010 ---- ---- ---- ---- ----
Unassigned	0011 ---- ---- ---- ---- ----
Unassigned	0100 through 1101
Unassigned	1110 ---- ---- ---- ---- ----
AVICOM Japan	1111 0000 00-- ---- ---- ----
Brazil	1111 0000 01-- ---- ---- ----
Unassigned	1111 0000 10-- ---- ---- ----
China	1111 0000 11-- ---- ---- ----
Honeywell	1111 0001 00-- ---- ---- ----
Unassigned	1111 0001 01-- ---- ---- ----
Unassigned	1111 0001 10-- ---- ---- ----
AEROTHAI	1111 0001 11-- ---- ---- ----
Test DSP	1111 0010 00-- ---- ---- ----
Jetstar	1111 0010 01-- ---- ---- ----

Russia	1111 0010 10-- ---- ---- ----
Unassigned	1111 0010 11-- ---- ---- ----
Unassigned	1111 0011 00 through 1111 1111 10
Reserved	1111 1111 11-- ---- ---- ----

Table 7-5 - VDLM2 Ground Station DSP Address Assignments

The remaining bits after the prefix are set to all 1’s to indicate broadcast.

Note: ARINC Asian partners Aerothai, China, and Korea are currently using 0001 prefix for the ground station addresses and will need to be upgraded for the ARINC 631 defined mask as a part of the ground station update for IPS.

7.1.3 Single attempt on uplinks to IPS, no retry

The ground station will only make a single delivery attempt for IPS messages as the retry logic is controlled by the IPS Gateway

7.2 GS Downlink Requirements

7.2.1 Process Broadcast Downlinks

The downlink UI frame will use the ground station broadcast address of a particular DSP as the destination address. The ground stations will have to process all broadcast UI frames.

7.2.2 Route to IPS Gateway based on IPI indicating IPS

The ground station will route broadcast UI frames based on the IPI. If the IPI indicates IPS then the data is sent to the IPS Gateway.