



# IPS Deployment Options

Date July 26, 2018

Presented by Jonathan Graefe



## Diagram Definitions

- Air/Ground Router (Layer 2 Orange)– De-duplication, layer 2 segmentation, layer 2 MIC check, aircraft logon check. (VDL Specific)
- Active Aircraft Session List: Maintains a list of aircraft known by this IPS gateway by direct link, other media or by mobility.



## Diagram Definitions– Page 2

- **Key Server:** Provide the authentication and authorization service to access the network. Certificate lookup service provided by each service provider. The Primary Service provider must validate (or not) all keys that claim to be signed by that service provider or its designate.
- **Key/Cert Management:** Function to manage keys and certificates on aircraft.



## Diagram Definitions– Page 3

- Media Arbitration, Customer Policy Engine and compression (Layer 3):  
The central brains of the IPS Gateway. For Uplinks provides Media Arbitration to select the best media as per customer policies and compression if needed. On downlinks decompresses if needed and detects the type of message and security then directs the downlink:
  - To the protocol converter if requires conversion
  - To the end customer if IPS and directly connected customer
  - To the mobility router if IPS and non-directly connected customer



## Diagram Definitions– Page 4

- Protocol Converter: Provides protocol conversion capabilities between an aircraft and an end system when one side does not support IPS. Available conversions will be:
  - IPS to 620
  - IPS to ATN
  - ATN to IPS
  - 620 to IPS
- ACARS: Aircraft communications addressing and reporting system network
- ATN: Aeronautical Telecommunications Network
- IPS Ground Host: A customer end system that is IPS capable
- Mobility Router: Provides access network mobility management. A router equipped with IPv6 mobility functions that advertises aircraft and customer availability to other service providers and receives advertisements from other service providers.



## Diagram Definitions– Page 5

- **Other IPS Service Provider:** The Primary Service Provider of an aircraft and customer host if not the current IPS host. Further the entity responsible for key management and IP addressing of the aircraft.
- **Name Lookup:** Name lookup server provided by the primary service provider or a trusted companion service provider. If the name is not available via the host IPS server the primary service provider will be contacted to provide information.
- **DNS:** Domain Name Server an RFC compliant Name server commonly used on the web.







## Possible IPS Gateway system deployment options

- Based on the Deployment scenarios presented by M. Olive, the following deployment architecture options are defined:
  - Option 1: Logon at Layer 2 and Layer 3 separately
    - Maps to Mike Olive's presentation options: DS-03b, DS-03d, DS-04a, DS-04b, DS-07b, DS-07d, DS-08
  - Option 2: SESAR Model
    - Maps to Mike Olive's presentation options: DS-01, DS-02



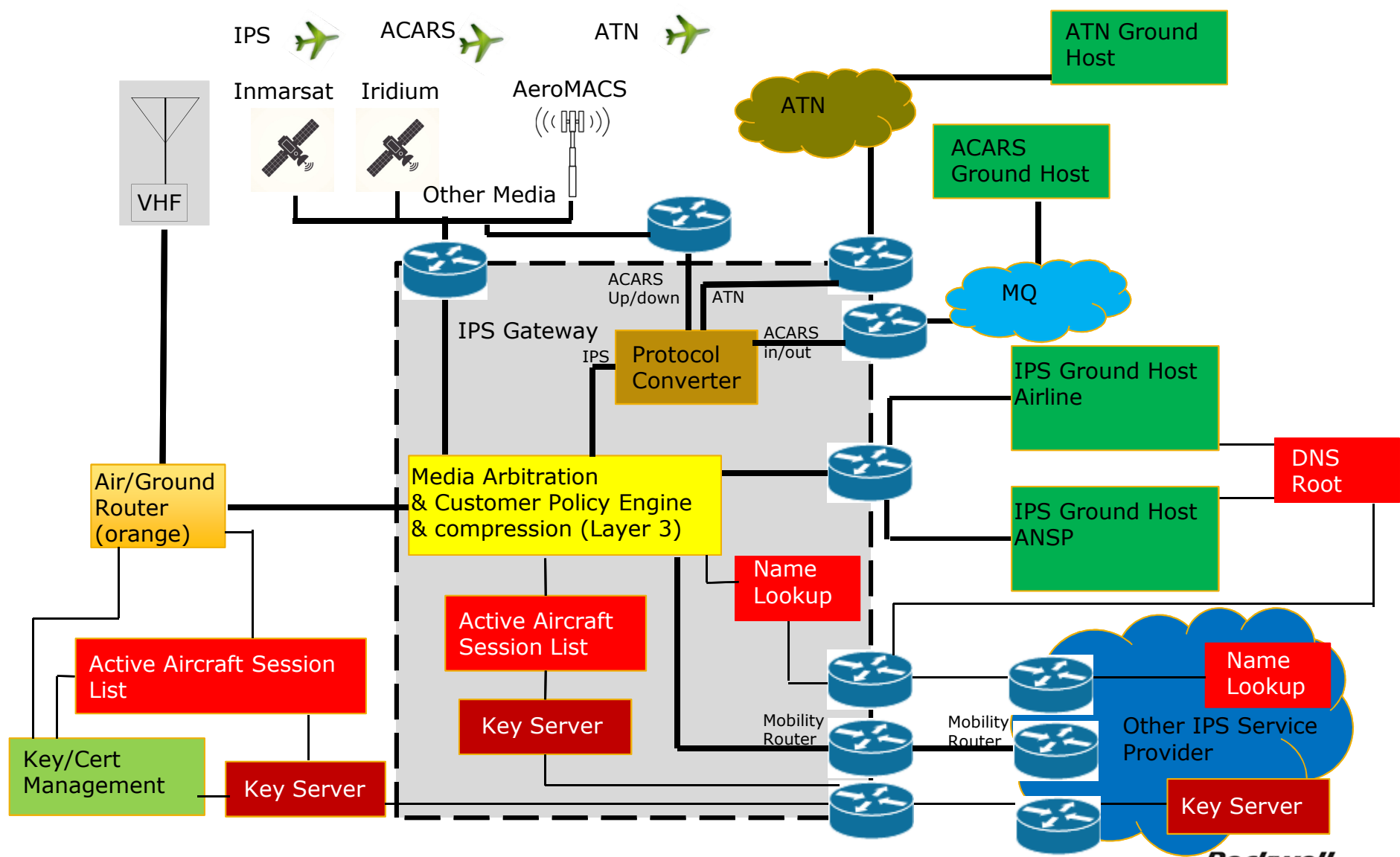
## System data flow key

-  Message Data Path
-  Support Traffic Path (non message traffic)
-  Aircraft (Type)
-  Responsibility boundary (perhaps optional)

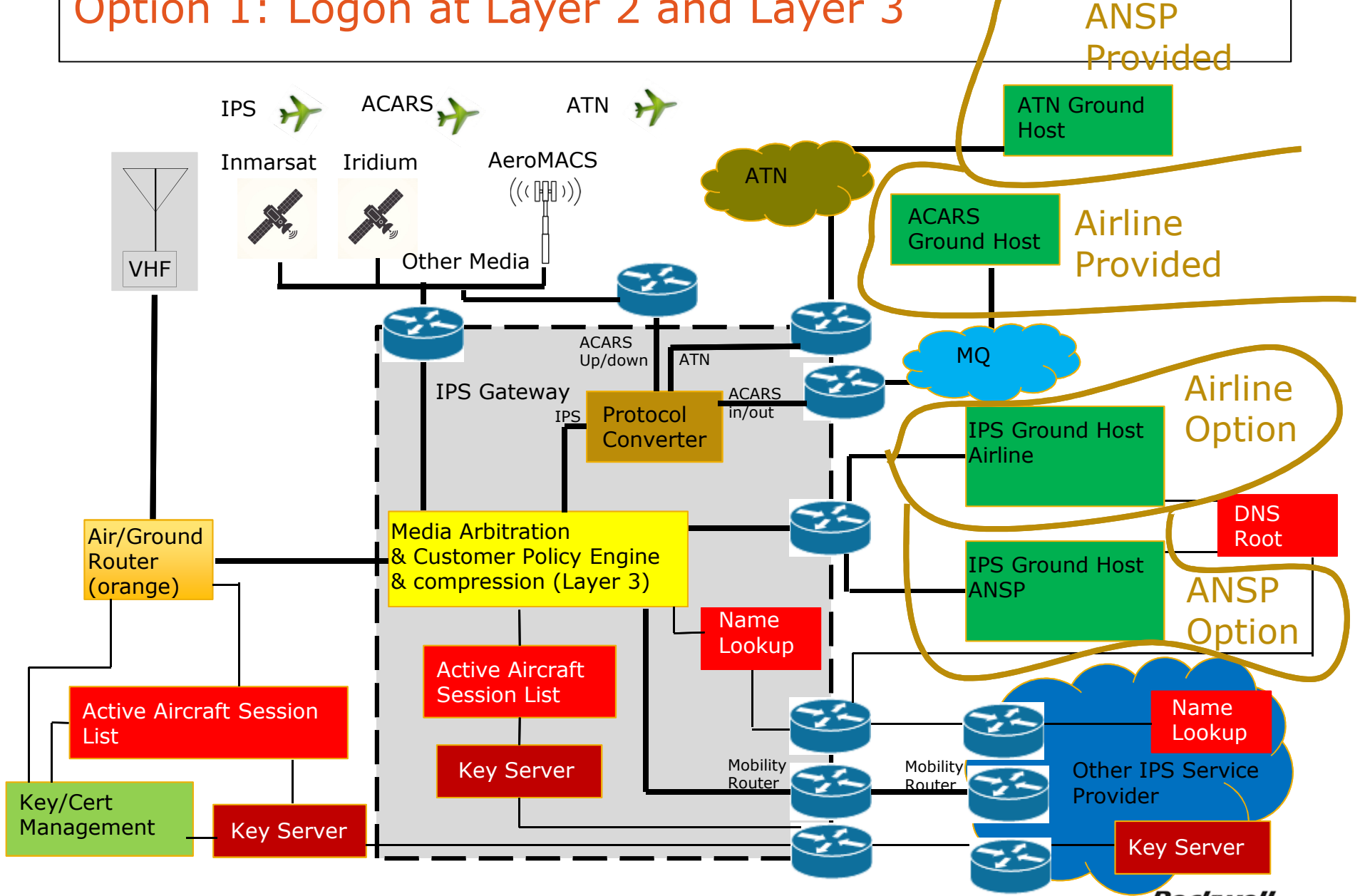




# Option 1: Logon at Layer 2 and Layer 3



# Option 1: Logon at Layer 2 and Layer 3





## IPS System Design option 1

- Option 1: Logon at Layer 2 and Layer 3
  - Model allows airlines and ANSPs to use the same infrastructure as today and they can choose when, if ever, to upgrade their back office to include an IPS end system. Protocol conversions are available for legacy systems to newer aircraft and vice versa.
  - DTLS Logon at Layer 2 and again at IPS. Aircraft must be on Service provider's network to use the generated Layer 2 session key. Migration to another media (such as Satcom/AeroMACS etc) will require a new logon with that agency, but IPS session key can be retained.
  - Fulfills Airbus requirement of securing Layer 2.



## IPS System Design option 1 - continued

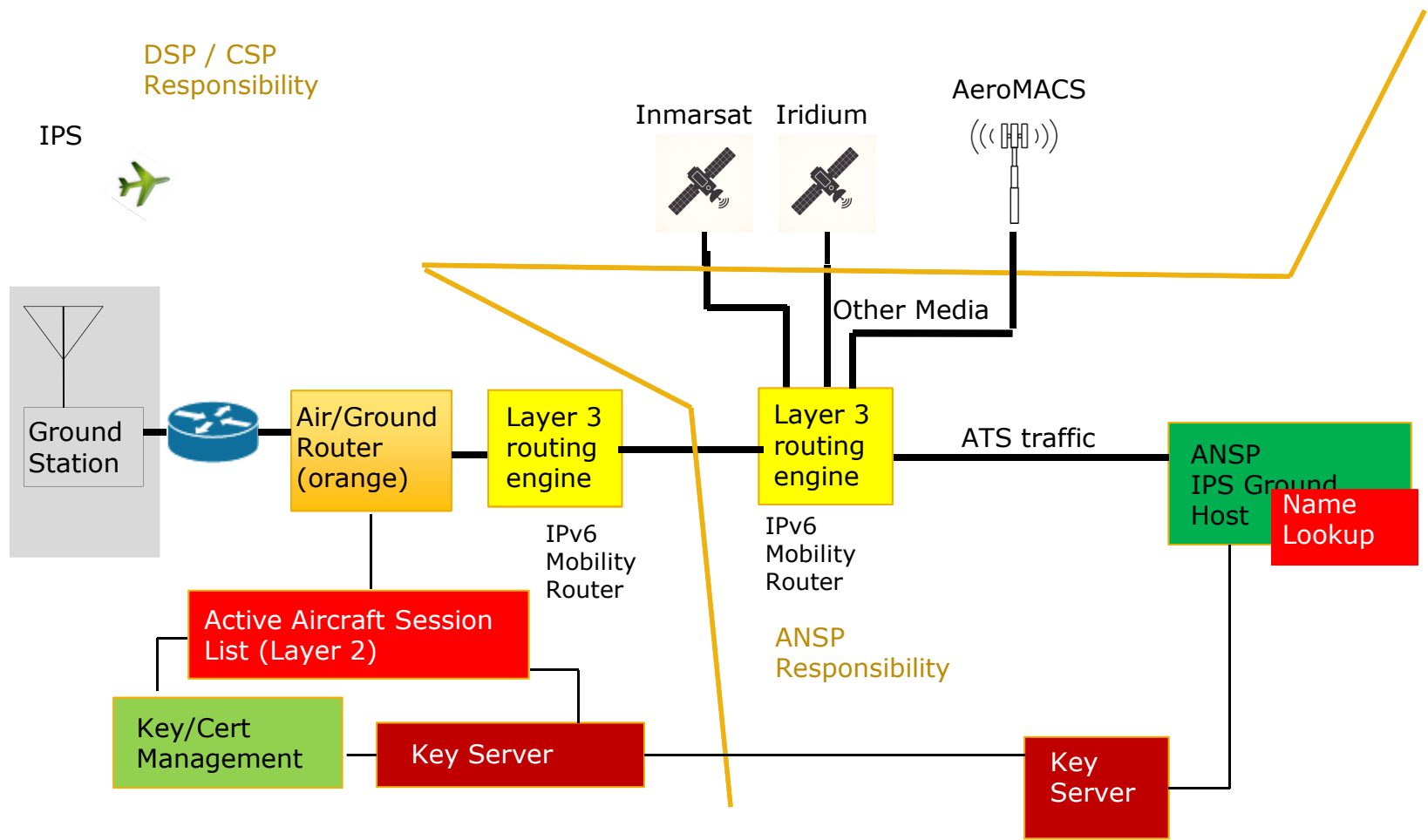
- Option 1: Logon at Layer 2 and Layer 3
  - Aircraft session is tracked over multiple different media types, same session key can be used Layer 3 across all media routing via this IPS Service Provider, the same session key, Layer 3 MIC generation, can be used on Satcom, VHF, AeroMACS, etc. No need for media advisory messages. It is possible that aircraft traversing the ocean may only need to logon at Layer 3 once for the entire voyage. Layer 2 logon needed for every media switch.
  - Layer 3 Compression can be used over all media types to reduce transmission sizes and subsequent bills for byte charged services.
  - Allows Key Management at Layer 2 over Primary IPS Service Provider's network only. No Layer 3 Key Management.
  - Airlines can choose to run their own RFC compliant DNS Ground/Ground Server to supplement the simple name lookup. The IPS Service provider will implement the Air/Ground simple name lookup and query the airline's or ANSP's DNS for any requests that do not have an entry in the simple name lookup server.



# SESAR Model

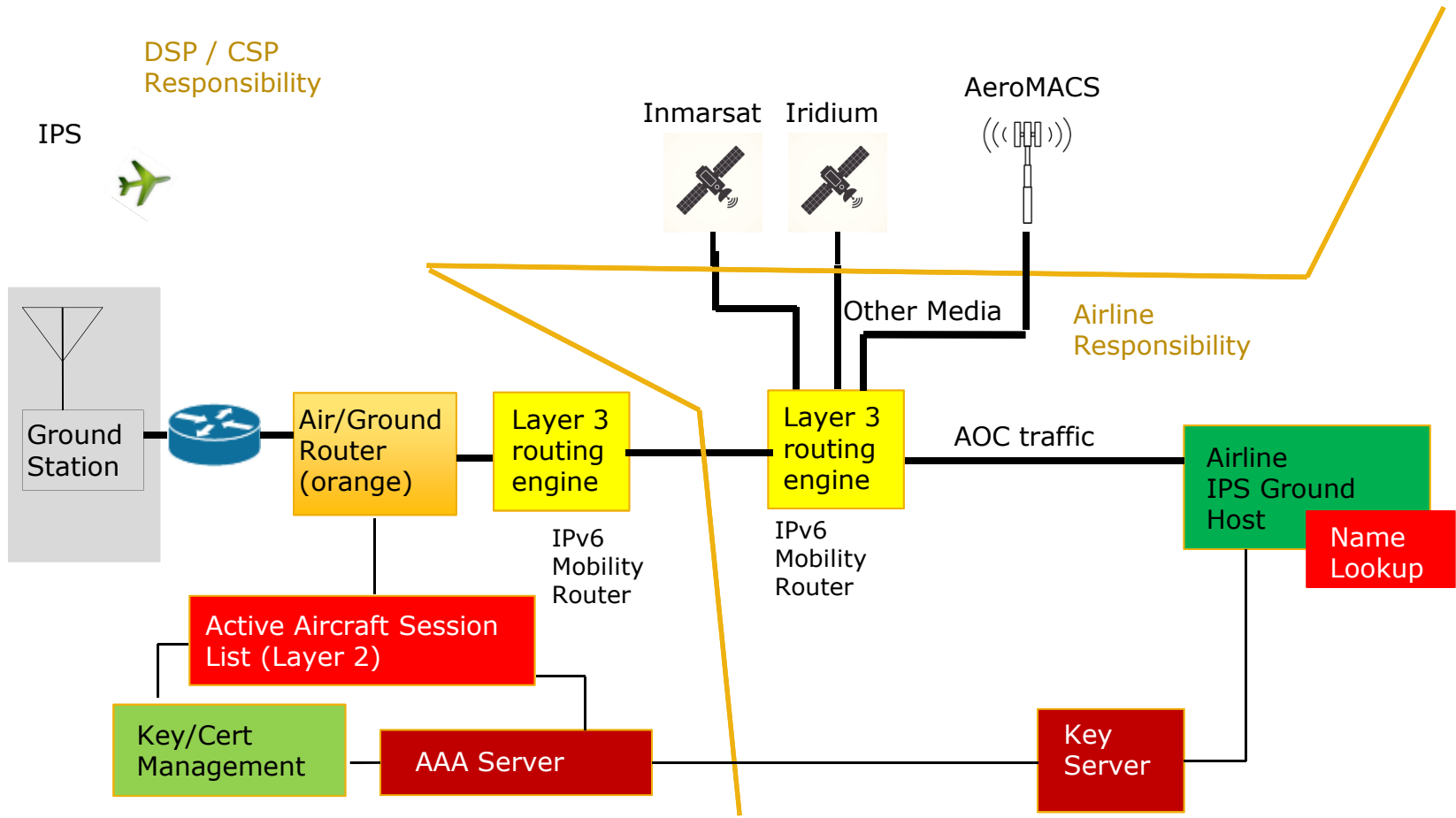


# Option 2A: IPS SESAR ANSP Model





# Option 2B: IPS SESAR Airline Model





## IPS System Design Option 2

- Option 5: IPS European Model (SESAR)
  - Model allows ANSP maximum flexibility to setup their own IPS Gateway, develop their own simple name lookup, maintain their own AAA server for IPS. ANSPs must upgrade their back office or have a protocol conversion gateway. No protocol conversion is provided by the CSP/DSPs.
  - DTLS Logon is only at Layer 2. Aircraft must be on Service Provider's network to use the generated session key. Migration to another media (such as Satcom/AeroMACS etc) will require a new logon with that agency.
  - Fulfills requirement of securing Layer 2.
  - Aircraft are not tracked across media, a new logon is required for each media type. Media advisory messages are required to inform the home IPS provider of the media types that aircraft has currently available. Aircraft traversing the oceans will need to make several connections and logins





## IPS System Design Option 2 - Continued

- Option 5: IPS European Model (SESAR)
  - Compression is not available except for that provided at Layer 2. ATNPKT compression as defined in 9896 remains but regulatory restrictions area problem without a DSP in the middle.
  - Airlines will need to supply their own simple name lookup server DAY 1 to supply their aircraft with name information services. (This is not the RFC compliant DNS server under other options)
  - Aircraft key management can only be done over the airline and ANSP. Aircraft may need many keys.
  - Each airline will need to connect with each ANSP and CSP/DSP for key authentication.
  - System opening between CSP and IPS Service Provider, IPS Service Provider and ANSP, and/or IPS Service Provider and airline. Many places for an insertion attack.