AEEC Internet Protocol Suite (IPS) for Safety Services End to End Approach

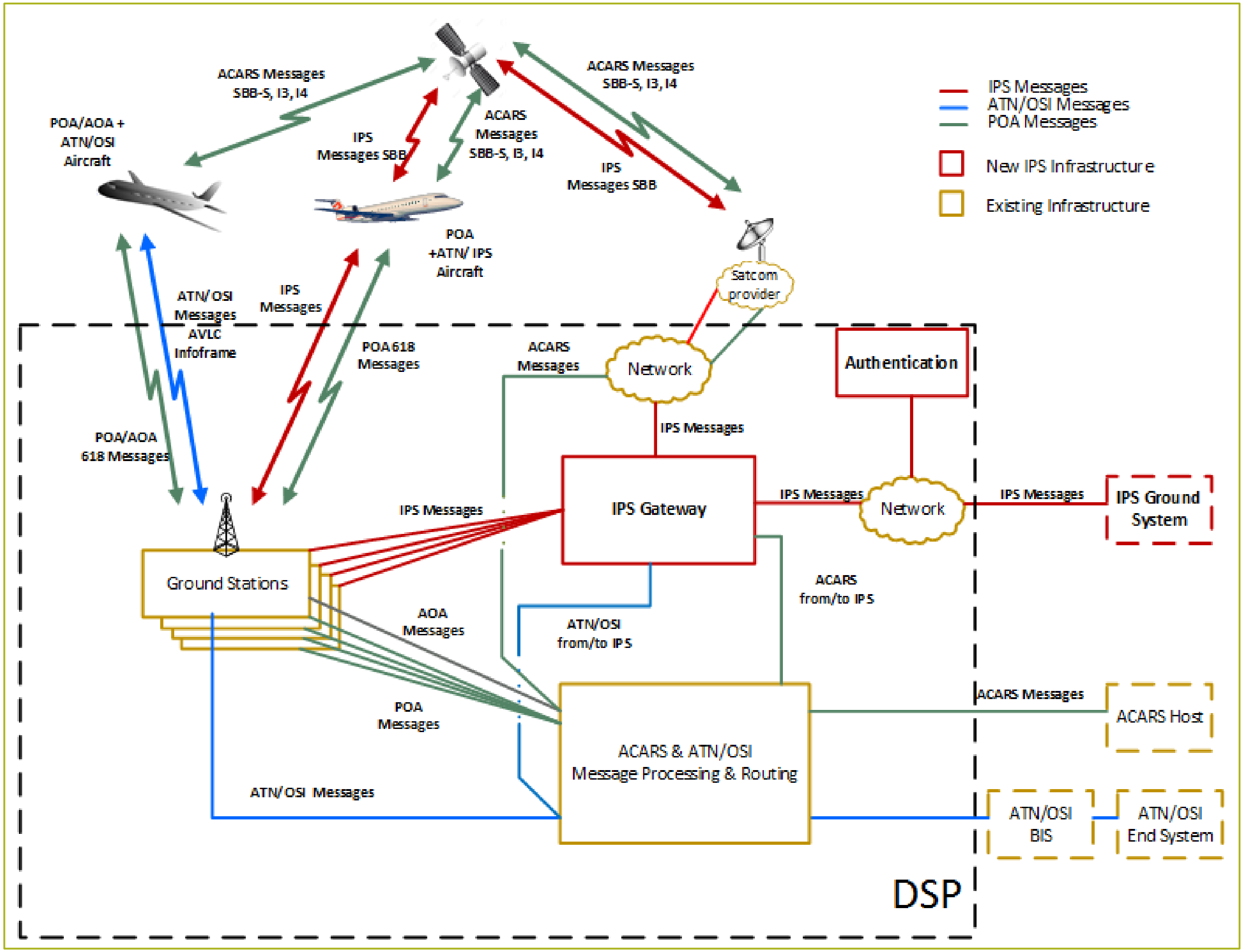
Jonathan Graefe
Ron Dlouhy
Mark Layton
Madhu Niraula
Mark Stevenson

January, 2018

Discussion

- IPS End to End Architecture
- IPS Ground Message Gateway
- Addressing and IPS Domain
- High Level Network Data Flow
- DOC 9896 ATNPKT protocol overview for IPS safety service applications
- IPv6, UDP, and service and port definitions
- Authentication and Key Management
- Ground IPv6 address lookup and retrieval
- IPS Information message
- IPS End to End message Encapsulation
- IPS over VDL M2
- Example Scenarios
- Quick Demo / Q & A

IPS End to End Architecture



IPS Ground Message Gateway

Functions of the IPS Message Gateway:

- Authentication
  - Initiate authentication
  - Maintain list of currently authenticated aircraft
  - Provide mobility and share aircraft info with other providers
- Compression/decompression
- Address lookup service
- Support legacy A620 ground hosts by converting IP message to/from A620 for communication (FANS 1/A, airline host)
  - Manage ACK/retry across protocol conversion
  - Allows use of existing A620 customer-initiated message copy and routing
- Support OSI/ATN ANSPs by converting IPS message to/from ATN/OSI for delivery through the existing ATN/OSI ground system
  - Manage ACK/retry across protocol conversion
  - ATN/OSI link management
- Packet fragmentation management

IPS Ground Message Gateway

- As IPS is rolled out, there will be many years where IPS and legacy aircraft and ground systems will co-exist.
  - ATN/OSI will remain active
- Propose DSP-operated ground IPS Gateways to provide interoperability between FANS, ATN/OSI, and IPS aircraft, and ATN/OSI, 620, and IPS ground end systems.
- Provides seamless, global datalink harmonization – <u>any aircraft can fly anywhere</u>

IPS Ground Message Gateway

IPS – IPS

- ATN/IPS Gateway will primarily be a pass through
- ATN/IPS Gateway will perform air-ground segmentation

IPS – A620 and FANS - IPS

- ATN/IPS Gateway will perform message conversion
- Packet format is tailored to carry FANS/ACARS/620 traffic
- Custom use of selected ATNPKT fields
- ATN/IPS Gateway will perform air-ground segmentation and compression

IPS – ATN/OSI

- ATN/IPS Gateway will be a ATN/OSI DTE for connection with either legacy ATN/OSI ground end system or ATN/OSI aircraft
- ATN/IPS Gateway will perform message conversion
- ATN/IPS Gateway will perform air-ground segmentation and compression

IPS Message Gateway - Sub-Network Architectural Considerations

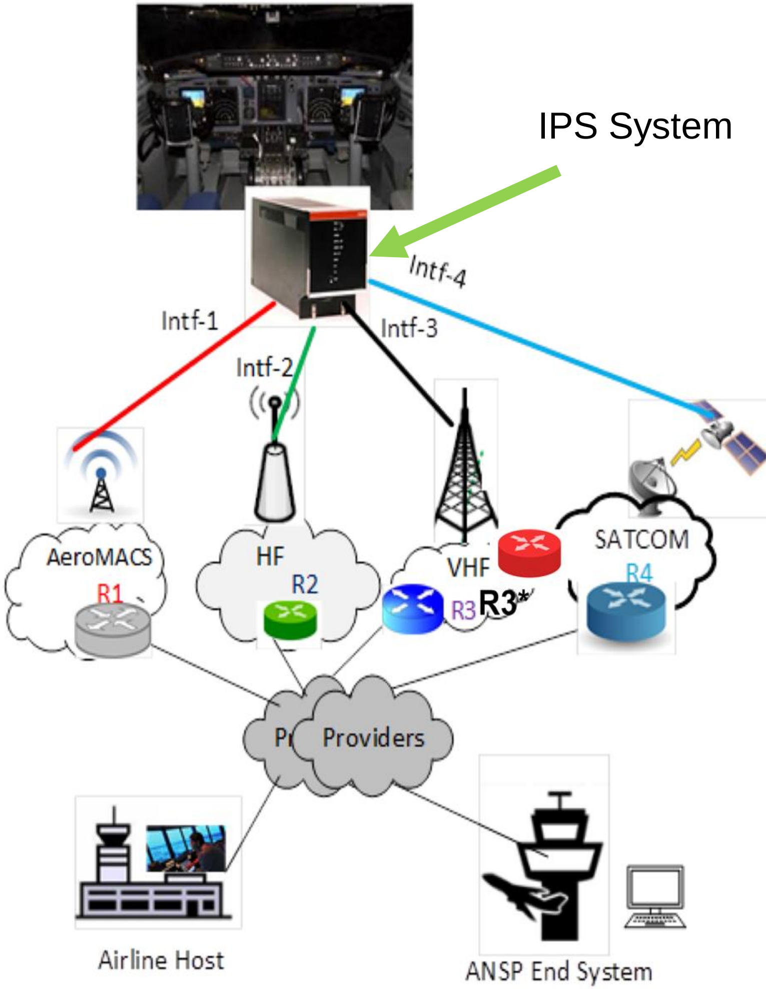
- Support VDL M2, SDU and other air to ground media (media agnostic)
- Fully integrated with OSI and ACARS protocol
- Supports existing applications over IPS
- Smart routing optimization
- Applications will utilize appropriate transport protocol (TCP when needed, UDP for maximum bandwidth utilization)

Addressing and IPS Domain

Avionics IPv6 IPS Network Domain (1/2)

Multihoming with Multiple Addresses

- Each attached interface is assigned a different set of prefixes (IPv6 addresses)
- Each interface has multiple addresses assigned(Multiple addresses per interface)
- Per RFCs, IPv6 hosts are required to be able to handle multiple addresses per interface
- Each interface has a DSP assigned and media specific globally routable IPv6 prefix. SLAAC (RFC 4862) will be used to auto configure the address at boot time or each time the point of attachment changes.
- Each aircraft will have a nomadic fixed address assigned, by ICAO, to the aircraft for all interfaces.
- Each interface will have a related default gateway router

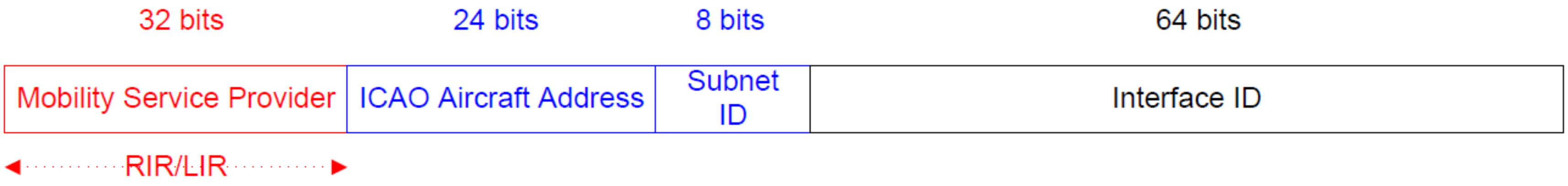


Intf – n (interface 1 through n)
Rn – Default router for the specific access network

CSP specific IPS network Addressing

Aircraft Addressing

- IPS nodes use globally scoped IPv6 addresses when communicating over the ATN/IPS.
- Communication service provider will mange their own address their Administrative Domains obtains IPv6 address prefix assignments from their Local Internet Registry (LIR) or Regional Internet Registry (RIR).
- Aircraft will discover the communication service provider (CSP) prefix based on the associated media and configure CSP specific address for the aircraft using the following format.
- CSP will implement IP Version 6 Addressing Architecture as specified in RFC 4291.
  - Aircraft will use globally scoped (fixed nomadic) IPv6 addresses when communicating over the ATN/IPS.
- Use of 64 bit prefixes and 64 bit IDs (for Aircraft use both 24 bit address), Complementary, for IPS ground-ground communications
- CSP prefix may or may not be 32 bits in which case this need to be changed.



32 bits	24 bits	8 bits	64 bits
Mobility Service Provider	ICAO Aircraft Address	Subnet ID	Interface ID

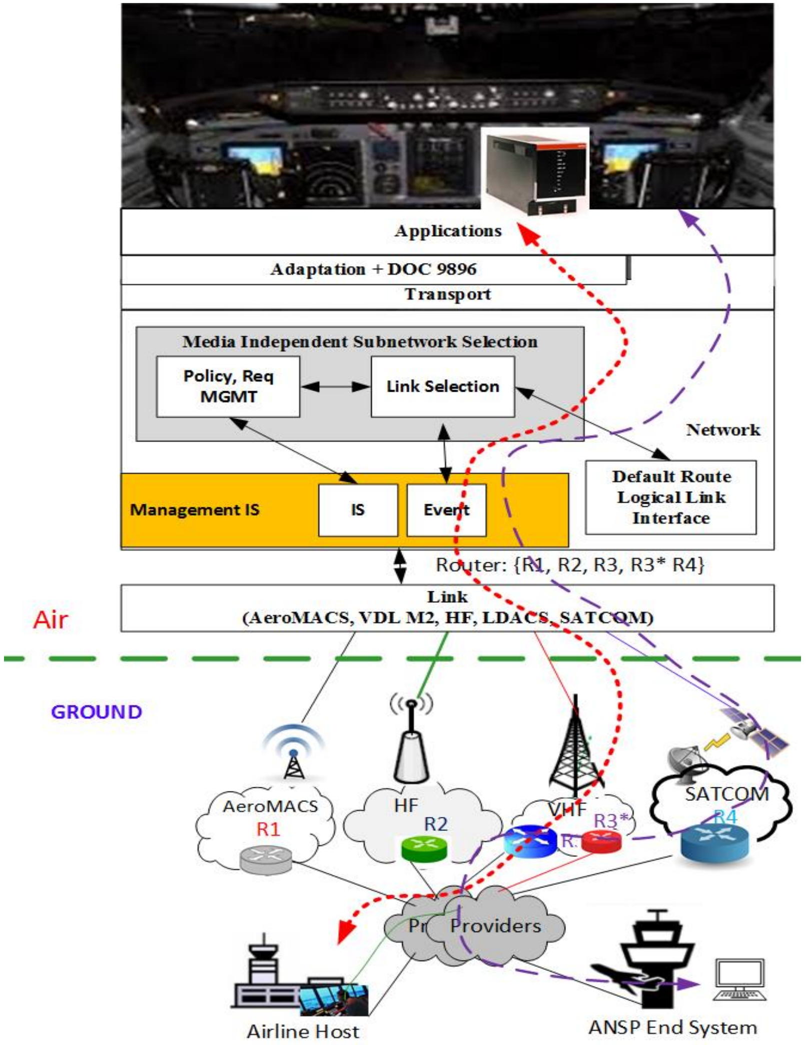
◄ RIR/LIR ►

The above scheme has the advantage to incorporate the ICAO 24 bits Aircraft Address. The /32 IPv6 address prefix assignment is under CSP responsibility that needs to request it from their Local Internet Registry (LIR) or Regional Internet Registry (RIR). Such approach implies allocation processes under well-established frameworks managed by RIRs.

Avionics IPv6 IPS Network Domain (2/2)

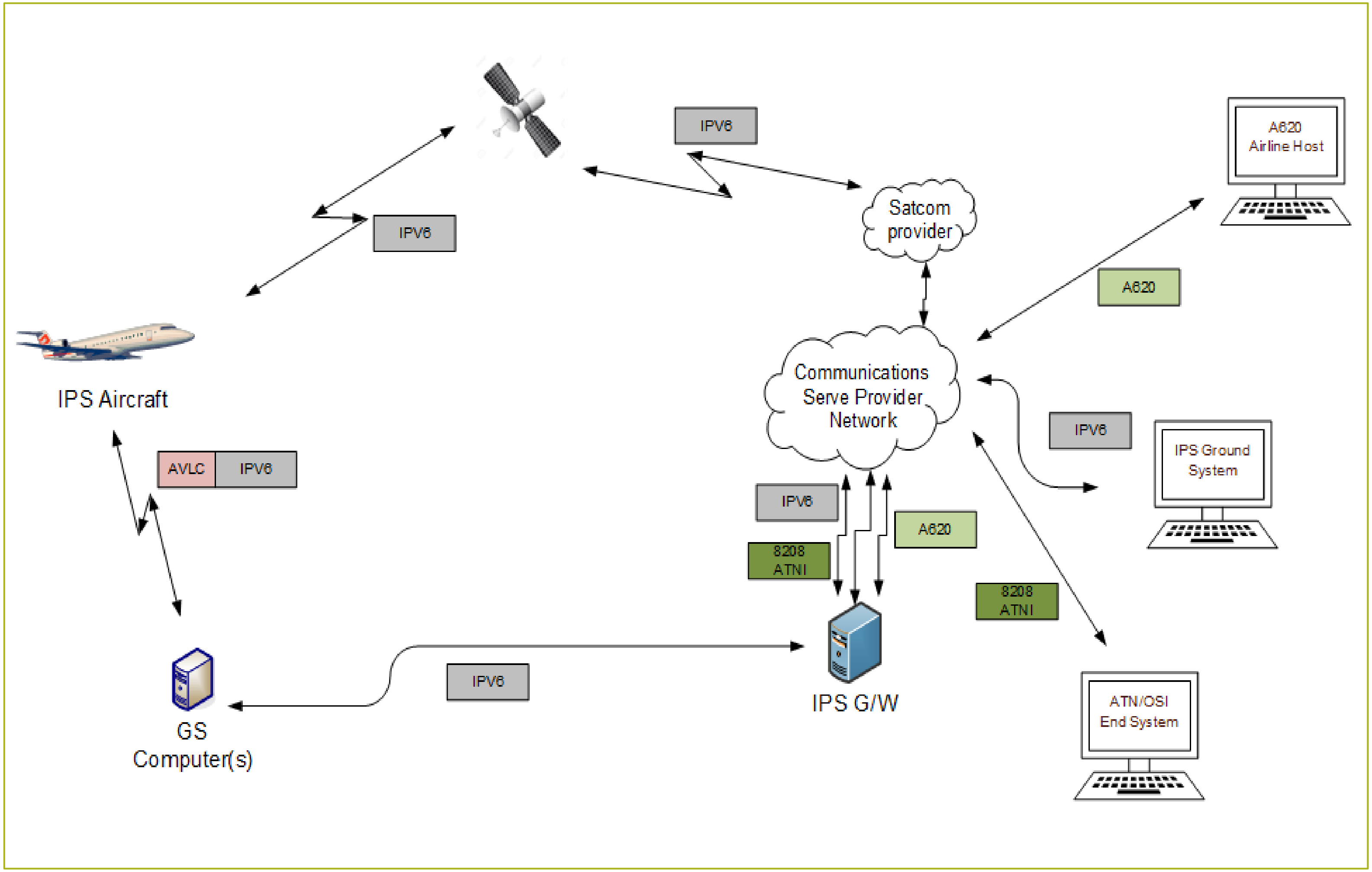
Multihoming with Multiple Addresses

- Intf: Interface, R: Router on the ground for each access network which is the default router for the avionics hosts for that particular interface
- Behind one access network, avionics may have multiple networks (VHF radio can reach multiple CSP network with different router and prefix, this can be resolved giving each CSP dedicated frequency)
- All communication from aircraft that is routed globally will use aircraft Nomadic fixed address as source address
- All traffic target to aircraft should use aircraft nomadic fixed address as destination address
- Each DSP/CSP announces a default route, meaning that they are willing to accept packets destined for the Aviation Intranet
- Avionics will select default route to select the appropriate media that meet cost, performance, priority and preference



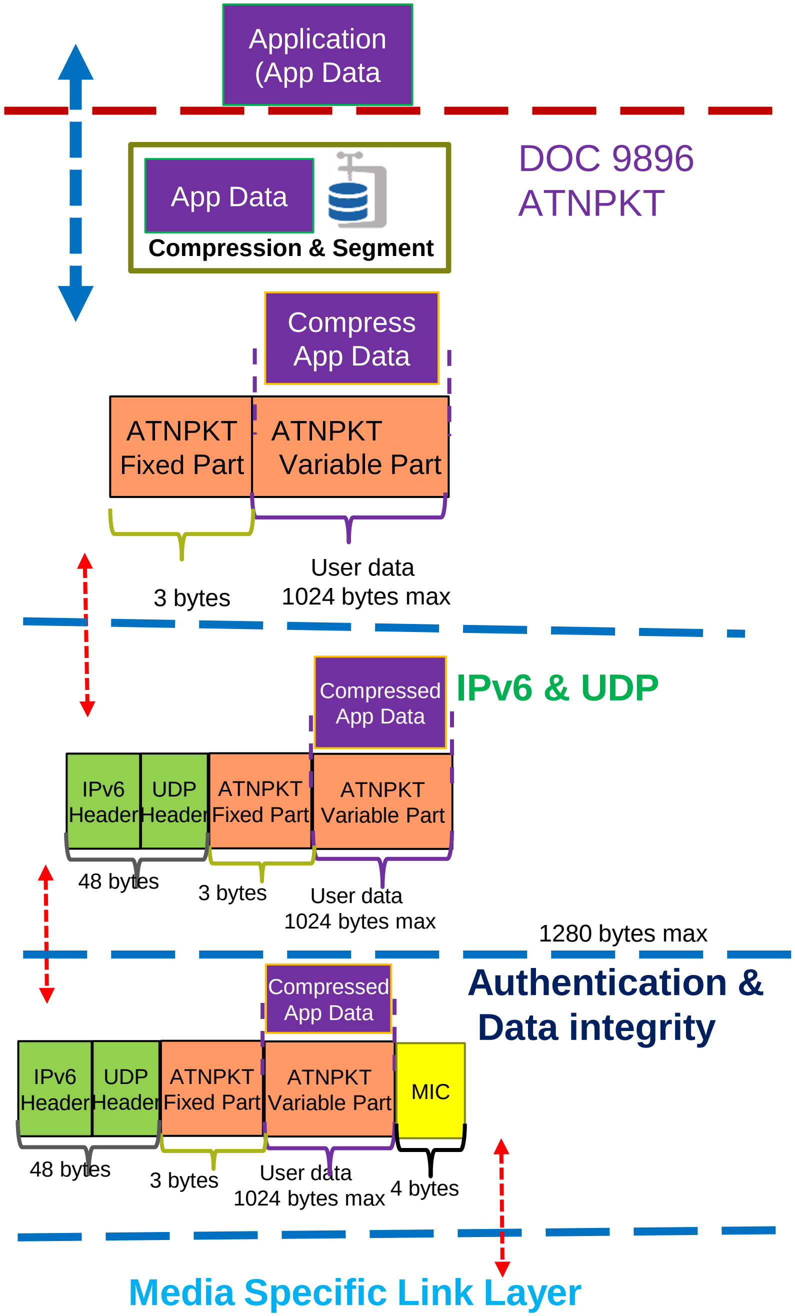
Traffic originated or destine to aircraft will use the aircraft nomadic IPv6 address as the source or destination IP address regardless of air to ground media. The avionics host follows the default gateway mechanism, which will choose the unify gateway among more than one default route (::/0).

IPS High Level Network Data Flow

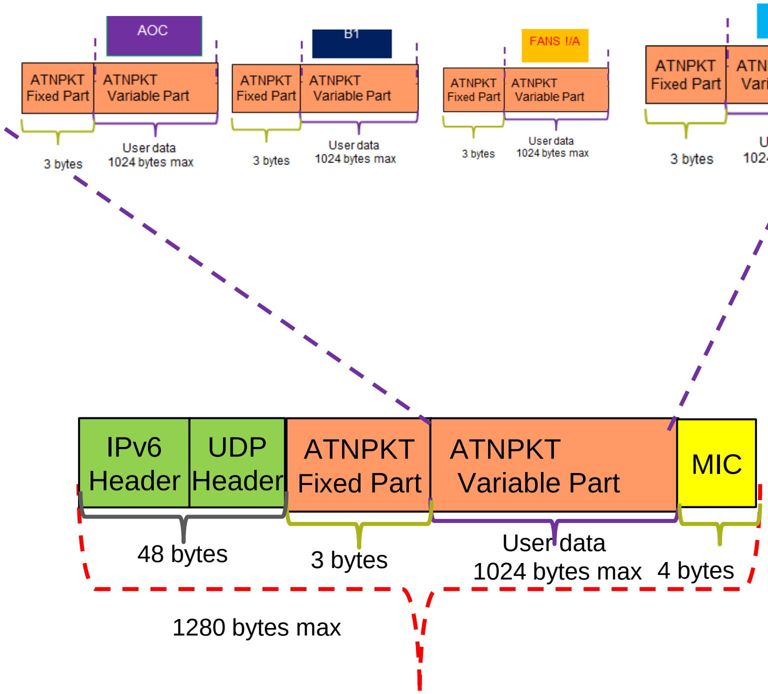


IPS Protocol Overview / ATNPKT

IPS Protocol Overview



- ATNPKT is used to convey information between air and ground peer.
- Per Doc. 9896, ATNPKT has a maximum user data size of 1024 bytes.
- User data exceeding this size will be fragmented in ATNPKT.

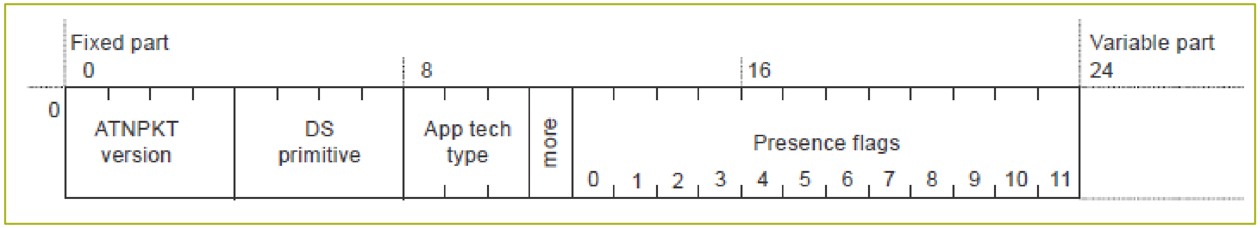


The IPv6 minimum MTU is 1280. IPv6 MTU will accommodate the ATNPKT.

ATNPKT Format

ATNPKT:

- The ATNPKT is defined in ICAO Doc. 9896
- ATNPKT it used to provide reliability for B1, B2, FANS and AOC data over AVLC
- The ATNPKT consists of a fixed header and a variable portion



ATNPKT Version

- 0 is used for the version

App Tech Type

- b000 – indicating ATN/IPS DS
- b001 – indicating AOC DS
- b011 – indicating FANS/IPS DS

More Bit

The more bit is used to indicate segmentation of the ATNPACKET

- 0 – Single segment or the last segment of a segmented message
- 1 - the rest or an intermediate segment of a segmented message
- More bit is always set to 0 for the Primitives 6,7,8,9

ATNPKT DS Primitives

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*

ATNPKT DS Primitive Use

- B1 and B2 all primitives except D-UNIT-DATA are being used
- FANS 1/A and AOC only D-DATA and D-ACK are being used

Presence Field Details (1/4)

Bit	Optional Field	Size (byte)*		Description	Notes
		Length	Value		
0	Source ID	N/A	2 bytes	DS connection identifier of the sender	1
1	Destination ID	N/A	2 bytes	DS connection identifier of the recipient	1
2	Sequence Numbers	N/A	1 byte	Sequence numbers (Ns, Nr). Sequence numbers can range from 0 to 15	
3	Inactivity Time	N/A	1 byte	Inactivity timer value of the sender (in minutes)	
4	Called Peer ID	1	3 to 8 bytes	Called peer ID (provided by the local DS-user)	1
5	Calling Peer ID	1	3 to 8 bytes	Calling peer ID (provided by the local DS-user)	1
6	Content Version	N/A	1 byte	Version of the application data carried	
7	Security Indicator	N/A	1 byte	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	1 Byte	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	1 Byte	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	1 Byte	Originator of the abort: 0 – user (default value) 1 – provider 2 … 255 – reserved	
11	User Data	2	0 to 1023 bytes	User data	

1 = This field has customized to encapsulate A620 data

* = when length is present it always precedes the value

Presence Field Details (2/4)

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. The Source ID is also present in the D-DATA primitive for A620 downlink data. The meaning of this 2 byte field is based on the type of A620 data:

AOC – Service point definition – Label
FANS1/A – Service point definition – MFI

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. The Destination ID is also present in the D-DATA primitive for A620 downlink data. The meaning of this 2 byte field is based on the type of A620 data:

AOC – sub service point definition – Sub label
FANS 1/A – first two character of IMI

Sequence Number

- 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
- N(S) – Sequence number of ATNPKT sent
- N(R) - next expected ATNPKT sequence number to be received
- Ack is performed for high water mark.

Sequence Number Format

4	3	2	1	4	3	2	1
N (S)				N (R)			

Presence Field Details (3/4)

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.

If the D-DATA primitive is for A620 FANS 1/A data, then this field is an 4 to 8 bytes mandatory field and the meaning of this field is defined to be the Center Name.

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 characters ICAO facility designation and have the format 24 to 64 bits.

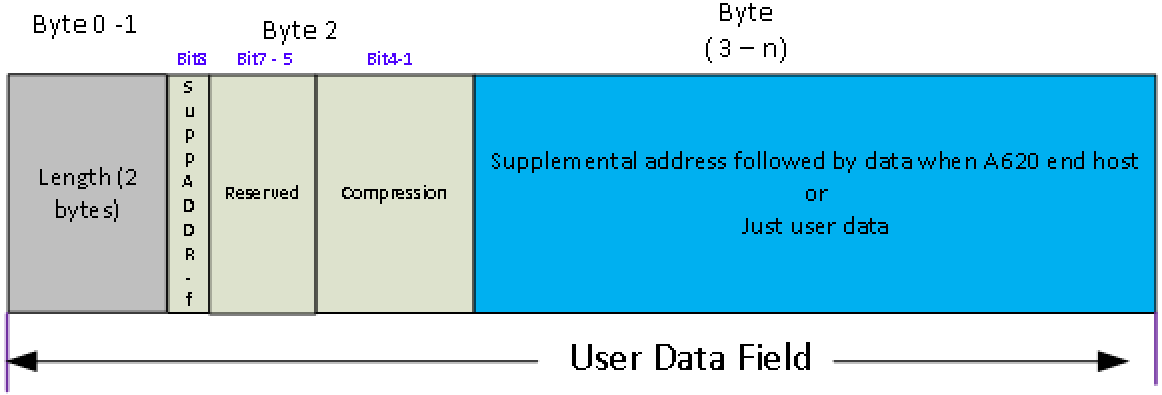
If the D-DATA primitive is for A620 data, then this field is up to 8 byte optional field and the meaning of this field is redefined to be the ICAO flight ID. This field will be populated by the aircraft whenever the flight ID has changed or the aircraft has re-authenticated.

Presence Field Details (4/4)

User Data

The user data field of the ATNPKT contains application data. The user data is variable size, 0 bytes to a maximum of 1023 bytes.

The first two bytes contain the user data length (in bits). Following the 2 bytes of the length there is a byte (compression byte) used to indicate whether the user data is compressed, the compression method, and whether any supplemental addresses are present (applicable only to 620 data).

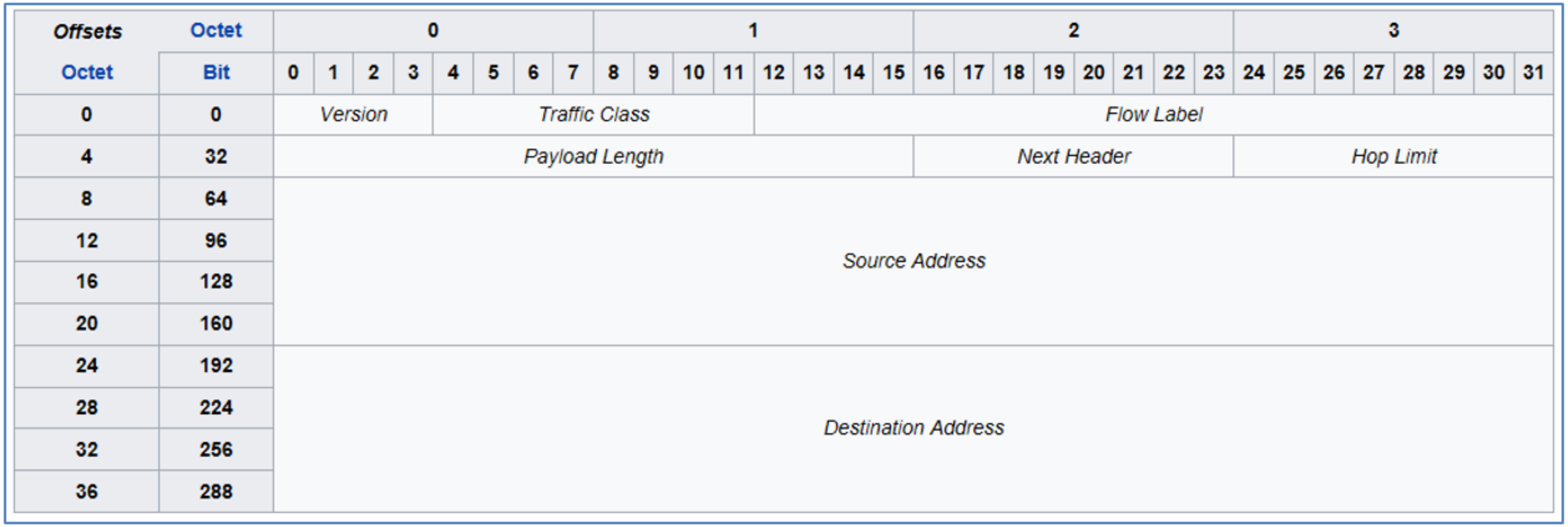


Bit	Meaning	Description
1 to 4	Compression Flag	0 - No compression 1 - indicates deflate compression 2-15 to be defined for future compression method to be used
8	Supplemental presence flag	One (1) indicates the presence of supplemental address data (only applicable to 620 data). If present, the supplemental addresses will follow the compression byte. Each address will be delineated by an underscore and the last addresses will be followed by a period (addr_addr_addr.)
5-7	Reserved	

IPv6, UDP and Ports

IPv6 Header Information

- Source IPv6 address will contain Aircraft Nomadic fixed address assigned by ICAO
- Destination IPv6 address will contain the ground system IPv6 address (DSP gateway for A620 Host End System or ATN OSI End System)
- The IPv6 base header is the first 40 bytes



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																																

IPv6 Header Format

TCP/UDP Service Name and Port Definition

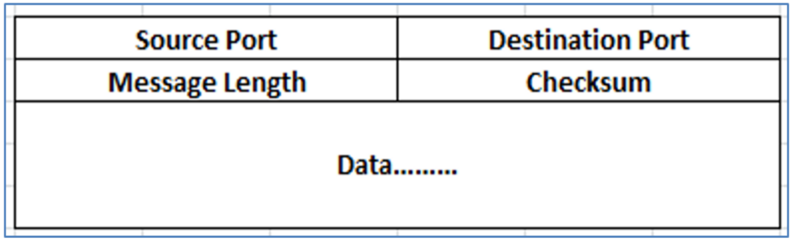
Service Name	Port	Notes	Avionics Configuration	Ground Configuration	Current IANA Status
Authentication / Management	5908		Client	Server	Need to register
AOC	5909	ARINC 620 data	Both	Both	Need to register
CM	5910	IP App	Both	Both	Registered
CPDLC	5911	IP App	Server	Client	Registered
ADS-C	5912	IP App	Server	Client	Registered
AFN	5915	ARINC 620 data	Both	Both	Need to register
FANS ADS-C	5916	ARINC 620 data	Server	Client	Need to register
FANS CPDLC	5909	ARINC 620 data	Server	Client	Need to register

- Port number defines the service access points
- DOC 9896 has some definition. Will need updates to cover missing applications
- All other ports are Native IP applications

UDP Header Information

UDP

- *Destination Port < Application specific port>*
- *Source Port <ANY if CMU is client>*
- For authentication, the key tag field value must be 0x0A. Prior to authentication, port 5908 will be the only open port
- *All traffic are dropped until authentication is done*



Source Port	Destination Port
Message Length	Checksum
Data.........	

UDP Packet

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:

UDP Destination Port 5908 Tag Field (First byte of Data)	Message
0x0A	Authentication
0x0B	IPS Information
0x0C	IP Lookup
0x30 – 0x3F	Key Management

Authentication and Key Management

Mutual Authentication

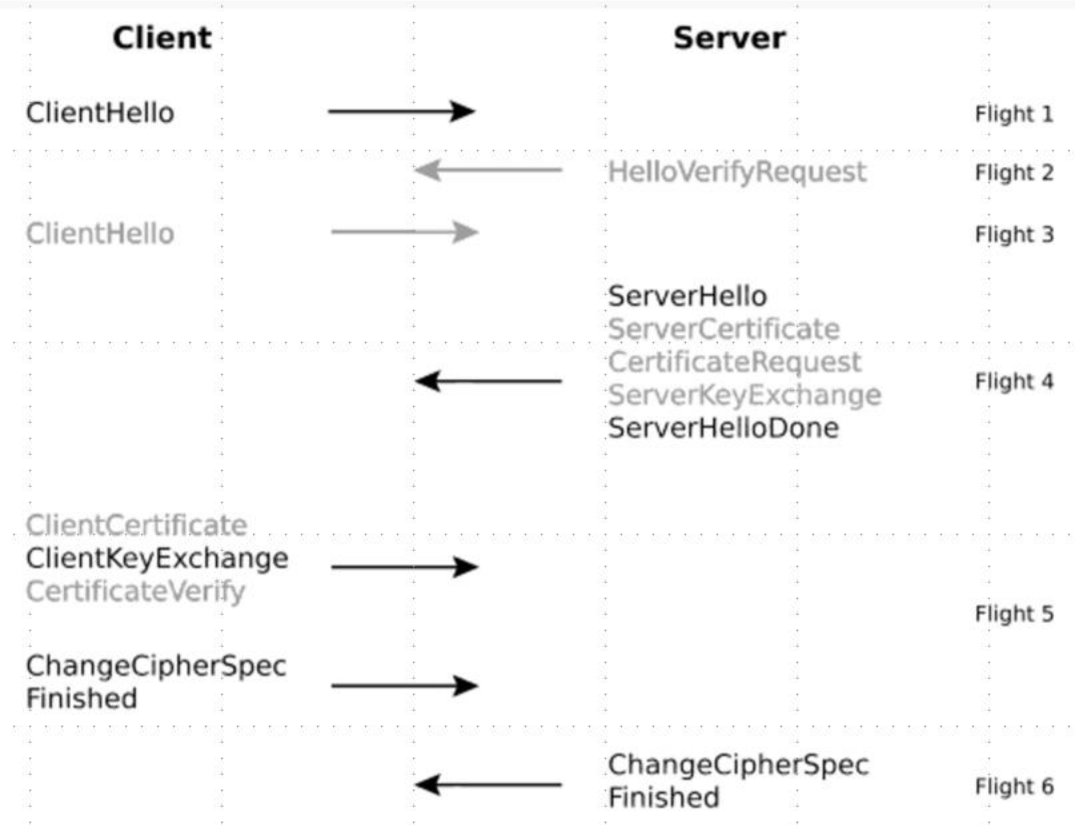
- Aircraft-initiated authentication
  - Each DSP is Authenticated by aircraft
  - DSP authenticates each aircraft
- The IPS Gateway and Aircraft authenticate each other using DTLS authentication process (using UDP port 5908 key selector 0x0A). Authentication remains valid for 8 hours or end-of-flight.
- The DTLS Protocol (RFC 6347) is used to authenticate the ground and aircraft, establish the session keys.
- Session keys is used to generate the Message Authentication Code (MIC) based on SHA384 crypto hash functions
- The message integrity check (MIC) is computed for each packet generated for a given subnetwork after authentication has been completed. For IPv6 networks, the MIC is computed for each IPv6 packet, for non-IP networks the MIC is computed for each subnetwork packet transmitted in order to secure the subnetwork.
- DTLS is an enhancement on TLS for secure UDP connections.
- If aircraft key compromised, aircraft will have a one-time-use back-up key that can be used to authenticated. Of course, after using back-up key, airline must data load new keys during or after flight.
- Elliptic curve cryptography (ECC) based public crypto systems
- Issue for Industry – how to handle aircraft with failed authentication – deliver messages to ANSP? FAA requires delivery of all ATS traffic on Datacomm service. Liability, safety, and security concerns intersect.
- After DTLS handshake completes the aircraft will follow up with a message to exchange the IP address, Tail Number and Flight ID of the aircraft
- This is media agnostic

DTLS Session Parameters

Field	Value
Keys	ECDSA
Diffie Hellman	ECDHE
Elliptic Curve	secp384r1
Encryption	AES 256 CBC
Hash	SHA 384
Compression	Deflate

DTLS Handshake

FLIGHTs



Client

Server

ClientHello → Flight 1

← HelloVerifyRequest Flight 2

ClientHello → Flight 3

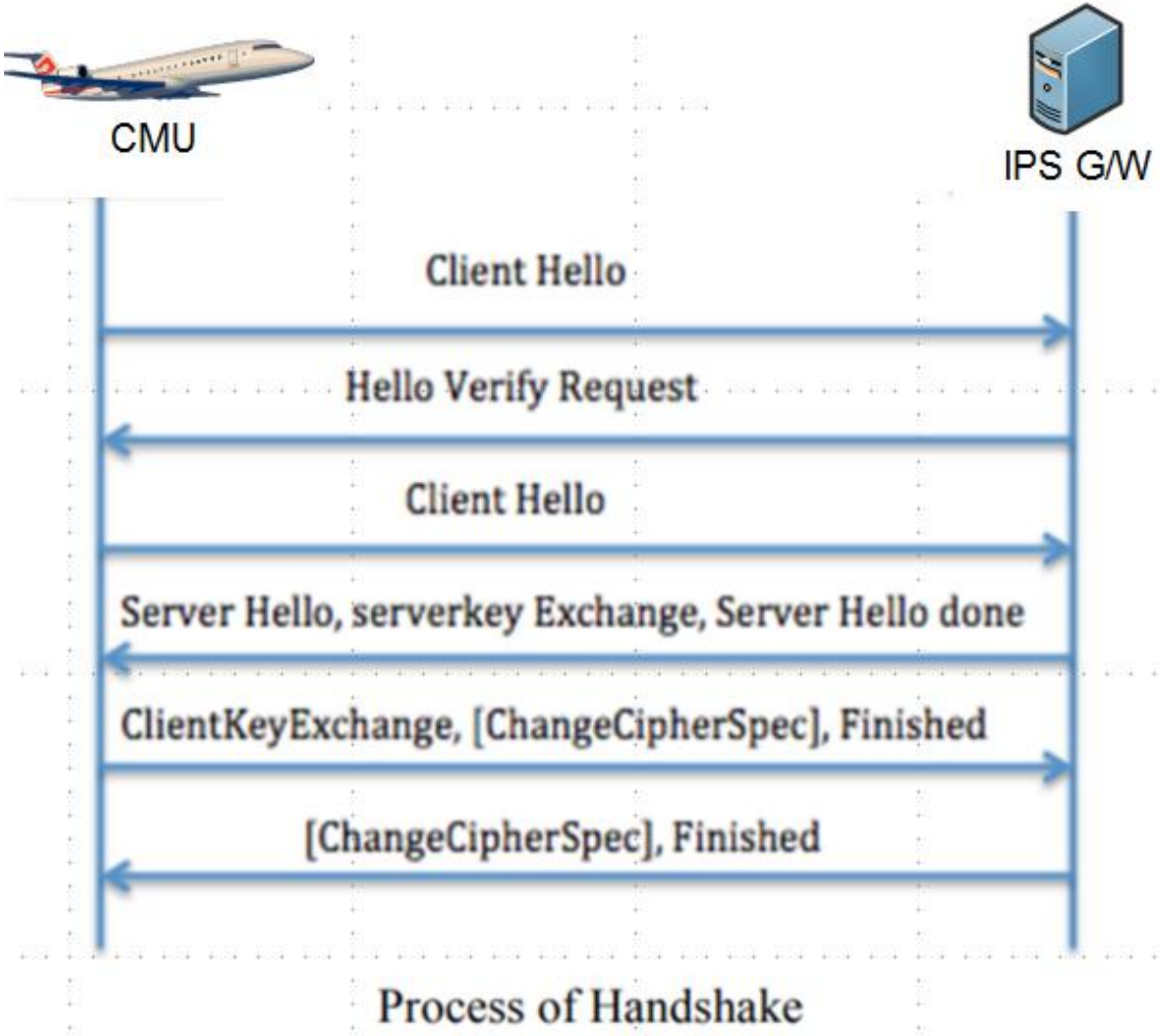
← ServerHello
ServerCertificate
CertificateRequest
ServerKeyExchange
ServerHelloDone Flight 4

ClientCertificate
ClientKeyExchange
CertificateVerify →

ChangeCipherSpec
Finished → Flight 5

← ChangeCipherSpec
Finished Flight 6

DTLS Sequences


CMU
IPS G/W
Client Hello
Hello Verify Request
Client Hello
Server Hello, serverkey Exchange, Server Hello done
ClientKeyExchange, [ChangeCipherSpec], Finished
[ChangeCipherSpec], Finished
Process of Handshake

DTLS Sequences

- 01 Client Hello
- 02 Server Hello
- 03 Certificate
- 04 Server Key Exchange
- 05 Server Hello Done
- 06 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
- 07 Application Data
- 08 Change Cipher Spec
- 09 Hello Request, Hello Request
- 10 Encrypted Alert
- 11 Client Hello

Authentication / Key Management

- ECDSA keys pairs will be provided by the primary service provider for each aircraft subscribed
- Keys will be signed by the primary service provider’s own or designate’s certificate authority (CA) key and be verifiable by any entity possessing the service provider’s or designate’s public key
- Each aircraft will receive a public key and a private key. The public key is used for authentication with the IPS Gateway(s) and the private key is kept secret with the aircraft
- To minimize the size of the public keys, suggest encoding in X.509 certificate DER format. The private keys are never transmitted
- Each service provider or designate will maintain a service key directory of X.509 certificates for all aircraft for which they are the primary service provider. 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
- 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.

Key Management (1/3)

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

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 Handshake completion.

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

Key Management (2/3)

Initial Key installation: Upon manufacture completion, avionics will contain no keys or IP address for IPS authentication. It is recommended that the manufacturers provide a service whereby avionics can be pre-loaded with certificates, IP addresses and keys from an IPS service provider prior to installation in an aircraft.

- Failing pre-load by the avionics manufacturer, it is recommended that avionics have a physical way, to load certificates, IP address configuration 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.

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.

Upload a new Root CA Certificate: 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.

- 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).

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.

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.

Key Management (3/3)

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.

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.

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

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.

Ground IPv6 Address Lookup and Retrieval

Ground System IPv6 Address Lookup / Retrieval

FANS1/A, B1 and B2 Applications

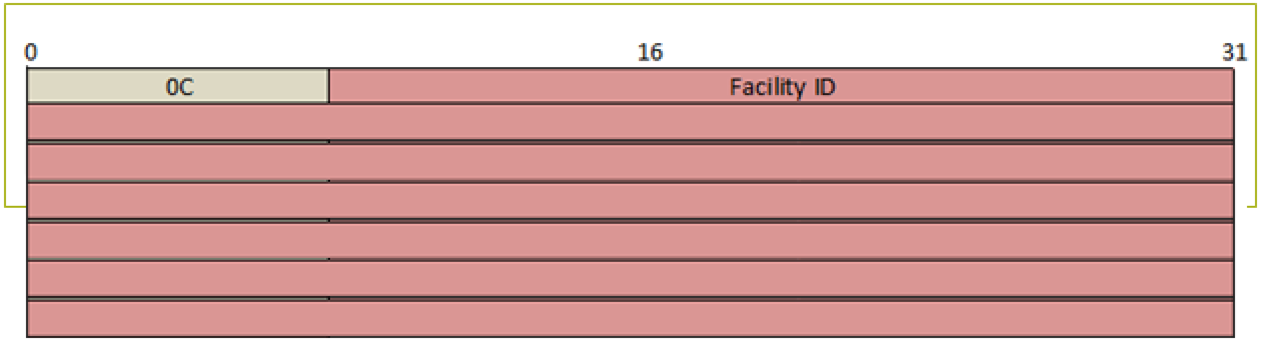
- *Aircraft will retrieve the Ground System IP address from a ground system using simple address lookup.*
- *This will simplify the address management since aircraft doesn’t need to carry ANSPs address database currently done for the ATN B1 systems*
- *It will automatically occur at ATNPKT layer when crew performs the logon to specific center such as EDMD, KUSA etc.*

IPS provides the name lookup on standard port 5908

- *First octet 0x0C identifies it is name lookup on port 5908*
- *The Ground IP Lookup message will be generated by the aircraft when it needs to obtain a specific facility IP address*
- *Source IPv6 address will contain Aircraft Nomadic fixed address assigned by ICAO*
- *Destination IPv6 address will contain the ground system IPv6 address that can provide the name lookup service*

IP Lookup Request Message

- *First octet 0x0C identifies it is name lookup on port 5908*
- *The Ground IP Lookup message will be generated by the aircraft when it needs to obtain a specific facility IP address*
- *Aircraft encapsulates the IP lookup message following format and send to the ground*
- *Message is encapsulated in UDP or TCP currently UDP only used*

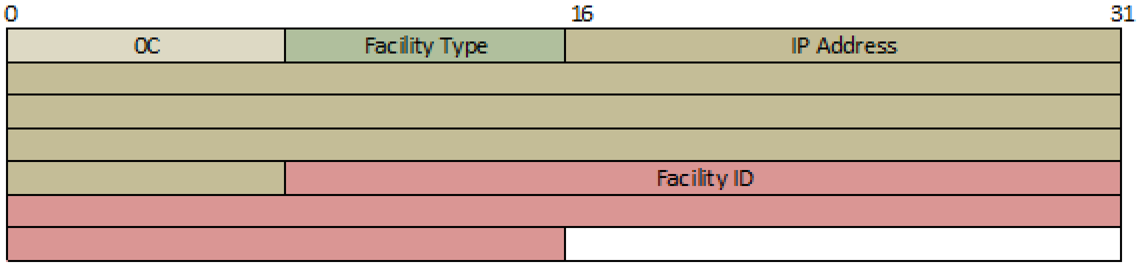


0 16 31

0C Facility ID

Ground IP Lookup Response Message

- First octet 0x0C identifies it is name lookup on port 5908
- The response will contain a facility type code, the 128 bit address followed by the facility ID in the request

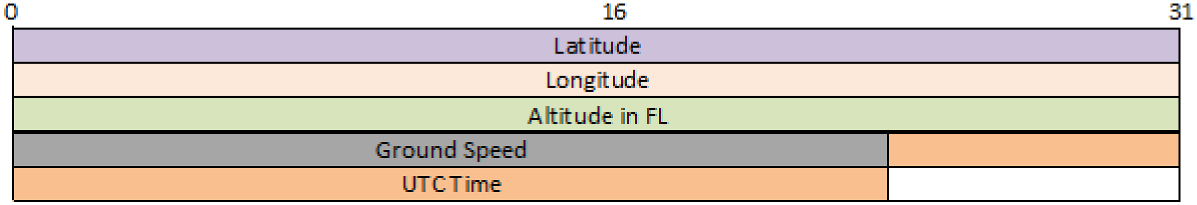


IPS Information Message

IPS Information Message

- ***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.
  - First octet 0x0B identifies it as Information message in the port 5908
  - This message may be encrypted between DSP and Aircraft using DTLS

IPS Information Message Format & Details



0

16

31

Latitude

Longitude

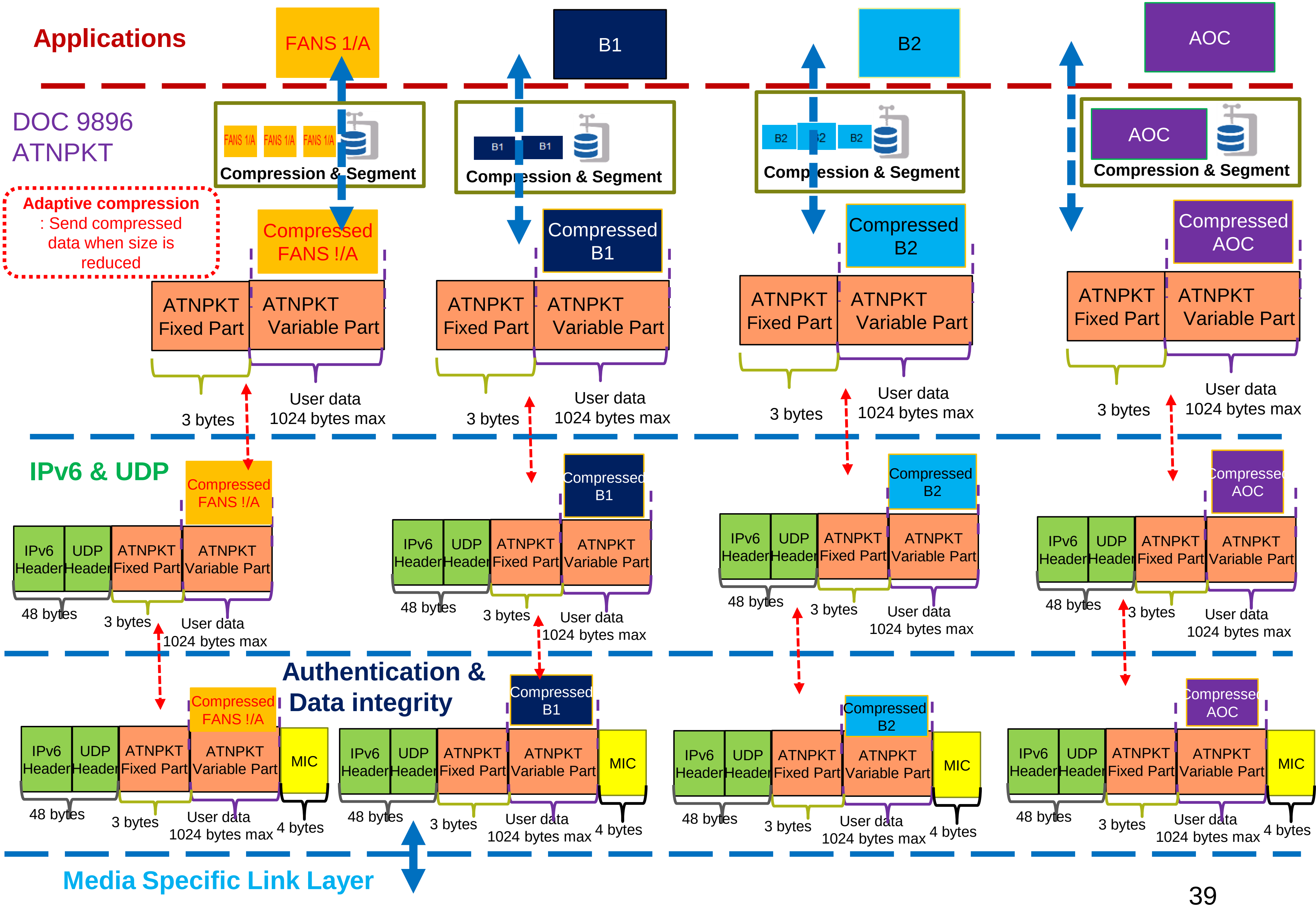
Altitude in FL

Ground Speed

UTCTime

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

IPS Message Encapsulation



Applications

FANS 1/A

B1

B2

AOC

DOC 9896 ATNPKT

FANS 1/A FANS 1/A FANS 1/A

Compression & Segment

B1 B1

Compression & Segment

B2 B2 B2

Compression & Segment

AOC

Compression & Segment

Adaptive compression : Send compressed data when size is reduced

Compressed FANS !/A

Compressed B1

Compressed B2

Compressed AOC

ATNPKT Fixed Part | ATNPKT Variable Part

3 bytes

User data 1024 bytes max

IPv6 & UDP

Compressed FANS !/A

Compressed B1

Compressed B2

Compressed AOC

IPv6 Header | UDP Header | ATNPKT Fixed Part | ATNPKT Variable Part

48 bytes

3 bytes

User data 1024 bytes max

Authentication & Data integrity

Compressed FANS !/A

Compressed B1

Compressed B2

Compressed AOC

IPv6 Header | UDP Header | ATNPKT Fixed Part | ATNPKT Variable Part | MIC

48 bytes

3 bytes

User data 1024 bytes max

4 bytes

Media Specific Link Layer

IPS over VDL Mode 2

IPS over VDL M2

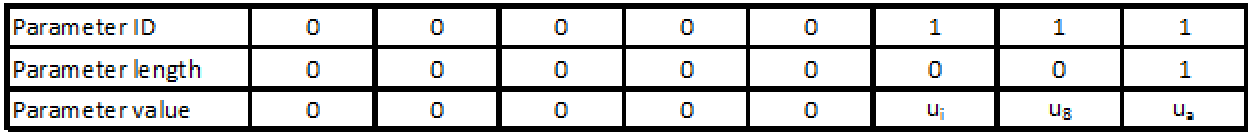
- Provides IP capability over existing VDLM2 infrastructure
- ISP Message Gateway provides value to operators and end users
- Supports IPS end Systems, ATN/OSI, IPS, and A620 across multiple regions
- New VDLM2 UI frame approach provides more message delivery reliability, improved bandwidth utilization, and improved performance

IPv6 over Connection-less VDL 2

- Ground station broadcast the AOA, ATN and IPS capabilities in the GSIF frame
- Existing link establishment and handoff mechanism are left as is.
- Existing mechanism can be used to move aircraft to new frequency
- Aircraft utilizes UI frame to send data to all ground station (aircraft will use any ground station address specific to a particular DSP)
- Data will be received from multiple ground station
- Ground Gateway will perform de-duplication and send to the end system
- Ground Gateway will determine best ground station to deliver messages, retry and re-transmission logic
- Ground Gateway Utilize the UI frame AVLC destination address specific to the aircraft

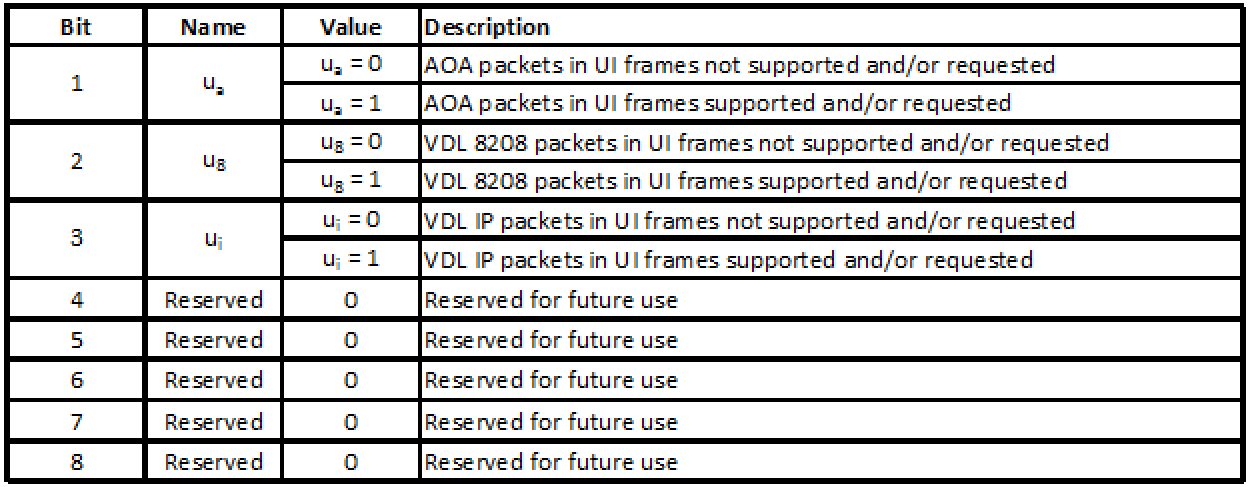
GSIF – Additional Parameter UI Support

1. New parameter to advertise support of exchanging data using UI frames
2. The parameter indicates if UI frames are supported for AOA packets, and/or VDL 8208 packets and/or VDL IPS packets



Parameter ID	0	0	0	0	0	1	1	1
Parameter length	0	0	0	0	0	0	0	1
Parameter value	0	0	0	0	0	u_i	u_8	u_a

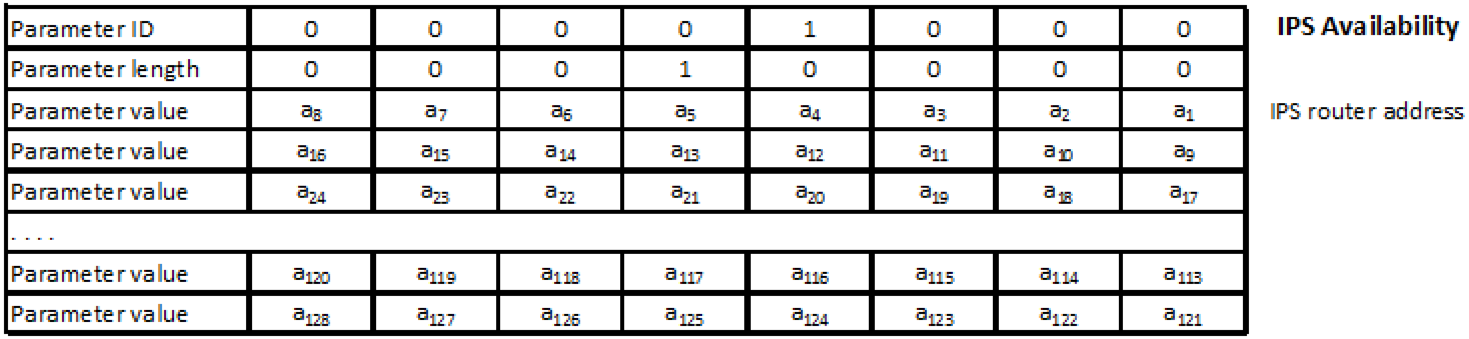
UI Frames Support



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 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

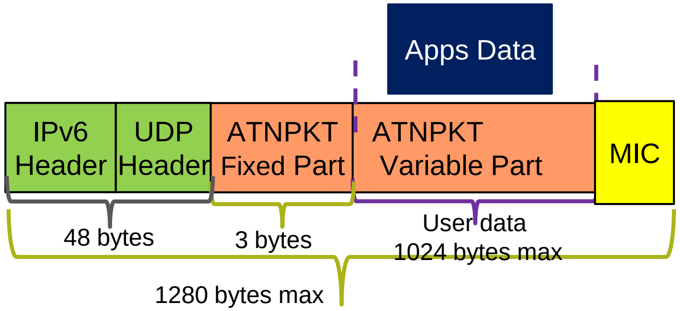
GSIF –Propose parameter for Default Gateway

- New parameter to advertise IPS availability
- Presence of the parameter indicates IPS availability and provides the IPv6 address of the IPS Gateway / Router

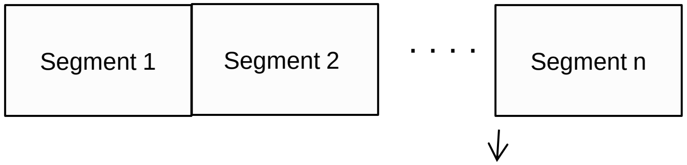


Parameter ID	0	0	0	0	1	0	0	0	**IPS Availability**
Parameter length	0	0	0	1	0	0	0	0	
Parameter value	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	IPS router address
Parameter value	a_{16}	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	
Parameter value	a_{24}	a_{23}	a_{22}	a_{21}	a_{20}	a_{19}	a_{18}	a_{17}	
. . . .									
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}	

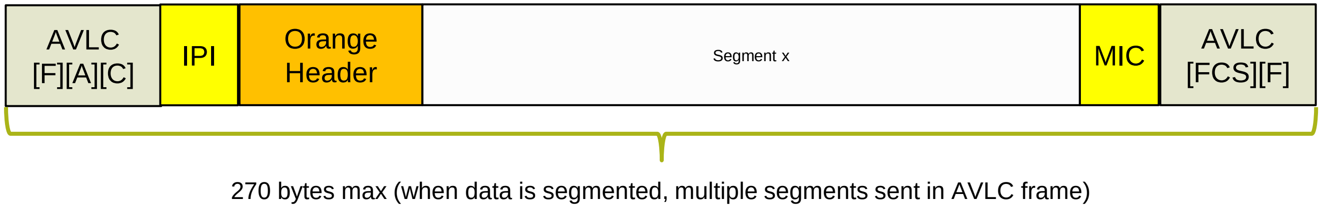
VDL2 Link layer segmentation for IPS



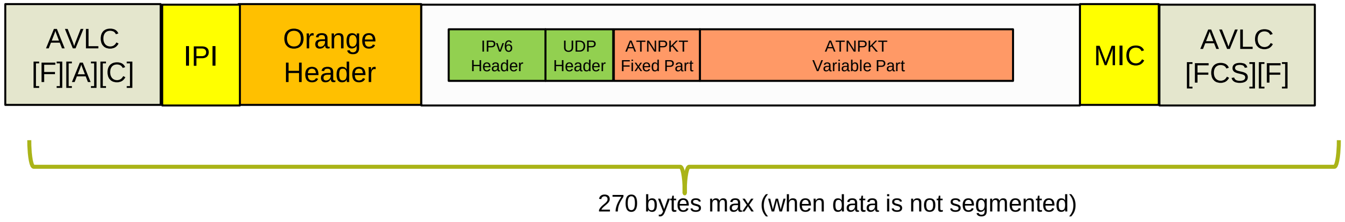
The IPv6 packet (1280 bytes max) will be segmented as needed for VDL



The number of segments generated will depend on the size of the IPv6 packet and the maximum AVLC frame size (270 for IMS)

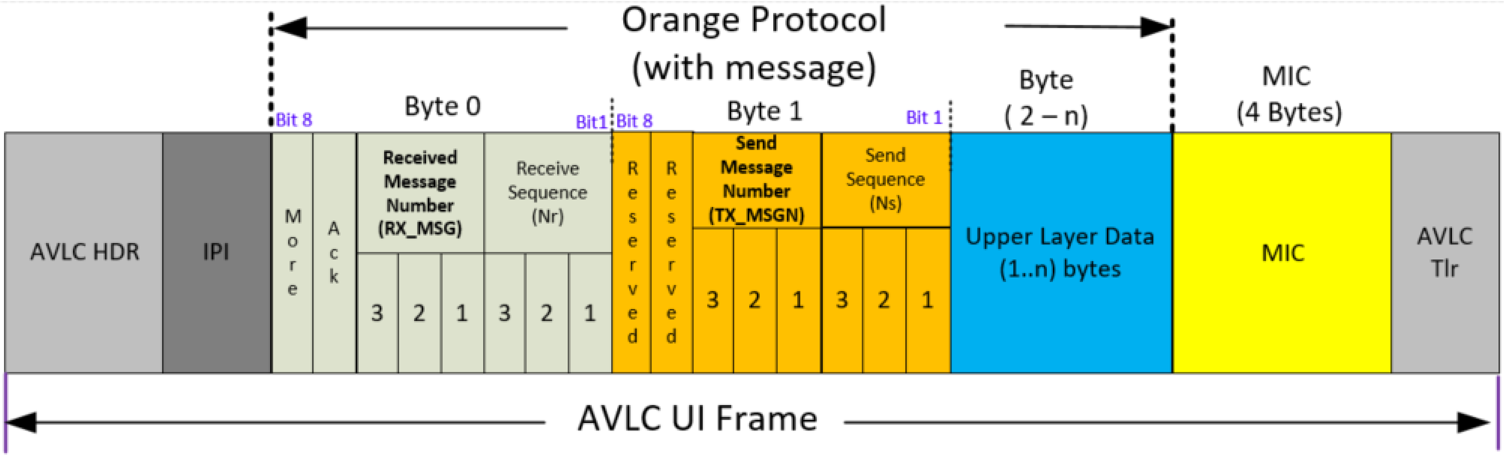

AVLC [F][A][C]
IPI
Orange Header
Segment x
MIC
AVLC [FCS][F]
270 bytes max (when data is segmented, multiple segments sent in AVLC frame)

Each segments will be in a AVLC frame with the IPS IPI, the ‘orange’ protocol header and a MIC.



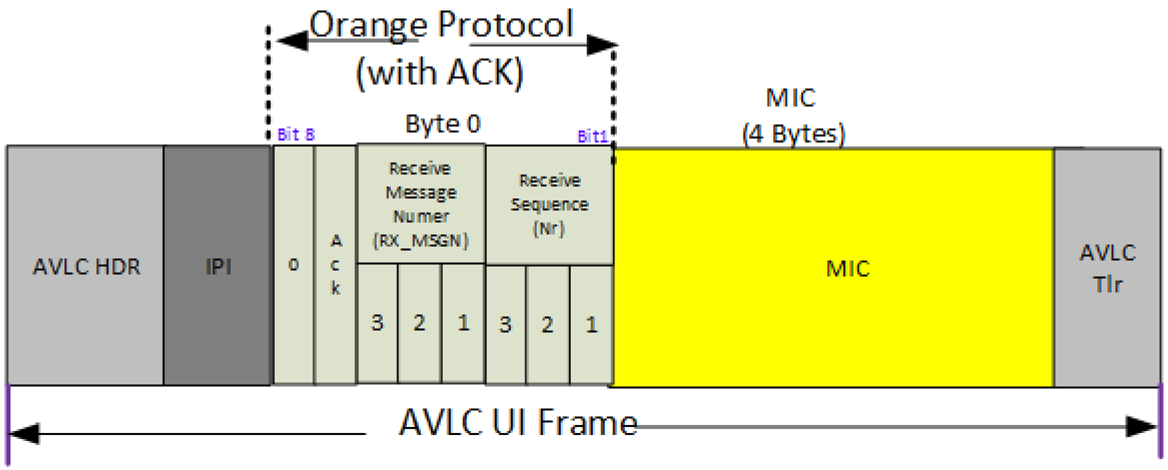
When the IPv6 packet is small, it will be contained in a single AVLC frame

Orange protocol consideration (1/2)



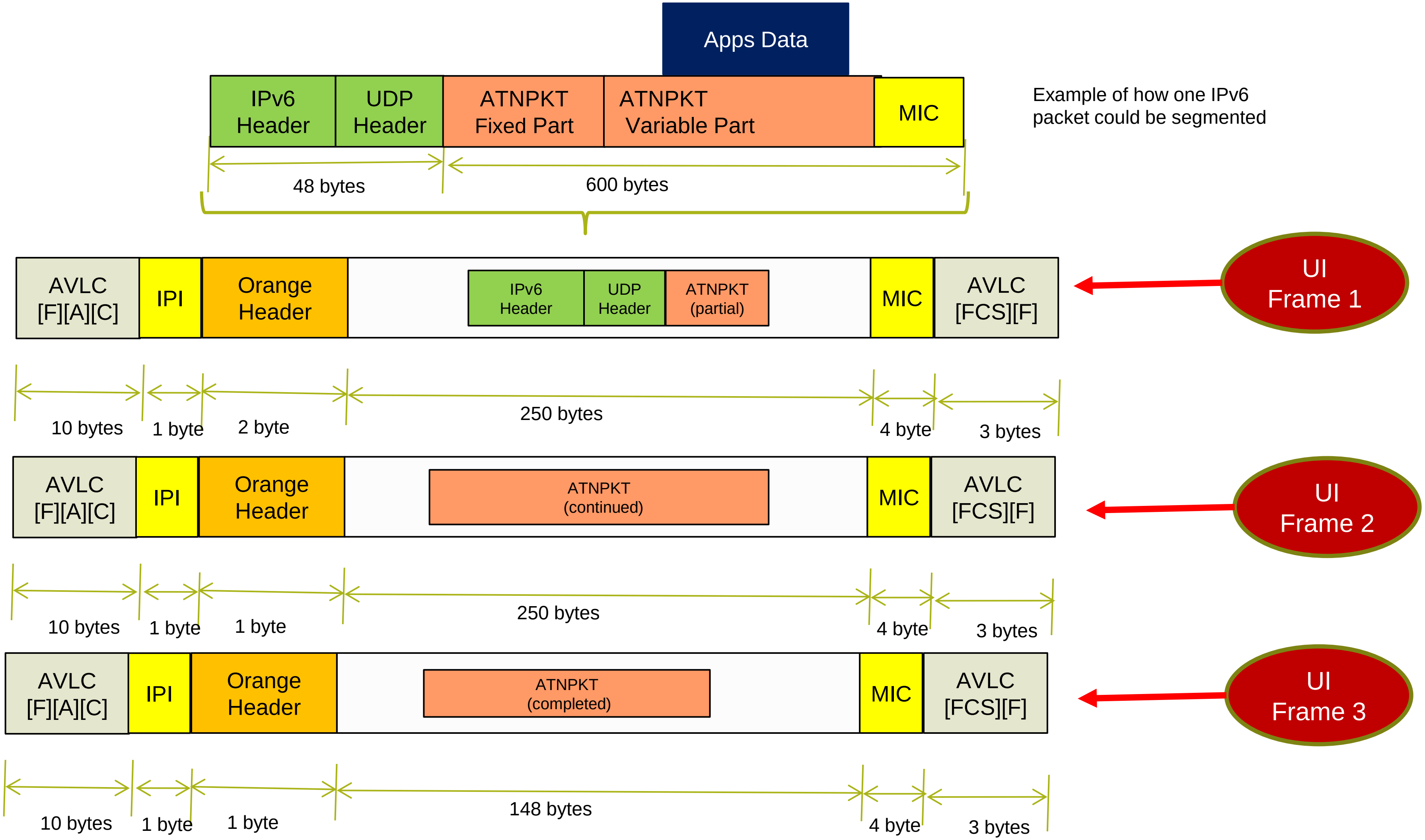
- More flag is set to one (1), when data are segmented and more data to come for a given message number.
- More flag for the last segment shall set to zero (0)
- Send Sequence Number (Ns): Segment sequence number of this segment that is being sent for a give message (TX_MSGN)
- Receive Sequence Number (Nr): Next expected sequence number of a segment (Nr -1 segment is being acked) for a give message (RX_MSGN)
- When message is not segmented, message number (TX_MSGN) shall set to zero (0).
- ACK bit shall be set when message contains the embedded Ack for a specific message number. Ack is performed for high water mark.
- When embedded Ack is not included, message number (RX_MSGN) and Receive sequence number (Nr) shall set to zero (0).
- Each segmented message contains a message number (1 through 7). When the message is segmented, message number indicates that each segment belongs to the specific message number (TX_MSGN).
- 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 (Destination address, Source address, Link Control Flag), IPI through last bytes of user data

Orange protocol consideration (2/2)



- IPI = 0x8E
- More flag shall set to 0
- ACK bit is set to 1
- Sequence number: Next expected segment (note if there is multiple segment and missed the first segment, sequence number is set to 0)
- Message number this segment is ACKed for
- Ack is only send for the segmented message
- MIC includes AVLC header, IPI and 1 byte of orange protocol.
- For authentication DTLS handshake, MIC is not included

VDL AVLC Segmentation example



Apps Data

IPv6 Header | UDP Header | ATNPKT Fixed Part | ATNPKT Variable Part | MIC

48 bytes | 600 bytes

Example of how one IPv6 packet could be segmented

AVLC [F][A][C] | IPI | Orange Header | IPv6 Header | UDP Header | ATNPKT (partial) | MIC | AVLC [FCS][F]

10 bytes | 1 byte | 2 byte | 250 bytes | 4 byte | 3 bytes

UI Frame 1

AVLC [F][A][C] | IPI | Orange Header | ATNPKT (continued) | MIC | AVLC [FCS][F]

10 bytes | 1 byte | 1 byte | 250 bytes | 4 byte | 3 bytes

UI Frame 2

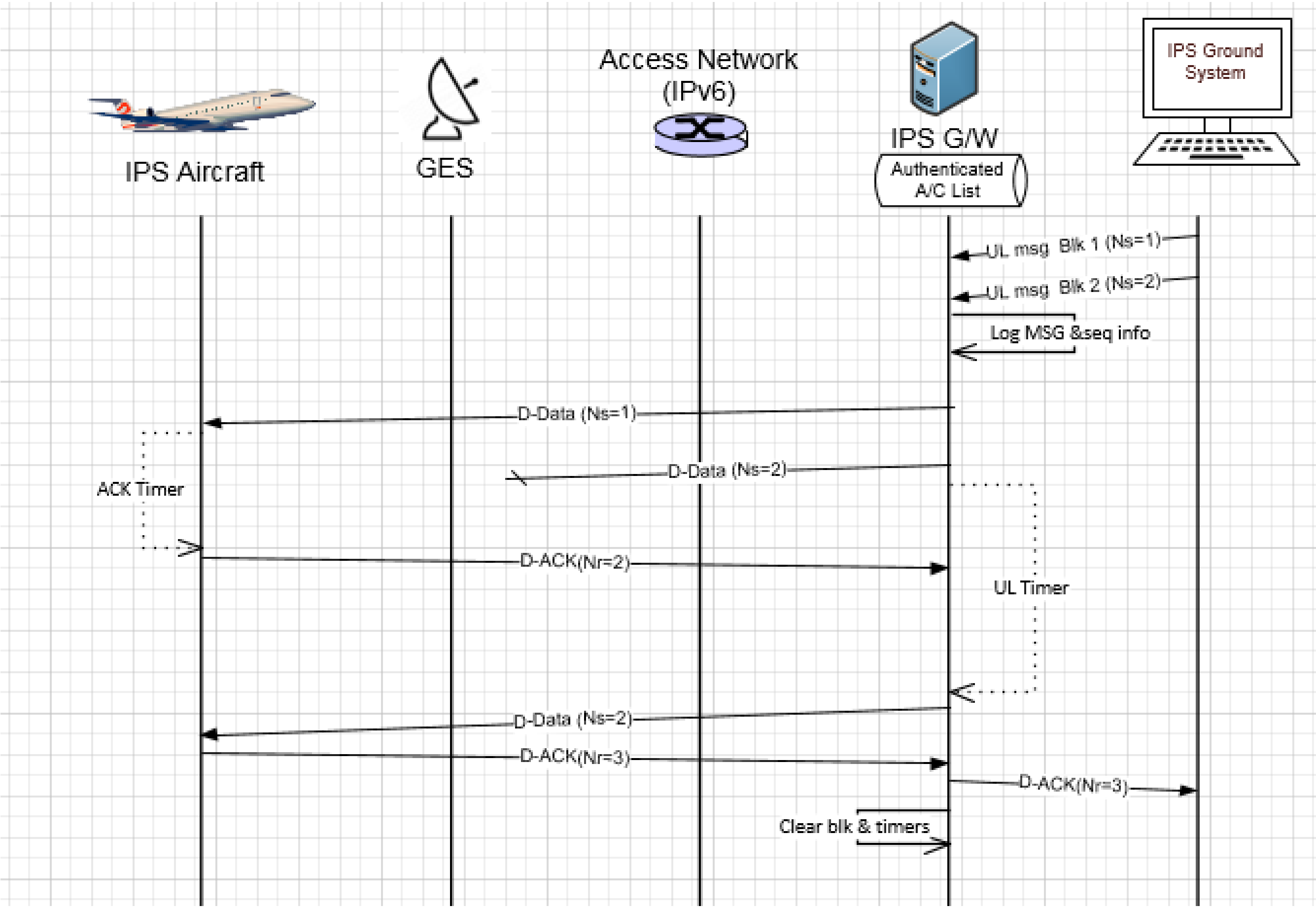
AVLC [F][A][C] | IPI | Orange Header | ATNPKT (completed) | MIC | AVLC [FCS][F]

10 bytes | 1 byte | 1 byte | 148 bytes | 4 byte | 3 bytes

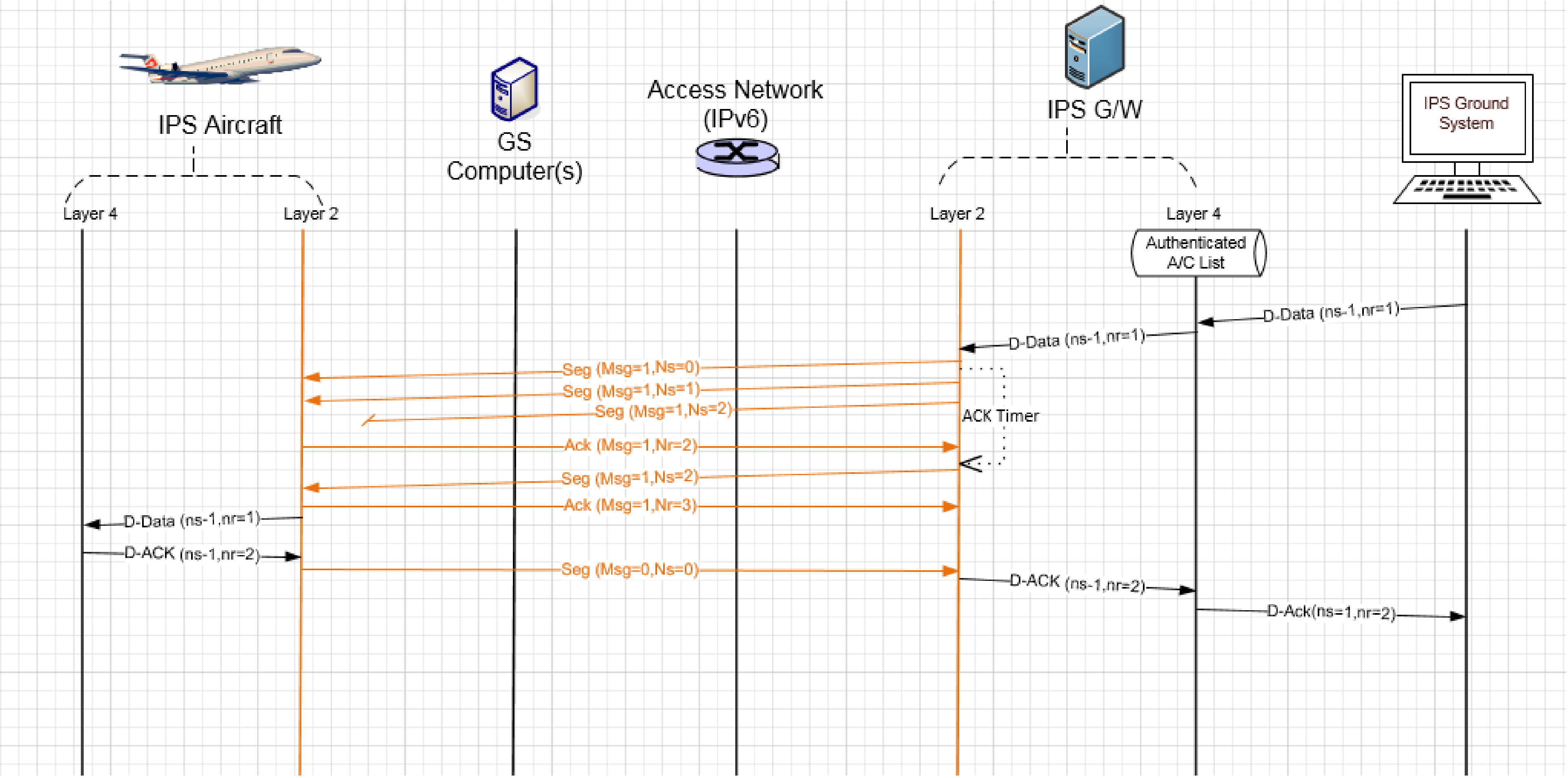
UI Frame 3

Example Scenarios

Example Scenario (1)



Example Scenario (2)



Quick Demo & Q/A