

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: March 13, 2010

C. Bauer
S. Ayaz
DLR
September 9, 2009

ATN Topology Considerations for Aeronautical NEMO R0
draft-bauer-mext-aero-topology-01

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on March 13, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

The aviation industry is in the process of moving from legacy and ISO-based protocols to an IP-based environment. This task will require adoption, modification and/or creation of IETF related protocols. The intention of this draft is therefore to provide an overview of the operational environment and the topology of the Aeronautical Telecommunications Network to the IETF.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Access Technologies	6
3.1.	Wifi/Gatelink	6
3.2.	WiMAX	6
3.3.	SATCOM	6
3.4.	Long range air-to-ground	7
4.	Topology of the ATN	8
4.1.	Nodes	8
4.2.	Global Structure	9
4.3.	Points of Attachment	10
4.4.	Location of Home Agents	13
4.5.	Trust Relationships	13
5.	ATN Applications	15
5.1.	ATS Applications	15
5.2.	AOS Applications	16
6.	Security Considerations	20
7.	Acknowledgements	21
8.	Changes from -00	22
9.	References	23
9.1.	Normative References	23
9.2.	Informative References	23
	Authors' Addresses	25

1. Introduction

The ATN is a global network interconnecting ground-ground networks and air-ground access networks used for Air Traffic Services (ATS) and Airline Operations Services (AOS). As part of the ICAO Convention, ICAO has published Annex 10 which standardizes the ATN (SARPs). The current ATN technology and architecture are defined by the ATN Manual documents published by ICAO [[icao9705](#)], based on the ISO protocol CLNP, using a modified version of the IDRP interdomain routing protocol to support mobility of aircraft. This version of the ATN is only partially deployed at the present time. Meanwhile an ICAO working group has produced an amended version of the manual that allows the ATN to be an internetwork based on IPv6 for both ground-ground and air-ground communications. States have already begun deployment of the ground portion. For supporting mobility of aircraft within this new ATN architecture the Mobile IPv6 protocol family has been chosen and referenced within the new ATN manual [[icao9896](#)].

This draft tries to provide an overview of the aeronautical operational environment, the access technologies currently used for planned for usage in the future as well as application layer signalling.

Most discussions are currently focussed on NEMO Route Optimization work and this draft tries to help with the analysis of the possible options of NEMO RO within this context. The Network Mobility Route Optimization Solution Space Analysis [[RFC4889](#)] provides a comprehensive overview of the possibilities how RO can be performed. The selection of the right solution has to be based on the requirements, which were defined for aviation in [[I-D.ietf-mext-aero-reqs](#)]. The aim of this document is to provide additional information about the aeronautical environment, apart from what is already provided within the requirements document. Ultimately, this should help in selecting the most suited solution for the NEMO RO problem.

2. Terminology

ATS, AOS, PIES

The three different service classes as introduced in the requirements document [[I-D.ietf-mext-aero-regs](#)]. PIES is considered as non-safety related, whereas ATS is safety-related. While AOS is at the moment an atomic service class, it is foreseen that in the future its applications are going to be split into safety- and non-safety related subclasses.

ATS message exchanges have to fulfill strict latency requirements, therefore making an R0 mechanism necessary. While this is also true for safety-related AOS messages, the delay requirements are not as strict as for ATS.

ACSP

An Air Communications Service Provider operating access networks for aeronautical purposes, including air/ground data links. Currently there are two global ACSPs utilizing terrestrial and satellite link technologies for providing ATS/AOS services. However in the future there might be several global ACSPs (gACSPs) and additional smaller, local ACSPs (lACSPs). The usage of the word ACSP is generic and can refer to either a local or a global ACSP, depending on the context.

gACSP

Global ACSP - see definition of ACSP. A global ACSP has a world-wide network that spans over several continents.

lACSP

Local ACSP - see definition of ACSP. A local ACSP owns a network that is limited to a continental region or a certain nation and its boundaries. Examples for this are Air Navigation Service Providers that operate their own air-ground access network.

ANSP

An Air Navigation Service Provider that manages the air traffic within a country or geographic region. Generally each ANSP has its own (ground-ground) network, and in addition the ANSP might also be an ACSP within that geographical region by operating its own air/ground access network, which might be due to security/policy or cost reasons. In this case we can call the ANSP a local ACSP.

Note: At least in Europe these are the only two existing business models as of now.

ICAO regulations and SARPs have to be respected and considered by the ANSP, nevertheless these organizations also have their own (network) policies. It should also be stated that ANSPs are usually governmental or at least state-owned institutions.

Data Link(s)

In the aviation environment it is common to call the air interface (layers 1 and 2 of the OSI model) 'data link' or sometimes also 'subnetwork' (e.g. the VDL Mode 2 subnetwork). This expression is equivalent to the more common 'access technology' terminology in other SDOs or the IETF.

3. Access Technologies

In the following we provide a short overview of IP-carrying technologies that are currently used or foreseen to be used in the future. In general there are regulatory aspects that limit the type of traffic that can be sent over certain frequencies, according to ITU-R regulations and allocations. Non-safety related services can not be carried over Aeronautical Mobile (Route) Service and Aeronautical Mobile Satellite (Route) Service bands.

3.1. Wifi/Gatelink

The well-known IEEE 802.11 family is already in use at airports today for AOS, operating in standard frequency bands. The AEEC, an aeronautical SDO, has specified Gatelink standards (802.11b/g, DHCP, DNS) that have the following characteristics:

1. Gatelink 822: 802.11i with WPA/WPA2
2. Gatelink 763: 802.11i with EAP-TLS (mutual authentication with client certificates) and RADIUS as AAA protocol

Apart from the Gatelink standard, airports are also using "normal" 802.11 equipment (e.g. WPA2 with static passwords). Airport authorities can operate the Wifi system themselves whereas at certain airports the access points are even operated by the airlines themselves.

3.2. WiMAX

It is planned to use the IEEE 802.16e standard for airport surface communications to carry ATS and safety-related AOS messages in a dedicated (safety-related) frequency band (at 5 Ghz with 60 Mhz bandwidth). The investigation and specification of this AeroWiMAX system is currently work in progress.

At the same time WiMAX systems within the standard frequency bands (2.5 Ghz, 3.5 Ghz, etc.) could also be used for non safety-related AOS applications and passenger internet access within airports.

The WiMAX security provisions might be reused for the aeronautical version of the standard.

3.3. SATCOM

Satellite communication systems are already in use today:

1. Connexion by Boeing: used to provide (IPv4) connectivity for PIES with a bandwidth of several Mbits/s. Not available anymore.
2. Inmarsat Swift-Broadband: Used for PIES and AOS communications, although not certified for safety-related services. Bandwidth is in the range of up to several 100 kbits/sec. Carries IPv4.

The currently available satellite systems that are certified for safety-related services are not providing native IP connectivity. Certain satellite operators are currently planning next-generation satellite constellations that will natively support IP and will most likely also be certified for safety-related services.

3.4. Long range air-to-ground

The following technologies are terrestrial systems relying on a network of base stations that can be used for communication when the aircraft is on cruise altitude.

1. L-Band Digital Aeronautical Communications System (L-DACS): two proposals for L-DACS are currently work in progress and one of them will be chosen for safety-related services (ATS and partially AOS). Bandwidth will probably be in the range of 1-2 Mbits/sec. Security provisions are not available (as of now).
2. Aircell: based on the 3GPP2 CDMA EV-DO standard and provides several Mbits/sec. It is currently only used for PIES (non-safety related).

4. Topology of the ATN

This section provides a description of the topology of the ATN, based on how it partially already exists and how it is planned.

4.1. Nodes

4.1.1. MR

The generic term 'airborne router' is also used in the aviation environment for the mobile router. It is reasonable to assume that in the future there is one IP based mobile router that handles ATS and a separate one for AOS and PIES traffic. Certain AOS messages might most likely also be routed over the ATS router (as it is already the case today). As in the future, at least from a strictly regulatory point of view, it is foreseen that AOS will be split into safety and non-safety related parts. In that case, the safety-related applications of AOS might be handled by the ATS router whereas non-safety related AOS applications rely on the the PIES router.

There are currently discussions related to potentially integrating ATS with AOS/PIES. It is not clear yet however how this integration could take place and whether it will happen at all.

4.1.2. ATS/AOS CNS

ATS CNS are Air Traffic Service Units (ATSUs) that refer to the controllers managing the air space. These nodes are located within the ANSP networks and are in general dynamic - as the aircraft traverses different regions of the world, the CN (the responsible ATSU) changes as well and is geographically close to the aircraft. The CNS mentioned here are the communication peers from the IP point of view and do not necessarily have to be the "real" end system.

An AO refers to an Airline Operations domain where AOS CNS are located. This is generally the airline headquarters/operations center or an airport. These nodes are relatively static throughout a flight; a number of 2 CNS can usually be expected. The connection options between the subnets at the airport and the airline headquarters can be manifold:

1. The subnet at the airport uses an Internet connection provided by the airport authority and establishes an IPsec VPN tunnel to the headerquarter
2. The subnet at the airport uses an Internet connection provided by a commercial Internet Service Provider and establishes an IPsec

VPN tunnel to the headerquarter

3. The subnet at the airport uses a connection provided by a gACSP to the headerquarter

Both ATS and AOS CNS are fixed, non-moving nodes.

4.1.3. MNNS

The MNNS of the ATS and AOS domains on board an aircraft are, as mentioned in [I-D.ietf-mext-aero-regs], LFNs and potentially even LMNs. They are operated by and are under control of the airline, although ICAO regulations and standards affect the ATS systems.

4.1.4. HA

We are considering HA(s) that are serving the ATS and AOS domain. The location of these entities is discussed in [Section 4.4](#). With the network-separation between safety and non-safety related services, there will most likely also be two Mobility Service Providers operating different HAs.

4.2. Global Structure

As already explained in [Section 2](#), access networks to which an aircraft may attach to are operated by either an ACSP or an ANSP. How these operational domains are related to each other in topological terms is explained below.

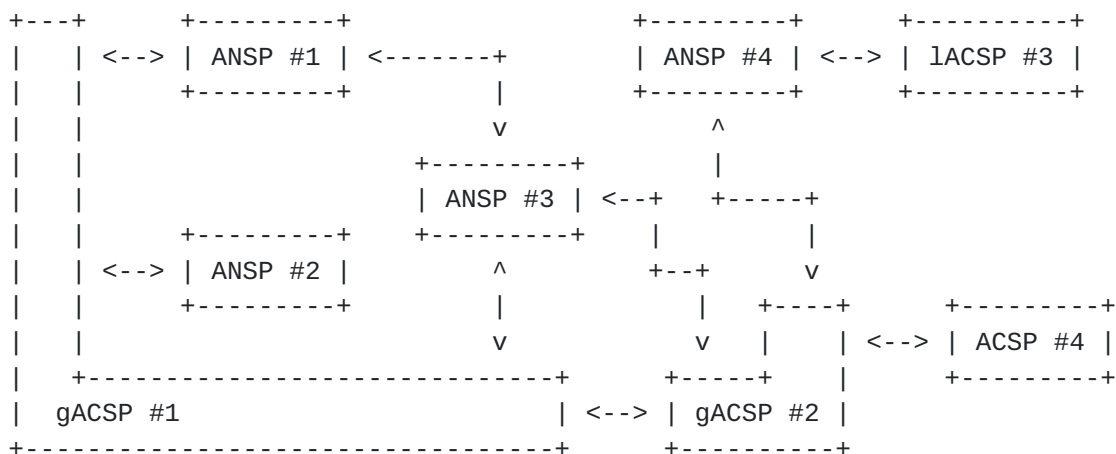


Figure 1: Global topology of the ATN.

The topology shown in Figure 1 is not representing the current real structure of the ATN, it is merely trying to show the basic hierarchical and interconnection layout. The prefixes 'g' and 'l'

before ACSP refer to global and local ACSPs respectively, whereas a missing prefix indicates that this ACSP can be either global or local. The difference between local and global is further elaborated below.

At the borders of ACSP and ANSP networks BGP routers are peering with each other and advertising routes. ANSPs have connections to other ANSP network(s) and to at least one gACSP.

It is important to note that ACSP access networks can be either local or global. An example for a local ACSP is an airport data link operated by the airport company (e.g. lACSP #3 in the figure), although this is not existing by the time this was written. As of today, two global ACSPs (gACSP #1 and gACSP #2) exist which have a world-wide network; they are comparable to the tier 1 service providers in the Internet. An ANSP can reach every other ANSP via these ACSPs in case they do not have a peering with each other or if there is no route over other ANSPs. ACSP #4 could be either local (airport) or global (not directly part of the ATN but interconnected via a gACSP).

It should also be mentioned that the direct interconnections between the ANSPs are, at the moment, only used for ground-ground communications and it is not yet clarified whether these connections might also be usable for the purpose of transit services/data forwarding of air-ground communications in the future.

Although at the moment planning only foresees ANSPs being connected to a single gACSP, it is possible that in the future a connection to more than one gACSP will be available (site multihoming as for ANSP #3 in the figure).

Redundancy, at least for ATS, is an important topic: it is not just limited to redundant routers, but also includes redundant lines (from a physical).

4.3. Points of Attachment

Basically an aircraft can attach to either an ACSP or an ANSP access network. There are three possibilities for how this attachment may look like and how it affects the routing path between MR and CN. The figures below show the direct routing path between the communication peers. In combination with Figure 1 this should allow to illustrate the the different possible paths implied by a certain RO solution, as well as the implications and limitations due to the placement of the functional RO entities.

4.3.1. ATS

The routing paths in the Figures below only depict ATS traffic, where the CNs are located inside the ANSP access network.

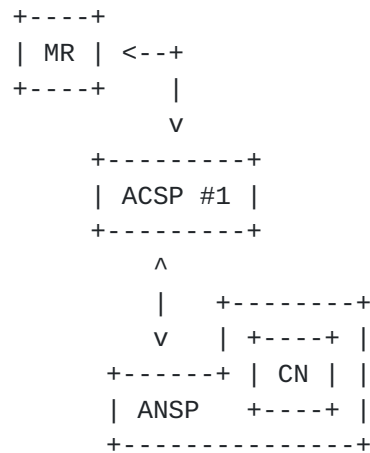


Figure 2: MR-CN communication via an ACSP.

Figure 2 shows a deployment that already exists today (not IP based though). The ANSP is not operating the access network in his country himself but contracts an ACSP for providing connectivity to aircraft. The data traffic from the MR flows through an access router of the ACSP and then, possibly via additional hops inside the ACSP, goes to the boundary router located at the ANSP where the packets are forwarded to the CN that resides inside this network.

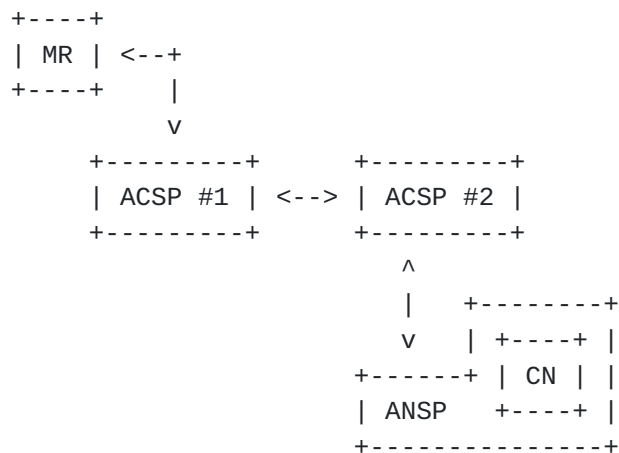


Figure 3: MR-CN communication via two ACSPs.

Figure 3 shows another potential deployment where the ACSP the aircraft is attached to is not directly connected to the ANSP. Routing between the MR and the CN is achieved by means of a transit

provider such as ACSP #2.

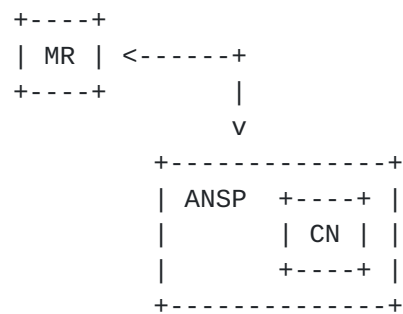


Figure 4: MR-CN communication directly via ANSP.

The option shown in Figure 4 is another existing deployment. The ANSP is operating its own access network to which aircraft can attach to. In this case the ANSP is also a local ACSP. Although the infrastructure might be provided by the ACSP, it is owned by the ANSP and therefore also under administrative control of the latter (and therefore topologically a part of the ANSP network).

[4.3.2.](#) AOS

The routing paths in the figures below depict AOS traffic only, where the CN might be located at the airline headquarters, the destination airport or somewhere else. The communication model is significantly different from ATS where the CNs change from time to time and are geographically close to the MR; for AOS the rate of CN changes is lower and the geographical distance can also be larger.

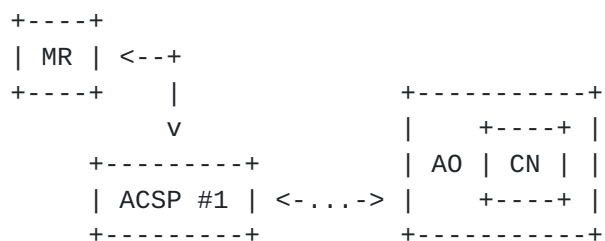


Figure 5: MR-CN communication with access router at the ACSP.

The scenario in Figure 5 is similar to that presented in Figure 2 where the aircraft attaches to an ACSP access network and the traffic is directly routed to the CN. The location of this node is in general usually in a subnet that belongs to the airline, and the routing path from ACSP #1 to the CN could be direct (subnet of CN is directly connected to ACSP #1). The dots in this figure (and the subsequent ones) indicate that several networks/operational domains could be between ACSP #1 and AO. For example this could be even

further generalized into having the possibility that the ACSP the MR attaches to is a local ACSP that in turn is only connected to a gACSP. In this case, the routing path would be MR -> lACSP -> gACSP -> AO -> CN.

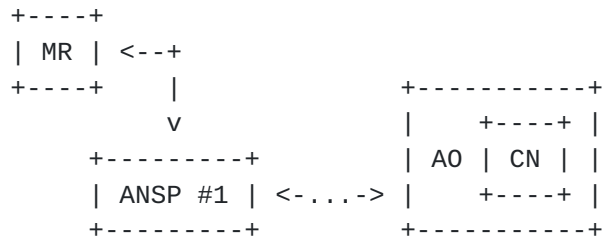


Figure 6: MR-CN communication with access router at the ANSP.

Figure 6 is based on Figure 4 with the MR attaching to an access network that is operated by an ANSP. The number of hops between the ANSP and the CN is not fixed, as there might be additional networks in between, e.g. if the airline contracts an lACSP to provide connectivity for the subnet the CN is connected to.

4.4. Location of Home Agents

As of now, there are no requirements by ICAO on where Home Agents should be located. There are basically two options:

1. An airline has a HA which is serving aircraft belonging to that airline.
2. One of the global ACSPs provides HA(s) for the airline if they have an agreement with them.

The solution with the gACSP as Mobility Service Provider is inline with the current business model. While airlines are not paying anything to ANSPs for communication services, there is a business contract between an airline and an ACSP for using the access networks for transmitting AOS packets.

Nevertheless it is also possible that (large) airlines might act as their own Mobility Services Provider operating Home Agents themselves, something that could become likely for airlines that do not have AOS communications and therefore no contract to a gACSP.

4.5. Trust Relationships

The basic trust model is comparable to the "Public Wireless Network with an Operator" model that is presented in [[RFC3756](#)], with aircraft being "client nodes". Aircraft can trust the infrastructure as

Aeronautical Communication Service Providers are certified, but other aircraft might be compromised and/or misbehave.

As can be seen from [Section 4.2](#), the two global ACSPs (as of today) are playing an important role. Both ANSPs and airlines have commercial contracts with (at least one of) them. Certificates can be assumed between the aircraft and the ACSP, at least for the one that the airline has a contract with.

The relationship between aircraft and ANSP - including ATS CNS within this network - is different, as these parties do not have commercial contracts with each other. Although there is some form of trust (the aircraft trusts the instructions coming from an ATSU), it is difficult to extend it on having certificates between these entities for the near future. Discussions related to a world-wide 'end-to-end' PKI for aviation are currently in progress, but no timeplan is available as of now. Having certificates between the aircraft and all potential CNS within ANSP networks is therefore difficult to answer with a clear 'yes', although in the very long term such a PKI is supposed to exist, albeit problems with these certificates are still possible (e.g. lack of participation of certain countries).

It should be noted that ANSPs often have their own additional local (network) policies that might impose restrictions (e.g. blocking of ICMP messages). In this case performing R0 might prove to be problematic, but still an optimized path has to be established as communication services between the aircraft and the CN have to be provided (that meet the delay requirements).

In addition some ANSPs even have the policy of not allowing encrypted traffic inside their network. It is also worth noting that in the future ANSPs, at least in Europe, will have to provide communication services to all equipped aircraft, independent of their contractual status with any of the ACSPs. This is complicating the basic trust model mentioned in the beginning as authenticating the aircraft (e.g. on layer 2) might become difficult to realize.

The situation between an aircraft and its AOS CNS is different, as both are operated by the same entity. Certificates between these nodes could be expected, and are partially already available today (e.g. X.509 certificates at application layer).

5. ATN Applications

In the following we provide an overview of ATS and AOS applications.

5.1. ATS Applications

5.1.1. Current State

The Controller Pilot Data Link Communications (CPDLC) is used for communication between the Air Traffic Controller and the cockpit. The application layer message exchange is shown in Figure 7, as currently used in Europe [[link2000manual](#)].

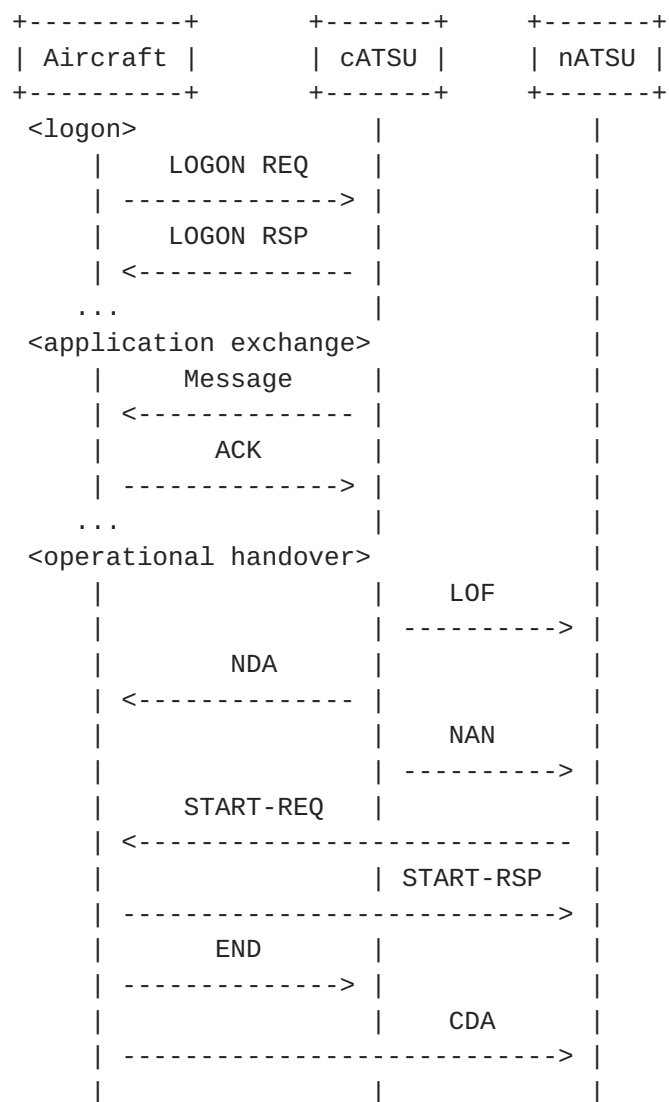


Figure 7: CPDLC communications for ATS.

The communication model is as follows: the aircraft has to perform a

logon procedure to the ATSU (Logon Request and Logon Response). Afterwards, the ATSU has flight data available and can unambiguously identify the aircraft with the help of locally available information.

Application message exchanges can be initiated by either the aircraft or the ATSU. They are usually completed with an Acknowledgement from the aircraft.

With the aircraft moving to airspace that is controlled by another ATSU, an operational handover is performed. The current ATSU (cATSU) forwards aircraft logon context information via the Log-On Forwarding (LOF) message to the next ATSU (nATSU) over the ground network. Afterwards the cATSU sends a Next Data Authority (NDA) message to the aircraft that authorizes the incoming connection request from the nATSU, followed by a NAN message to the nATSU that triggers the START-Request message. The aircraft confirms by means of a START-Response message. The END message from the aircraft to the cATSU then informs the old ATSU (cATSU) of session termination. The Current Data Authority (CDA) message from the aircraft to nATSU confirms the authority transfer.

5.1.2. Deployment

While basically there are several ATSUs per ANSP/country, the two currently deployed systems where CPDLC is in operational use both rely on a centralized model. This means that from the network layer perspective there is only a single ATN end system (CN). This end system acts as a application layer gateway distributing the information flow to the 'real' end systems.

This model is not mandated by anyone, the decision on how to deploy CPDLC is up to the ANSP. It is likely to assume that in the future there will be deployments with one ATN end system per ATSU (decentralised).

5.1.3. Future Architecture (SWIM)

There are currently ongoing efforts on defining future applications within the scope of various System Wide Information Management (SWIM) efforts. However, at the current stage it is too early to provide useful information related to application architecture and signalling.

5.2. AOS Applications

Airline communications is different as the communication peers of the aircraft are not so frequently changing as in ATS.

5.2.1. Current State

A variety of communications protocols are in use for AOS, such as the Aircraft Communication Addressing and Reporting System, (ACARS), VDL Mode 2 (also used by CPDLC) and even IP based access networks for certain applications.

In general, the communication procedure is similar to that of ATS: the aircraft first performs a log-on operation and only then information between the communication peers is exchanged. A generic diagram of the exchanged signalling is shown in Figure 8. Note that the logon procedure can also be implemented as an IPsec tunnel establishment.

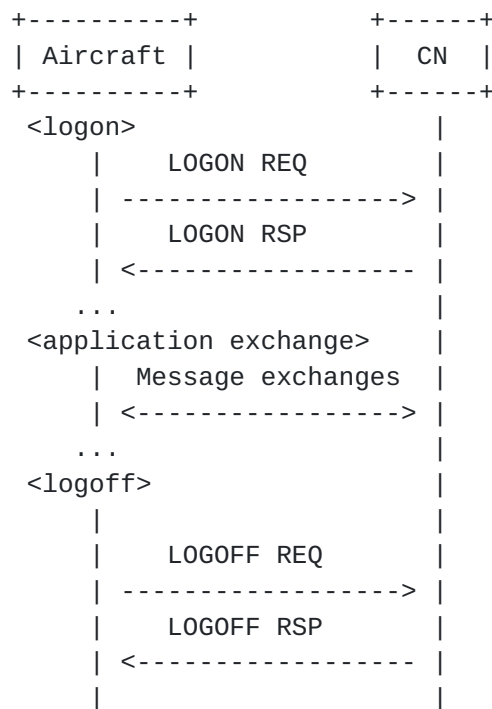


Figure 8: Old AOS communications.

5.2.2. Future Architecture (AGIE)

There is currently an effort in an aeronautical SDO in defining a common interface for application information exchanges between an aircraft and ground-based airline systems [[agiedraft](#)]. The architecture consists of an airborne proxy and a ground gateway and provides store-and-forward semantics with TCP as transport protocol. FTP is used for large file transfers.

Signalling is shown in Figure 9. The airborne client/applications/end systems register with the aircraft proxy. In case data has to be

transmitted to the ground, the client will inform the proxy about its data transfer intent via a Downlink Request message. The proxy then retrieves the files from the client and indicates the successful completion of the data transfer. The proxy then sends a Downlink Request message to the Ground Gateway, followed by the transfer of the data itself via the Downlink message. The gateway then indicates the availability of new data to the CN on the ground that can then retrieve the files. As soon as the CN received all files, a cascade of Downlink Response messages is returned to the airborne client.

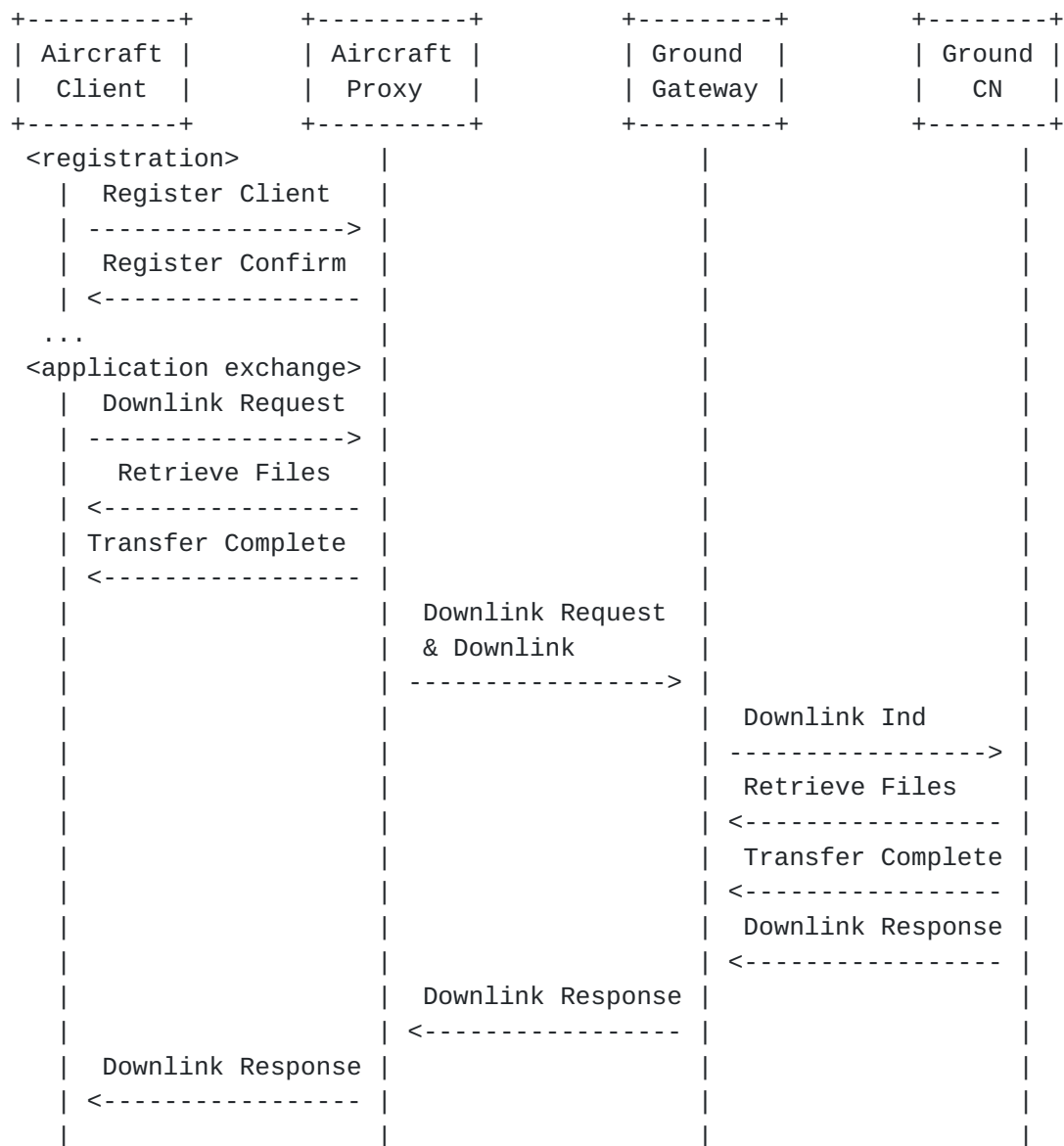


Figure 9: AGIE-based AOS communications.

The procedure for uplink messages, that is sending data from the ground to airborne end systems, is similar.

Connections are not end-to-end as end systems only establish connections with proxy and gateway respectively. Proxy and gateway posses caching capabilities for enabling store-and-forward behaviour, e.g. if a preferred link is not available, the proxy can delay sending data to the ground.

Both gateway and ground client use X.509v3 certificates for mutual authentication within TLS.

It should be noted that the information provided above is based on a draft version of the AGIE.

6. Security Considerations

This document only presents information related to aeronautical information systems. There are no security issues in this document.

7. Acknowledgements

Special thanks to Eivan Cerasi and Wesley M. Eddy for suggestions to improve this document.

We would also like to thank (in alphabetical order) Max Ehammer, Klaus-Peter Hauf and Phil Platt for their comments and related discussions.

The authors have been partially supported by the European Commission through the NEWSKY project. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NEWSKY project or the European Commission.

8. Changes from -00

Slightly restructured document and included information on access technologies and applications.

9. References

9.1. Normative References

- [I-D.ietf-mext-aero-reqs]
Eddy, W., Ivancic, W., and T. Davis, "Network Mobility Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks", [draft-ietf-mext-aero-reqs-04](#) (work in progress), August 2009.
- [RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.
- [RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", [RFC 4885](#), July 2007.
- [RFC4889] Ng, C., Zhao, F., Watari, M., and P. Thubert, "Network Mobility Route Optimization Solution Space Analysis", [RFC 4889](#), July 2007.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", [RFC 5213](#), August 2008.

9.2. Informative References

- [agiedraft]
AEEC, "Aircraft/Ground Information Exchange (AGIE) Specification", Project Paper 830 ANFS Munich draft, December 2008.
- [icao9705]
ICAO, "Manual of Technical Provisions for the Aeronautical Telecommunications Network (ATN)", Third Edition, June 2002.
- [icao9896]
ICAO, "Manual for the ATN using IPS Standards and Protocols (Doc 9896)", 1st edition (unedited), February 2009.
- [link2000]
Eurocontrol, "Link2000+ Network Planning Document", May 2007, <http://www.eurocontrol.int/link2000/gallery/content/public/files/documents/NPD_3.4.pdf>.
- [link2000manual]

Link2000+ Operational Focus Group, "ATC Data Link Manual
for Link 2000+ Services", May 2005.

Authors' Addresses

Christian Bauer
German Aerospace Center (DLR)

Email: Christian.Bauer@dlr.de

Serkan Ayaz
German Aerospace Center (DLR)

Email: Serkan.Ayaz@dlr.de