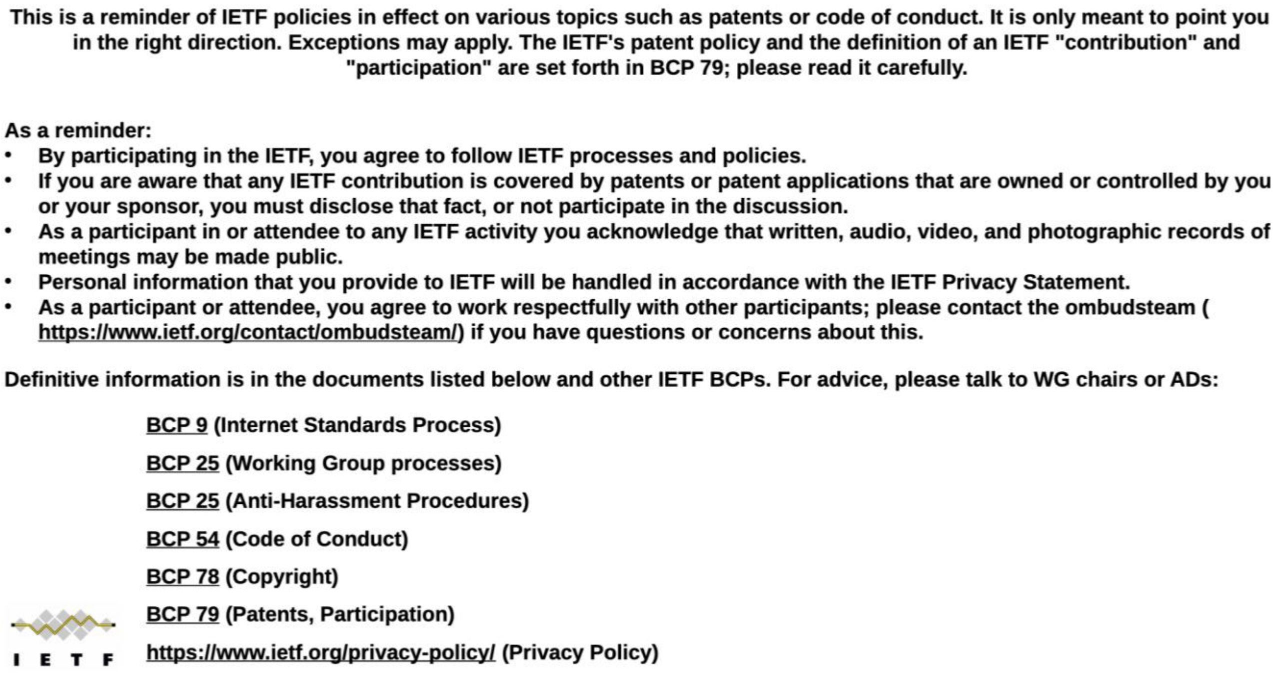
L-band Digital Aeronautical Communications System (LDACS)

draft-ietf-raw-ldacs-09

Nils Mäurer, Thomas Gräupl, Corinna Schmitt

Note Well



This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

BCP 9 (Internet Standards Process)

BCP 25 (Working Group processes)

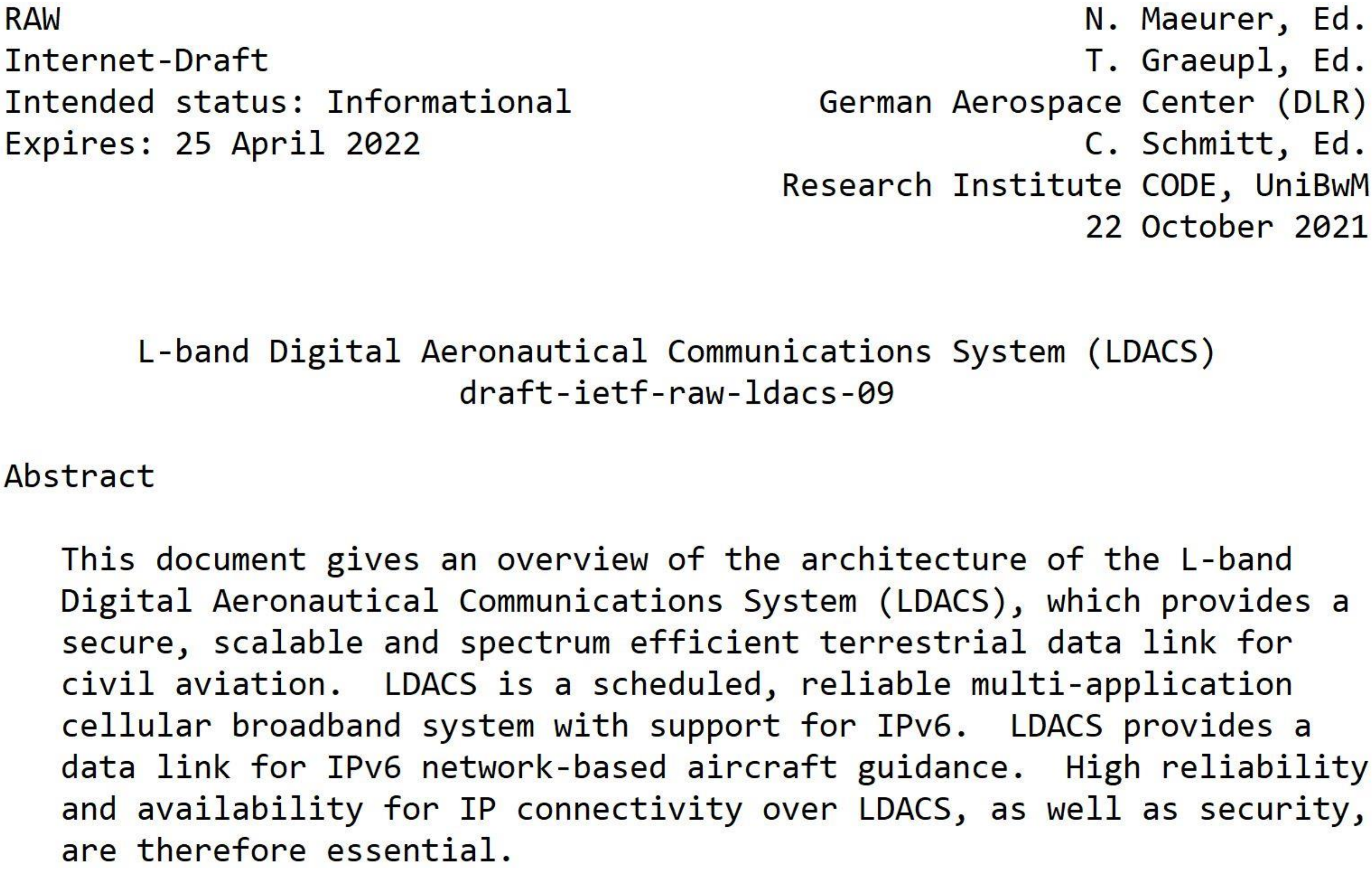
BCP 25 (Anti-Harassment Procedures)

BCP 54 (Code of Conduct)

BCP 78 (Copyright)

BCP 79 (Patents, Participation)

https://www.ietf.org/privacy-policy/ (Privacy Policy)



```
RAW                                                       N. Maeurer, Ed.
Internet-Draft                                            T. Graeupl, Ed.
Intended status: Informational         German Aerospace Center (DLR)
Expires: 25 April 2022                                    C. Schmitt, Ed.
                                        Research Institute CODE, UniBwM
                                                          22 October 2021
```

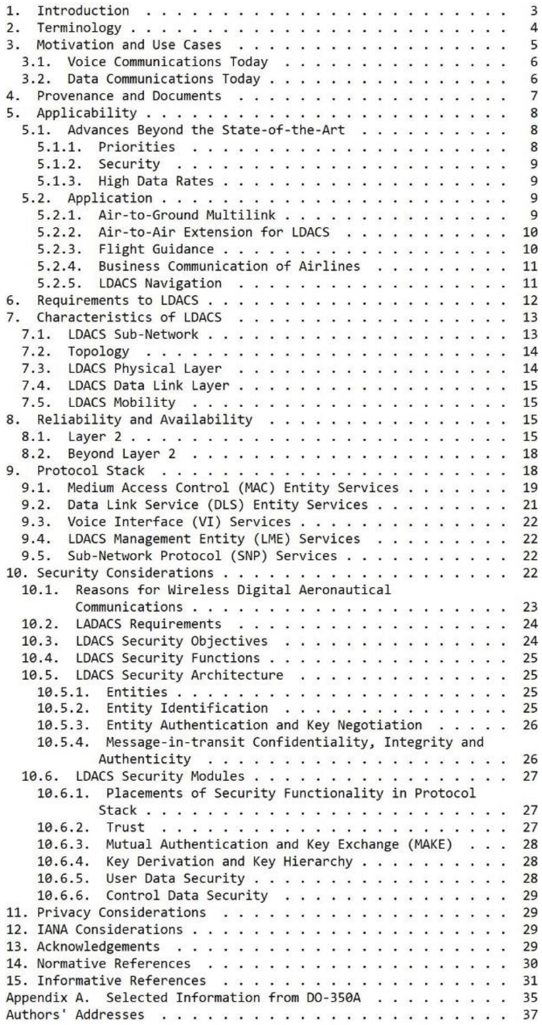
L-band Digital Aeronautical Communications System (LDACS)

draft-ietf-raw-ldacs-09

Abstract

This document gives an overview of the architecture of the L-band Digital Aeronautical Communications System (LDACS), which provides a secure, scalable and spectrum efficient terrestrial data link for civil aviation. LDACS is a scheduled, reliable multi-application cellular broadband system with support for IPv6. LDACS provides a data link for IPv6 network-based aircraft guidance. High reliability and availability for IP connectivity over LDACS, as well as security, are therefore essential.

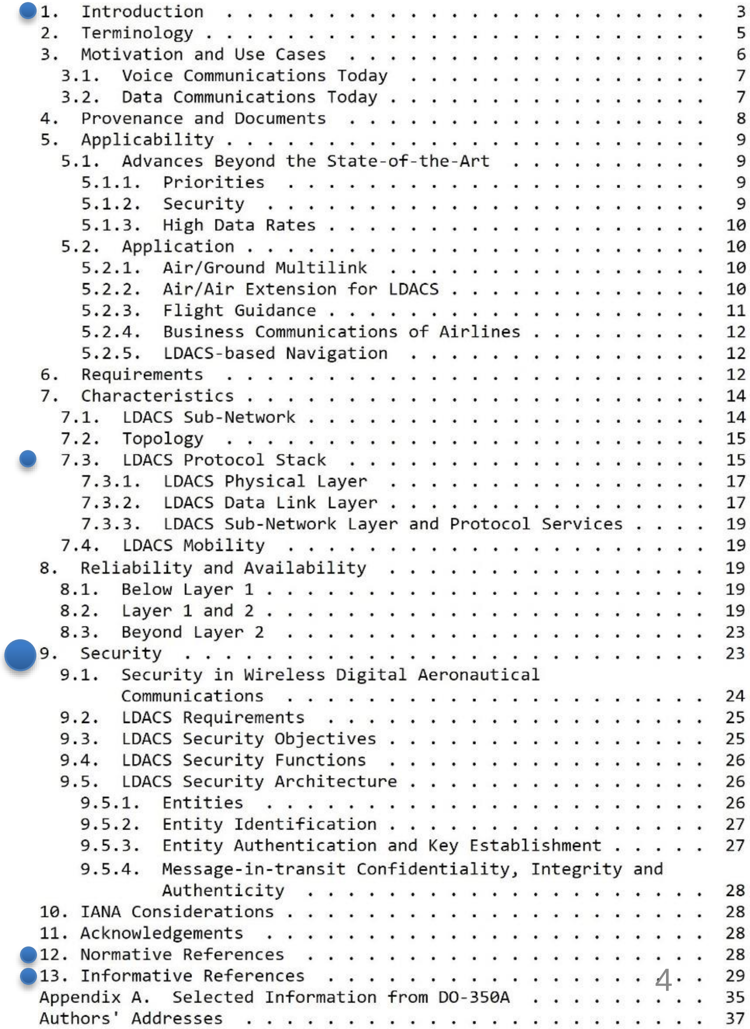
draft-ietf-raw-08 (IETF 111)



1. Introduction 3
2. Terminology 4
3. Motivation and Use Cases 5
3.1. Voice Communications Today 6
3.2. Data Communications Today 6
4. Provenance and Documents 7
5. Applicability 8
5.1. Advances Beyond the State-of-the-Art 8
5.1.1. Priorities 8
5.1.2. Security 9
5.1.3. High Data Rates 9
5.2. Application 9
5.2.1. Air-to-Ground Multilink 9
5.2.2. Air-to-Air Extension for LDACS 10
5.2.3. Flight Guidance 10
5.2.4. Business Communication of Airlines 11
5.2.5. LDACS Navigation 11
6. Requirements to LDACS 12
7. Characteristics of LDACS 13
7.1. LDACS Sub-Network 13
7.2. Topology 14
7.3. LDACS Physical Layer 14
7.4. LDACS Data Link Layer 15
7.5. LDACS Mobility 15
8. Reliability and Availability 15
8.1. Layer 2 15
8.2. Beyond Layer 2 18
9. Protocol Stack 18
9.1. Medium Access Control (MAC) Entity Services 19
9.2. Data Link Service (DLS) Entity Services 21
9.3. Voice Interface (VI) Services 22
9.4. LDACS Management Entity (LME) Services 22
9.5. Sub-Network Protocol (SNP) Services 22
10. Security Considerations 22
10.1. Reasons for Wireless Digital Aeronautical Communications 23
10.2. LADACS Requirements 24
10.3. LDACS Security Objectives 24
10.4. LDACS Security Functions 25
10.5. LDACS Security Architecture 25
10.5.1. Entities 25
10.5.2. Entity Identification 25
10.5.3. Entity Authentication and Key Negotiation 26
10.5.4. Message-in-transit Confidentiality, Integrity and Authenticity 26
10.6. LDACS Security Modules 27
10.6.1. Placements of Security Functionality in Protocol Stack 27
10.6.2. Trust 27
10.6.3. Mutual Authentication and Key Exchange (MAKE) 28
10.6.4. Key Derivation and Key Hierarchy 28
10.6.5. User Data Security 28
10.6.6. Control Data Security 29
11. Privacy Considerations 29
12. IANA Considerations 29
13. Acknowledgements 29
14. Normative References 30
15. Informative References 31
Appendix A. Selected Information from DO-350A 35
Authors' Addresses 37

Changes

draft-ietf-raw-09 (IETF 112)



1. Introduction 3
2. Terminology 5
3. Motivation and Use Cases 6
3.1. Voice Communications Today 7
3.2. Data Communications Today 7
4. Provenance and Documents 8
5. Applicability 9
5.1. Advances Beyond the State-of-the-Art 9
5.1.1. Priorities 9
5.1.2. Security 9
5.1.3. High Data Rates 10
5.2. Application 10
5.2.1. Air/Ground Multilink 10
5.2.2. Air/Air Extension for LDACS 10
5.2.3. Flight Guidance 11
5.2.4. Business Communications of Airlines 12
5.2.5. LDACS-based Navigation 12
6. Requirements 12
7. Characteristics 14
7.1. LDACS Sub-Network 14
7.2. Topology 15
7.3. LDACS Protocol Stack 15
7.3.1. LDACS Physical Layer 17
7.3.2. LDACS Data Link Layer 17
7.3.3. LDACS Sub-Network Layer and Protocol Services 19
7.4. LDACS Mobility 19
8. Reliability and Availability 19
8.1. Below Layer 1 19
8.2. Layer 1 and 2 19
8.3. Beyond Layer 2 23
9. Security 23
9.1. Security in Wireless Digital Aeronautical Communications 24
9.2. LDACS Requirements 25
9.3. LDACS Security Objectives 25
9.4. LDACS Security Functions 26
9.5. LDACS Security Architecture 26
9.5.1. Entities 26
9.5.2. Entity Identification 27
9.5.3. Entity Authentication and Key Establishment 27
9.5.4. Message-in-transit Confidentiality, Integrity and Authenticity 28
10. IANA Considerations 28
11. Acknowledgements 28
12. Normative References 28
13. Informative References 29
Appendix A. Selected Information from DO-350A 35
Authors' Addresses 37

Overall changes

- Adressed entire feedback from the Routing Directorate
- Clarified normative and informative references
- Streamlined work
- (Re-)Moved chapters to better fitting location in text
- Reworked LDACS security section
- Added post-quantum security to LDACS security

Chapter 1 – Introductions

- Transition from analogue to digital in aeronautical communications
  - Analogue to digital datalinks
  - Introduction of IPv6 based networking protocols

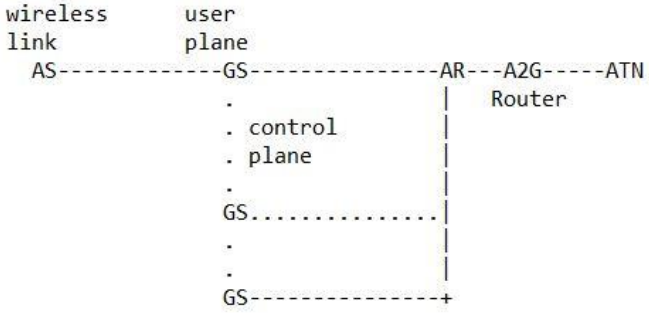
- Regulatory documents:
  - ICAO 9896 v03
  - RTCA DO-379
  - ARINC P-858
  - EUROCAE ED-262

- LDACS regarded as „access network“ in larger Aeronautical Telecommunications Network (ATN)/Internet Protocol Suite(IPS) framework

- Initial LDACS rollout in Europe

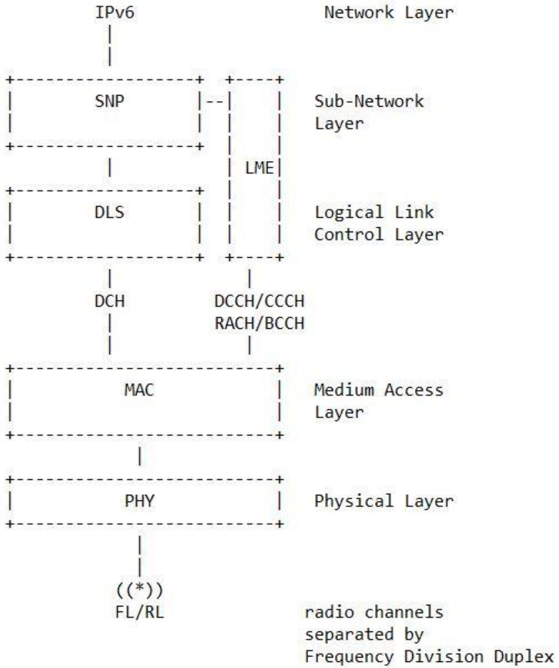
Chapter 7 – Characteristics

- Moved LDACS protocol stack details here



```
wireless      user
link          plane
  AS-------------GS---------------AR---A2G-----ATN
                 .                |    Router
                 .  control       |
                 .  plane         |
                 .                |
                 GS...............|
                 .                |
                 .                |
                 GS---------------+
```

LDACS sub-network



```
        IPv6                   Network Layer
         |
         |
+------------------+  +----+
|       SNP        |--|    |  Sub-Network
|                  |  |    |  Layer
+------------------+  |    |
         |            | LME|
+------------------+  |    |
|       DLS        |  |    |  Logical Link
|                  |  |    |  Control Layer
+------------------+  +----+
         |               |
        DCH         DCCH/CCCH
         |          RACH/BCCH
         |               |
+--------------------------+
|           MAC            |  Medium Access
|                          |  Layer
+--------------------------+
              |
+--------------------------+
|           PHY            |  Physical Layer
+--------------------------+
              |
              |
            ((*))
            FL/RL            radio channels
                             separated by
                             Frequency Division Duplex
```

LDACS protocol stack

Chapter 9 – Security

- Clarified view from regulatory documents:
  - LDACS is network access technology in ATN/IPS
  - RTCA DO-350A specifies 10s for RCP 130/A1 message types

- Presented user-/control data protection of LDACS

- LDACS PKI with corresponding certificates
  - AS certificates valid 3 years
  - GS certificates valid 1 day (sent via LDACS)
  - OCSP for certification revocation
  - CSP for certificate roll-out

Chapter 9 – Security

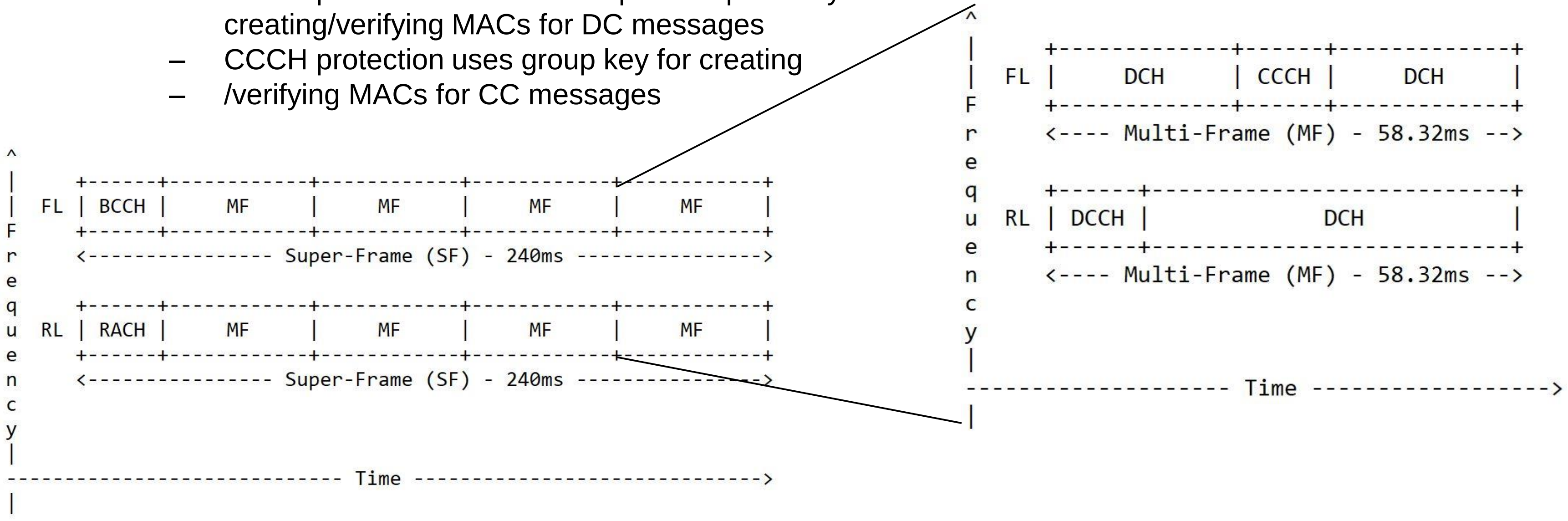
- LDACS cell-attachment procedure:
  - LDACS cell-entry procedure: basic communications enabled, security protocols and algorithms negotiated
  - LDACS Mutual Authentication and Key Establishment (MAKE) procedure: mutual authentication, key establishment derivation, group key establishment

- LDACS security levels
  - Pre-Quantum: Elliptic-curve based
  - Post-Quantum:
    - Supersingular Isogeny Key Encapsulation (SIKE) KEM
    - FALCON signature

- LDACS user-data protection
  - AES-CMAC for data integrity/authenticity only
  - AES-CCM for Authenticated Encryption with Associated Data (AEAD)

Chapter 9 – Security

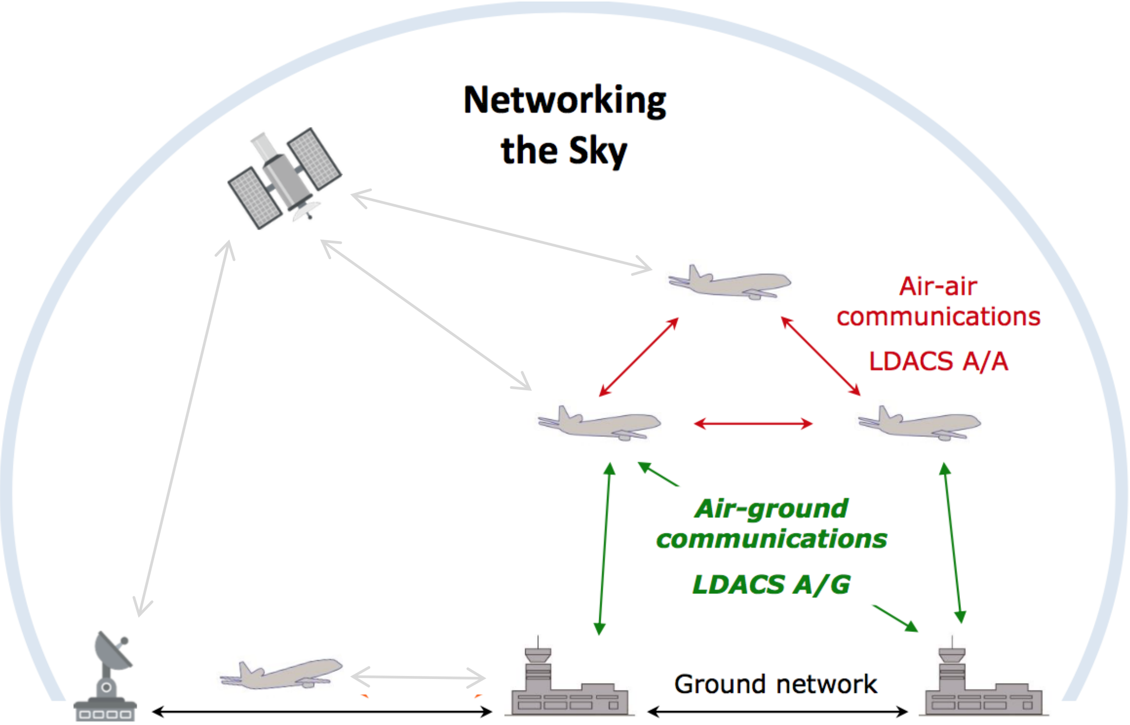
- LDACS control-channel protection:
  - No protection at RACH, BCCH
  - DCCH protection uses AS-GS point-to-point key for creating/verifying MACs for DC messages
  - CCCH protection uses group key for creating
  - /verifying MACs for CC messages



```
^
|     +-----+-----------+-----------+-----------+-----------+
|  FL | BCCH |    MF     |    MF     |    MF     |    MF     |
F     +-----+-----------+-----------+-----------+-----------+
r     <--------------- Super-Frame (SF) - 240ms --------------->
e
q     +-----+-----------+-----------+-----------+-----------+
u  RL | RACH |    MF     |    MF     |    MF     |    MF     |
e     +-----+-----------+-----------+-----------+-----------+
n     <--------------- Super-Frame (SF) - 240ms --------------->
c
y
|
-------------------------- Time ------------------------------>
|
```

```
^
|     +-------------+------+-------------+
|  FL |     DCH     | CCCH |     DCH     |
F     +-------------+------+-------------+
r     <---- Multi-Frame (MF) - 58.32ms -->
e
q     +------+---------------------------+
u  RL | DCCH |            DCH            |
e     +------+---------------------------+
n     <---- Multi-Frame (MF) - 58.32ms -->
c
y
|
------------------- Time ------------------>
|
```

Thanks


Networking
the Sky
Air-air
communications
LDACS A/A
Air-ground
communications
LDACS A/G
Ground network