ICAO

Doc 10044

Manual on the Aeronautical Mobile Airport Communications System (AeroMACS)

Disclaimer

This document is an unedited version of an ICAO publication and has not yet been approved in final form. As its content may still be supplemented, removed, or otherwise modified during the editing process, ICAO shall not be responsible whatsoever for any costs or liabilities incurred as a result of its use.

First Edition (advance unedited) — 2017

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard,
Montréal, Quebec, Canada H3C 5H7

For ordering information and for a complete listing of sales agents
and booksellers, please go to the ICAO website at www.icao.int

Doc 10044, AN/514
Order Number: xxx
ISBN xxx-xx-xxxx-xxx-x

.

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

FOREWORD

The purpose of this manual is as follows:

a) to provide guidance on the implementation and management of a mobile airport communications system (AeroMACS) and;

b) to specify technical provisions for AeroMACS to ensure compliance with the requirements of the AeroMACS Standards and Recommended Practices (SARPs) (Annex 10, Volume III, Chapter 7) and achieve global interoperability.

The guidance material is provided in Chapter 2 whereas the technical provisions are provided in Chapter 3.

_____

TABLE OF CONTENTS

Page

TABLE OF FIGURES

LIST OF TABLES

GLOSSARY

TERMS AND ABBREVIATIONS

Access service network (ASN). A system comprised of an access gateway providing an IP interface and at least one base station (BS).

Adaptive modulation. An ability to change modulation and data rate to adapt to changing signal to noise or other environmental conditions to maintain connectivity with the peer entity.

Aerodrome. A defined area on land or water (including any buildings, installations and equipment) intended to be used either wholly or in part for the arrival, departure and surface movement of aircraft.

AeroMACS. Aeronautical mobile airport communications system.

AeroMACS downlink (DL). The transmission direction from the base station (BS) to the subscriber station (SS).

AeroMACS uplink (UL). The transmission direction from the subscriber station (SS) to the base station (BS).

AeroMACS handover. The process in which a subscriber station (SS) migrates from the air-interface provided by one base station (BS) to the air-interface provided by another BS.

AeroMACS subnetwork. A system comprising the subscriber stations (SSs), at least one base station (BS) and the access service network – gateway (ASN-GW) and all other elements in between.

Base station (BS). A generalized equipment set providing connectivity, management, and control of the subscriber stations (SSs).

Bit error rate (BER). The number of bit errors in a sample divided by the total number of bits in the sample, generally averaged over many such samples.

Carrier to interference plus noise ratio (CINR). A measure expressed in decibels, the ratio between the power of the wanted Carrier and the total power of the interference and thermal noise.

Convolutional codes. A type of forward error correction (FEC) code.

Data transit delay. In accordance with ISO 8348, the average value of the statistical distribution of data delays from the time that the data enters the AeroMACS subnetwork until the data exits the AeroMACS subnetwork. This delay does not include the network entry time.

Differentiated services code point (DSCP): A field in an IP packet that enables different levels of service to be assigned to network traffic.

Forward error correction (FEC). The process of adding redundant information to the transmitted signal in a manner which allows correction, at the receiver, of errors incurred in the transmission.

Frequency assignment. An allocation of centre frequencies to base stations (BSs).

Home-network service provider (H-NSP). A network service provider which is responsible for the authentication of the subscriber station for access to the subnetwork. *See also NSP*.

Mobile station (MS). A station intended to be used while in motion or during halts at unspecified points. An MS is always a subscriber station (SS).

Multicast and broadcast service (MBS). A method by which a BS transmit to all or a select group of SSs within its range.

Multicast and broadcast service group security association (MBSGSA). A method for providing authentication and encryption when using multicast and broadcast services.

Multiple-input multiple-output (MIMO). A system with plural antennas to improve the system coverage or throughput.

Network access provider (NAP). NAP is a business entity that provides radio access infrastructure.

Network service provider (NSP). NSP is a business entity that provides IP connectivity and services to users compliant with the service level agreement. From a user's standpoint, an NSP is classified as either a home NSP (H-NSP) or a visited NSP (V-NSP).

Note.— An NSP can also establish roaming agreements with other NSPs and contractual agreements as appropriate with third-party application providers (e.g. ASP or ISPs) for providing services to users.

Orthogonal frequency division multiplexing (OFDM). Orthogonal frequency-division multiplexing is a method of digital modulation in which a signal is split into several narrowband channels at different frequencies.

OFDM symbol. A waveform with a given amplitude and phase that persists for a fixed period of time representing an integer number of bits.

Partial usage subchannelization (PUSC). A technique in which the orthogonal frequency division multiplexing (OFDM) symbol subcarriers are divided and permuted among a subset of subchannels for transmission, providing partial frequency diversity.

Service data unit (SDU). A unit of data transferred between adjacent layer entities, which is encapsulated within a protocol data unit (PDU) for transfer to a peer layer.

Service flow. A unidirectional flow of media access control layer (MAC) service data units (SDUs) on a connection that is providing a particular quality of service (QoS).

Subscriber station (SS). An equipment set providing connectivity between user equipment and a base station (BS).

Subnetwork entry time. The time from when the subscriber station starts the scanning for BS transmission, until the link is established, and the first network user "protocol data unit " can be sent.

Subnetwork service data unit (SNSDU). An amount of subnetwork user data, the identity of which is preserved from one end of a subnetwork connection to the other.

Time division duplex (TDD). A duplex scheme where uplink and downlink transmissions occur at different times but may share the same frequency.

Visited-network service provider (V-NSP). A network service provider which provides a subscriber station with service, by authenticating the subscriber station through the Home-NSP. *See also NSP.*

WMF. WiMAX Forum.

_____

LIST OF ACRONYMS

A

A-SMGCS	Advanced surface movement guidance and control system
AAA	Authentication, authorization and accounting
AAC	Airline administrative communications
ACARS	Aircraft communications addressing and reporting system
ACD	Aircraft control domain
ACM	ATC communications management
ACMS	Aircraft condition monitoring system
ACSP	Aeronautical communication service provider
ADCC	Aviation Data Communications Corporation
ADS	Automatic dependent surveillance
ADS-B	Automatic dependent surveillance — broadcast
ADS-C	Automatic dependent surveillance — contract
AEEC	Airlines Electronic Engineering Committee
AeroMACS	Aeronautical mobile airport communication system
AF	Assured forwarding
AISD	Airline information services domain
AMC	Adjacent multi-carrier
AM(R)S	aeronautical mobile (route) service
AMT	Aeronautical mobile telemetry
ANSP	Air navigation services provider
AOA	Air operations area
AOC	Aeronautical operational control
AP	Action Plan
APPA	AeroMACS PKI policy authority
APT	Aeroport
AR	Access router
ARINC	Aeronautical Radio, Incorporated
ARU	AeroMACS radio unit
ASDE	Aeroport surface detection equipment
A-SMGCS	Advanced surface movement guidance and control systems
ASN	Access service network
ASP	Application service provider
ATC	Air traffic control
ATCT New	Air traffic control tower new
ATCT Old	Air traffic control tower old
ATIS	Automatic terminal information service
ATM	Air traffic management
ATM	Asynchronous transfer mode
ATN	Aeronautical telecommunication network
ATS	Air traffic services
ATSU	Air traffic services unit
AVICOM	AVICOM Japan Inc.
AVS	Advisory services
AWAS	Automated weather advisory system

B

BER	Bit error rate
BE	Best effort
BGP	Boundary gateway protocol
BIT	Built-in testing
bps	Bits per second
BS	Base station

C

CA	Certificate authority
CAC	Call admission control
CAA	Civil aviation administration
CDG Airport	Charles de Gaulle Airport
CDMA	Code division multiple access
CID	Connection ID
CINR	Carrier to interference plus noise ratio
CIS	Clearance/instruction services
CMC	Central maintenance computer
CMS	Centralized maintenance system
CN	Correspondent node
CNPC	Control and non-payload communications
CNS	Communications, navigation, and surveillance
CoA	Care of address
COM	Communications
COTS	Commercial off-the-shelf
CP	Certificate policy
CPDLC	Controller-pilot data link communications
CPS	Certification practice statement
CR	Correspondent router
CRL	Certificate revocation list
CS	Convergence sublayer
CSA	Certificate status authority
CSN	Connectivity service network
CSP	Communication service provider

D

D-ATIS	Data link — automatic terminal information service
DCM	Data communication management services
DF	Default forwarding
DHCP	Dynamic host configuration protocol
DiffServ	Differentiated service
DL	Downlink
DLR	German Aerospace Centre (Deutsches Zentrum Für Luft Und Raumfahrt)
DMZ	De-militarized zone
Doc	Document
D-OTIS	Datalink operational terminal info service
D-RVR	Digital runway visual range
DSA	Dynamic service addition

DSCP	Differentiated services code point
D-SIGMENT	Digital significant meteorological information
DSS	Delegated separation services
D-TAXI	Data link - taxi

E

EAP	Extensible authentication protocol
ECN	Explicit congestion notification
EF	Expedited forwarding
EFB	Electronic flight bag
EIRP	Equivalent isotropically radiated power
EMI	Electromagnetic interference
ertPS	Expedited real-time polling service
EUROCAE	European Organisation for Civil Aviation Equipment
EUROCONTROL	European Organisation for the Safety of Air Navigation

F

FA	Foreign agent
FAA	Federal Aviation Administration
FBO	Fixed base operator
FBSS	Fast-base station switching handover
FCC	Federal Communications Commission
FCI	Future communication infrastructure
FIFO	First in – first out
FIPS	Federal information processing standard
FIS	Flight information service
FMS	Flight management system
FOC	Flight operational control
FOD	Foreign object debris
FPS	Flight position/intent preference services
FSS	Fixed satellite service
FWC	Failure warning computer

G

GKEK	Group key encryption key
GNSS	Global navigation satellite system
GPCS	Generic packet convergence sublayer
GRE	General routing encapsulation
GSA	Group security association
GTEK	Group traffic encryption key

H

HA	Home agent
HARQ	Hybrid automatic request repeat
H-NSP	Home-network service provider
HO	Handover

I

IANA	Internet assigned numbers authority
ICAO	International Civil Aviation Organization
ID	Identification
IEEE	Institute of Electrical and Electronics Engineer
IETF	Internet Engineering Task Force
IMS	IP multimedia subsystem
Inmarsat	Inmarsat Ltd.
IntServ	Integrated service
IP	Internet protocol
IPS	Internet protocol suite
IPSEC	Internet protocol security
ITU	International Telecommunication Union

J

JFK Airport	John F. Kennedy Airport

L

LAN	Local area network
LEO	Low earth orbit
LIR	Local internet registry
LOS	Line of sight
LRUS	Line replacement units

M

MAC	Media access control
MAK	Multimedia multicast/broadcast service authentication key
MASPS	Minimum aircraft system performance specification
MBS	Multicast and broadcast service
MDHO	Macro-diversity handover
MGSGSA	MBS group security association
MGTEK	Multicast/broadcast service group traffic encryption key
MCDU	Multi-purpose display unit
MIB	Management information base
MIMO	Multi-le-input multiple-output
MIP	Mobile IP
MIS	Miscellaneous services
MLS	Microwave landing system
MLAT	Multilateration

MOPS	Minimum operational performance standards
MPDU	MAC protocol data unit
MR	Mobile router
MS	Mobile station
MSK	Minimum shift keying
MSP	Mobility service provider
MTC	Multicast traffic connection
MTK	Mobile broadcast multicast service traffic key

N

NAP	Network access provider
NASA	National Aeronautics and Space Administration
NAVAID	Navigation aid
NET	Network control/management
NextGen	Next generation
NF	Noise figure
NOTAM	Notice to airmen
NRM	Network reference model
nrtPS	Non-real-time polling service

O

OEP	Operational evolution partnership
OET	(FCC) Office of Engineering & Technology
OFDM	Orthogonal frequency division multiplexing
OFDMA	Orthogonal frequency-division multiple access
OID	Object ID
OOOI	Off/out/on/in
OSI	Open systems interconnection

P

PC	Personal computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal digital assistant
PDU	Protocol data unit
PF	Policy function
PHB	Per-hop behaviours
PHS	Payload header suppression
PHSF	Payload header suppression field
PHSI	Payload header suppression index
PHSM	Payload header suppression mask
PHSS	Payload header suppression size
PHSV	Payload header suppression valid
PIESD	Passenger information and entertainment services domain
PIREPS	Pilot reports
PKI	Public key infrastructure
PKMv2	Private key managementv2
PMIP	Proxy mobile IP
PMP	Point to multi-point
PODD	Passenger owned devices domain

POP	Point of presence
PTT	Press to talk

Q

QAM	Quadrature amplitude modulation
QoS	Quality of service
QPSK	Quadrature phase shift keying

R

RBW	Resolution bandwidth
RRC	Radio resource control
R&D	Research and development
RF	Radio frequency
RFI	Radio frequency interference
RIR	Regional internet registry
RNSS	Radio navigation satellite systems
ROHC	Robust header compression
RP	Reference point
RPAS	Remotely piloted aircraft systems
RRM	Radio resource management
RSA	Ron Rivest, ADI Shamir, Leonard Adleman (an encryption scheme)
RSSI	Received signal strength indicator
RTCA	RTCA, Inc. (an industry standards-making organization)
rtPS	Real-time polling service

S

SA	Security association
SAID	Security association ID
SAP	Service access points
SARPs	Standards and Recommended Practices
SATCOM	Satellite communication
SBB	“SWIFT” broadband
SDU	Service data unit
SESAR	Single European Sky ATM Research
SF	Service flow
SFA	Service flow authorization
SFID	Service flow identifier
SFM	Service flow management
SITA	Société internationale de télécommunications aéronautiques
SLA	Service level agreement
SMGCS	Surface movement guidance and control systems
SNMP	Simple network management protocol
SS	Subscriber station
SURV	Surveillance
SWIM	System wide information management

T

TCAS	Traffic alert and collision avoidance system
TCP	Transmission control protocol
Telco	Telecommunications
TIS-B	Traffic information service — broadcast
TLS	Transport layer security
TLV	Type, length, value

U

UAS	Unmanned aircraft systems
UAT	Universal access transceiver
UDP	Universal datagram protocol
UGS	Unsolicited grant service
UL	Uplink
UTC	Co-ordinated universal time
UUT	Unit under test

V

VDL	VHF digital link
VHF	Very high frequency
VLAN	Virtual local area network
VoIP	Voice over internet protocol
V-NSP	Visited-network service provider
VPN	Virtual private network

W

WG	Working group
WiMAX	Worldwide interoperability for microwave access
WMF	WiMAX Forum
WOI	Weather observation improvement
WOW	Weight-on-wheels
WRC	World Radiocommunication Conference
WXGRAPH	Graphical weather information

———————

REFERENCES

ICAO Publications

Annex 10 — *Aeronautical Telecommunications*, Volume III — *Communication Systems*, Chapter 7, AeroMACS SARPs, and Volume IV — *Surveillance and Collision Avoidance Systems*, sections 3.1.1.7.14.1 and 3.1.1.7.14.2, Volume V — *Aeronautical Radio Frequency Spectrum Utilization*

Annex 14 — *Aerodromes*, Volume I — *Aerodrome Design and Operations*

Doc 9137, *Airport Services Manual*

Doc 9157, *Aerodrome Design Manual*

Doc 9774, *Manual on Certification of Aerodromes*

Doc 9863, *Airborne Collision Avoidance System (ACAS) Manual*, section 3.5.2.1. "Multipath from terrain reflections"

Other Publications

[1] WMF-T23-001-R010v11, WiMAX Forum® Air Interface Specification, WiMAX Forum® Mobile System Profile.

[2] WiMAX Forum® AeroMACS Certification Requirements Status List (CRSL) Version 18.0.0

[3] WMF-T32-001-R010v05, WiMAX Forum® WiMAX Network Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Points) [Part 0]

[4] WMF-T33-001-R010v05, WiMAX Forum® Network Architecture (Stage 3: Detailed Protocols and Procedures), sections 4.2 and 4.8

[5] WMF-T24-003-R010v01, WiMAX Forum® AeroMACS Protocol Implementation Conformance Statement (PICS) Proforma

[6] AeroMACS Profile - Eurocae Document ED-222 and RTCA Document DO-345

[7] AeroMACS MOPS– Eurocae Document ED-223 and RTCA Document DO-346

[8] AeroMACS MASPS – Eurocae Document ED-227

[9] IEEE Standard 802.16-2009, IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Broadband Wireless Access Systems, May, 2009

———————

CHAPTER 1

GENERAL

1.1 Introduction

1.1.1 AeroMACS (aeronautical mobile airport communication system) is an ICAO standardized data link system aiming to support the communication exchanges dealing with the safety and regularity of flight operations in the aerodrome (airport) environment.

1.1.2 AeroMACS is based on IEEE 802.16 [9] and is a modern (fourth generation, 4G) mobile wireless communication system providing broadband connectivity on the airport surface. AeroMACS can support the integration of the safety and regularity of flight communications of aircraft operators, air navigation service providers and airports authorities by providing high bandwidth and prioritized communication exchanges over a common infrastructure dedicated to critical communication exchanges in the airport environment.

1.1.3 AeroMACS systems can operate in the 5 030 to 5 150 MHz band under the ITU allocation for AM(R)S type of services (offering protection from interference from unauthorized users of the band).

1.1.4 The AeroMACS Manual complements the AeroMACS Standards and Recommended Practices (SARPs) (Annex 10, Volume III) and aims to provide guidance to regulators, manufacturers and system integrators for the deployment and configuration of AeroMACS systems. The scope of the manual includes information on aspects such as the concept of operations, architecture specifications, security and guidelines on siting, frequency allocations and interfacing to AeroMACS components.

1.1.5 Chapter 1 of the manual covers an overview, some background information and key features of AeroMACS.

1.1.6 Chapter 2 contains the guidance material for issues typically arising in AeroMACS deployments such as applicable services, media access configuration, BS siting, frequency allocation, architecture and interfaces to network layers.

1.1.7 Chapter 3 of the manual describes the technical specifications that are required to achieve compliance with the AeroMACS SARPs (Annex 10, Volume III, Chapter 7) and global interoperability.

1.2 Background information

1.2.1 The recommendation for AeroMACS comes from the outcome of the EUROCONTROL and FAA/NASA coordination activity called Action Plan 17 (AP17), Future Communications Study, which outlined guidelines and recommendations for the operational requirements of the future communication infrastructure (FCI) composed of radio systems, networks and applications to support future aeronautical operations. AP17 estimated that the future operations are expected to generate significant data link throughput requirements which will increase heavily due to new applications being developed in R&D programmes such as SESAR and NextGen. Therefore, AP17 concluded that a new communications infrastructure will be required to support the future communication exchanges and

recommended that FCI needs to also include current systems (analogue voice and VDL Mode 2). AP17 recommended the introduction of three new data link systems: a new SATCOM system, a new terrestrial system, in particular for the en-route and terminal areas of operation, and a new system for the airport surface, in particular where the volume of the exchanges is expected to be more significant compared to other flight phases.

1.2.2 AeroMACS is the AP17 proposed FCI data link for the airport surface and delivers an IP high data rate radio link that support the ATN/IPS, to enable future services including:

a) air traffic services (ATS), which includes the safety critical communications related to aircraft;

b) aeronautical operational control (AOC), which include, airline communications between aircraft and the airline operational control centre which are linked to the safety or regularity of flight; and

c) airport authority communications that affect the safety and regularity of flight involving vehicles, ground services and sensors, lighting systems, runway/taxiway safety management equipment and radar.

1.2.3 The choice of AeroMACS, based on an open standard used for commercial communications (operating in other bands), highlights the underlying objective of aviation and ICAO in particular to capitalize on existing technologies and benefit of past development efforts. This approach leverages existing commercial off-the-shelf (COTS) industry products and relies on existing commercial standards such as internet protocol (Doc 9896) for aviation communications.

1.2.4 As a result of ITU WRC-07 Conference, AeroMACS received an AM(R)S allocation in the 5 GHz band and is, therefore, eligible to make use of the protected spectrum in the 5 GHz band for the safety of life and regularity of flight services.

1.3 AeroMACS overview

1.3.1 In summary, the potential benefits from using AeroMACS include:

a) higher throughput in airport surface communications;

b) providing relief on the congested VHF spectrum in airports;

c) worldwide interoperability and integration of critical coms for ANSPs, airspace users and airports;

d) synergies through the sharing of infrastructure;

e) increased security capabilities; and

f) support/enable reducing airport congestion and delays and enhancing situational awareness of controllers.

1.3.2 AeroMACS is an important data link for aviation as it is the first new pillar of a wider future aviation COM infrastructure used as a model for:

a) leveraging on commercial communication developments and technologies;

b) pooling synergies between ANSPs, airports and airlines;

c) handling the security issues of future aviation COM infrastructure; and

d) implementing IP data link on-board aircraft.

1.3.3 AeroMACS is a wideband wireless radio specification that enables cellular networking between a set of base stations (BSs) and mobile stations (MSs). The allowed radio channel bandwidth is 5 MHz. The waveform is based on orthogonal frequency division multiplexing (OFDM) modulation, which provides resistance to dispersive propagation environments, and an OFDMA media access scheme that allows point-to-multipoint transmission between a BS and multiple subscribers simultaneously with given quality of service (QoS). In addition to this, an adaptive modulation scheme is used in which throughput is gradually altered as propagation conditions change. For information, when 64 QAM modulation is used, throughput of approximately 7 Mbps in the downlink direction and approximately 5 Mbps in the uplink direction may be achieved. This will depend on system configuration and other conditions.

1.3.4 The MSs are part of the customer premise equipment embedded in the aircraft providing an IP interface for the airborne network. MSs can also be used in other vehicle types or handheld devices. BSs configure the cell planning, manage the channel assignment and access to the radio media in the cellular network. The access service network (ASN) consists of at least one BS and one ASN gateway. The ASN functional block is in charge of managing overall radio access aspects and provides an IP interface that facilitates the integration with the ATN network and services. AeroMACS security features include mechanisms for authentication, authorization and encryption that protects both the AeroMACS management information, as well as the user data carried by AeroMACS.

1.3.5 An AeroMACS system can potentially support a wide variety of IP data, video, and voice communications and information exchanges among mobile and fixed users at the airport. The airport communications, navigation, and surveillance (CNS) infrastructure that supports air traffic management (ATM) and air traffic control (ATC) on the airport surface can also benefit from secure wireless communications supporting improved integrity and diversity. A wideband communications network can enable sharing of graphical data and video to significantly increase situational awareness, improve surface traffic movement to reduce congestion and delays, and help prevent runway incursions. AeroMACS can provide temporary communications capabilities during construction or outages, and reduce the cost of connectivity. A broadband wireless communications system like AeroMACS can lead to enhanced collaborative decision making, ease updating of large databases, provide up-to-date weather graphics and aeronautical information (aeronautical information and meteorological services), enable aircraft access to system wide information management (SWIM) services and deliver time-critical advisory information to the cockpit.

1.3.6 Research and validation of the AeroMACS technology has been carried out by coordination of the EUROCAE WG-82 and RTCA SC-223 Working Groups. The result of this joint effort has led to the publication of an AeroMACS profile, stating the list of technical items mandated to be supported by the radio interface as referred to in the IEEE 802.16 Standard in order to guarantee radio interoperability. In addition, EUROCAE and RTCA jointly developed an AeroMACS minimum operational performance system (MOPS) specifying the functional features of the AeroMACS profile, and describing the environmental conditions and test cases required for aeronautical use. Finally, the AeroMACS minimum aircraft system performance specification (MASPS) by EUROCAE describes a set of system performance requirements and outlines possible implementation options (architectures, use cases) for AeroMACS.

1.3.7 A commercialized version of the IEEE 802.16 Standard is specified under the WiMAX brand and by the WiMAX Forum® (an industry-led, not-for-profit organization that certifies and promotes interoperability of products based on the IEEE 802.16 family of Standards) The WiMAX Forum in collaboration with the EUROCAE WG-82 and RTCA SC-223 Working Groups has also been supporting the standardization of AeroMACS. The WiMAX Forum Aviation Working Group has overseen the completion of the Protocol Implementation Conformance Statement (PICS) [4] and Certification Requirements Status List (CRSL) [2] documents.

1.3.8 Finally the ARINC Airline Electronics Engineering Committee (AEEC) is standardizing ARINC 766 to provide the form, fit and function characteristics for the AeroMACS airborne transceiver and interfaces with other systems on-board the aircraft.

1.4 Constraints, restrictions and limitations on AeroMACS use

1.4.1 This section summarizes the constraints associated with using AeroMACS on the airport surface. These constraints cover spectrum, services, aircraft application domains, velocity, airborne use and operation areas in the airport.

1.4.1.1 **Spectrum:** AeroMACS systems can operate in the band of 5 030 to 5 150 MHz under an ITU AM(R)S allocation. Currently the 5 091 to 5 150 is targeted internationally for AeroMACS operations. In addition, the system can also operate in the frequency range between 5 000 to 5 030 MHz should an administration authorize AeroMACS licenses in these frequency bands.

Note.— It is recommended that AeroMACS radios are manufactured to cover the band 5 000 to 5 150 MHz to cover all current and future allocations.

1.4.1.2 **Services:** AeroMACS operates under an ITU AM(R)S allocation. Therefore, AeroMACS networks should only support services that are relevant to the safety of life or the regularity of flight operations. AeroMACS can support exchanges from all key stakeholders in an aerodrome including: ANSPs (safety communications), aircraft operators (AOC, regularity of flight communications) and airport authorities (regularity of flights communications).

1.4.1.3 **Airborne use:** AeroMACS transmissions from an aircraft are only allowed when the aircraft is on the airport surface. This limitation is based on studies presented in WRC-07 in order to avoid interference to fixed satellite service (FSS) systems and is part of the conditions agreed in order to obtain the allocation in the 5 091 to 5 150 MHz band. Therefore, AeroMACS transmissions from airborne aircraft are to be inhibited.

1.4.1.4 **Velocity:** AeroMACS is validated for operations involving aircraft and vehicles moving at velocities up to 50 nautical miles per hour in relation to the base station.

Note.— While the requirement for AeroMACS is to operate at velocities up to 50 knots, it does not preclude operation at higher velocities.

1.4.1.5 **Airport domains:** AeroMACS systems can support communications exchanges between moving and fixed assets in various operating areas in the airport environment including gate, ramp, taxiways and runways.

1.5 Architectural and institutional considerations

1.5.1 AeroMACS physical network deployments and connections to service provider networks are influenced by a number of architectural and institutional considerations. As mentioned earlier, there are three types of service supported by AeroMACS: air traffic services, aeronautical operational control services and airport authority services. Therefore, the AeroMACS infrastructure may be owned and operated by multiple entities providing the services. In addition to this, services may be provided by a communication service provider (CSP), such as the aircraft communications addressing and reporting system (ACARS) service provision. The following discussion highlights a number of considerations that impact the physical AeroMACS network and the connections to other networks.

1.5.2 The possible entities which may own and operate an AeroMACS service could be one or more of the following:

a) airport authorities;

b) ANSPs;

c) airlines; and

d) CSPs.

1.5.3 One or more networks, operated by different entities, can be operational at a given aerodrome. AeroMACS may offer different services to different communities of users. Availability of certain services, e.g. ATS/AOC etc., should be advertised by the upper layer communication functions.

1.5.4 In the case where multiple entities provide differentiated service at an aerodrome, individual airlines or even the ANSP may contract with a particular service provider for their services. Safety-related traffic must be available through all providers of AeroMACS service at an aerodrome. This may be done through the sharing of this traffic by a process known as “internetworking”.

1.5.5 Where an ANSP provides the AeroMACS service at an aerodrome, CSPs may resell the service to airlines and others. In this case, the terrestrial network connection and any switching/routing will be provided by the CSP. Such switching/routing may also include “internetworking”. In this case, the ANSP acts as an NAP and the CSP acts as an NSP. These terms will be explained further in section 2.2 on system architecture.

1.5.6 The basic scenario where AeroMACS service is provided by one entity at an aerodrome is shown in Figure 1.

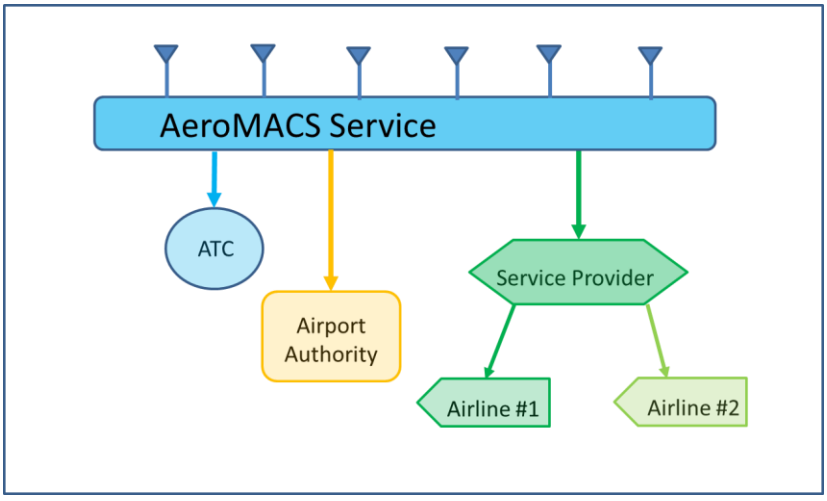


Figure 1. AeroMACS scenario provision by one entity

1.5.7 In the above diagram, ATC and the airport authority are connected locally, whereas the airlines are remotely located. In this case, the airlines are using a CSP that allows remote access. In this case, the CSP acts as an NSP as explained later in section 2.2.

1.5.8 Access to other media, i.e. VDL Mode 2, satellite services will be provided through a router.

1.5.9 The scenario where multiple AeroMACS systems may be operated by different entities at an aerodrome is show in Figure 2.

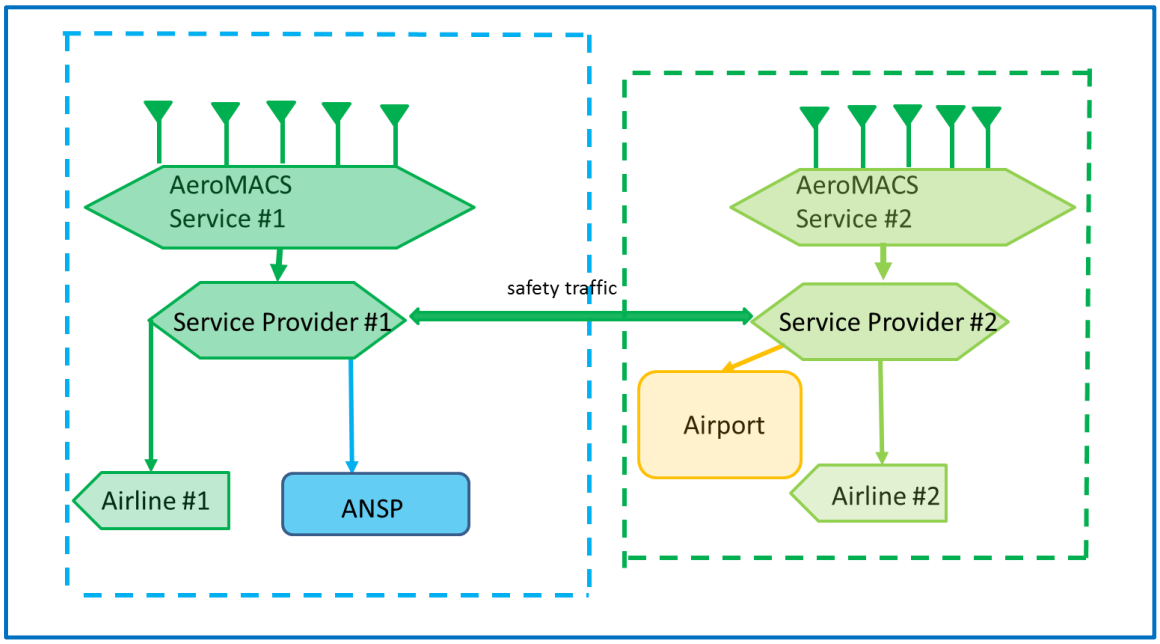


Figure 2. AeroMACS scenario provision by multiple entities

1.5.10 This represents the most complex scenario with multiple AeroMACS systems operated by different entities which, in turn, serve different groups of customers. In this example, safety-related traffic is available to all ground users, as internetworking is provided between the AeroMACS services. This may also extend to non-safety traffic.

1.5.13 In the above example, the ANSP and airport authority are connected to one service provider only. The internetworking link ensures that safety traffic is carried to aircraft via both networks. This allows the customer groups to preserve their standard commercial relationship with their chosen (often local) service provider. Without this, the ANSP and the airport authority would need to be connected to both service providers so as to achieve the appropriate connectivity.

1.5.12 As each aircraft can only log onto one network, each service provider must provide a back-up service for airlines contracted to the alternate service provider. This may be limited to safety traffic only.

1.5.13 In the case where a commercial entity such as a CSP or even an airport authority provides AeroMACS service a number of commercial issues may arise as commercial service providers must recover the costs of their investment.

CHAPTER 2

GUIDANCE MATERIAL

2.1 CONCEPT OF OPERATIONS

2.1.1 Introduction

2.1.1.1 AeroMACS can potentially support the wide variety services of voice, video, and data communications and information exchanges among fixed and mobile users at the airport.

2.1.1.2 The applications and communications provided by AeroMACS can generally be grouped into three major categories: air traffic services (ATS), airline operational control (AOC) services and airport authority services (see Figure 3). Within these broad categories, the data communications and applications can be described as either fixed or mobile, based on the mobility of the end user.

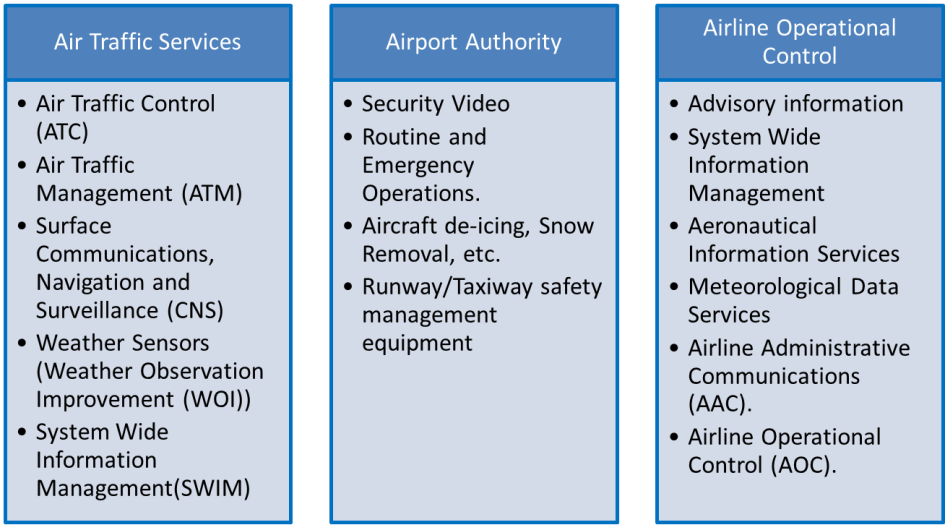


Figure 3. Example of AeroMACS applications

2.1.1.3 The application that a user will be connected to vary depending on the usage. For instance aircraft, which are mobile assets, are expected to have connectivity to both air traffic services group of applications as well as airline operational control group of applications and may have connection to an airport authority group of applications such as aircraft de-icing. Airport sensor systems, which are generally fixed assets, are expected to connect an airport authority type of application such as security video. Nomadic and non-aircraft mobile system may have connections to all three of the above cited groups of applications depending on their needs and authorizations. Determination of the type of user is critical to providing the correct level of service over AeroMACS.

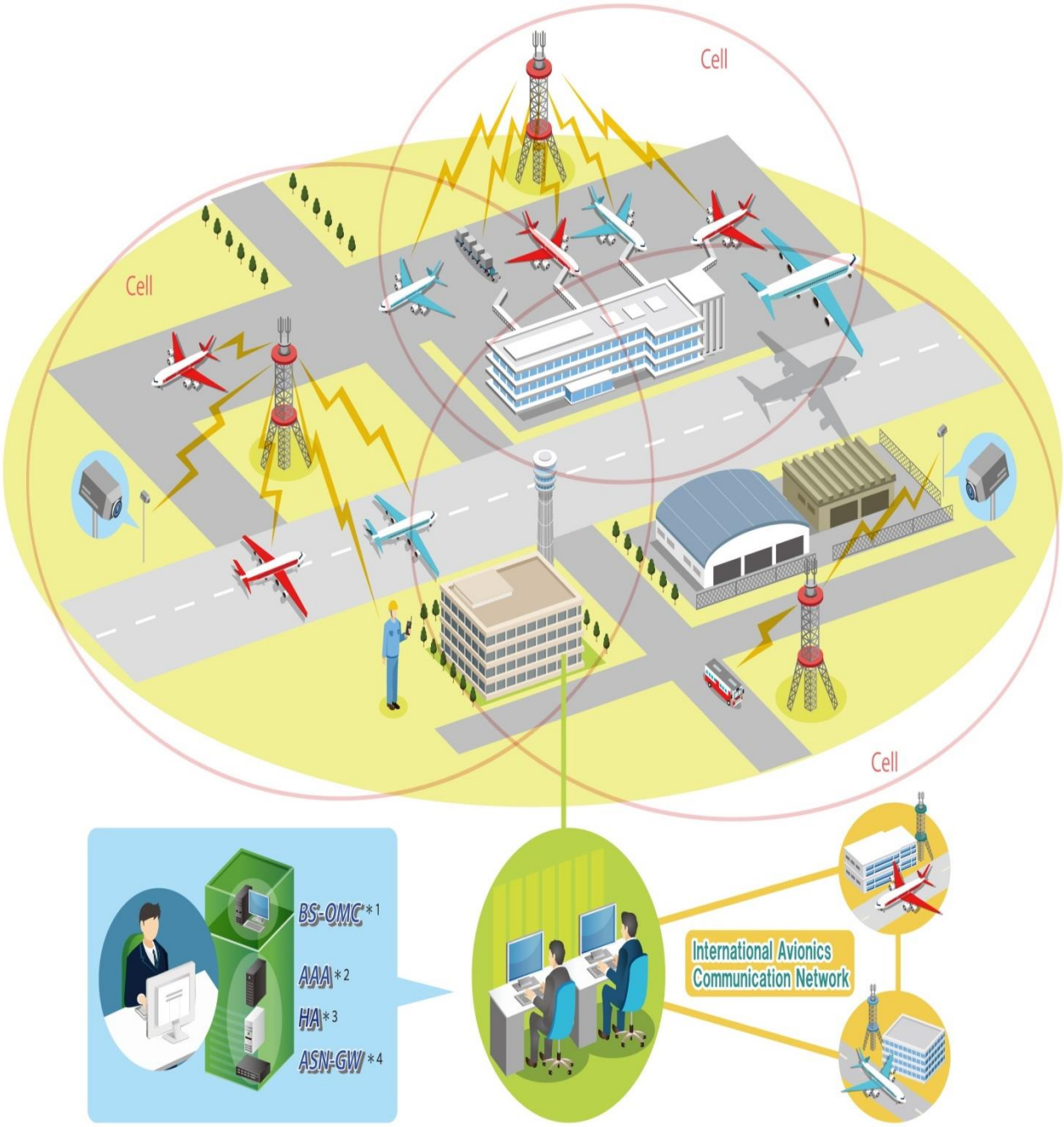


Figure 4. AeroMACS generic applications and communications overview

2.1.2 **Services**

The services that are described in the following scenarios could be handled by AeroMACS.

2.1.2.1 *Air traffic services*

2.1.2.1.1 Air traffic services are provided to regulate air traffic to ensure safe conduct of flight operations. Air traffic services can be grouped under eight major categories:

a) data communication management services (DCM);

b) clearance/instruction services (CIS);

c) flight information services (FIS);

d) advisory services (AVS);

e) flight position/intent preference services (FPS);

f) emergency information services (EIS);

g) delegated separation services (DSS); and

h) miscellaneous services (MIS).

2.1.2.1.2 Most of the ATS services that are accessible at airport terminal areas may use AeroMACS as the primary network.

2.1.2.2 *Aeronautical operational control services*

Generally, aeronautical operational control (AOC) services refer to a set of data link applications used to exchange messages between aircraft and airline centres or its service partner centres on ground. AOC is comprised of standard messages defined by AEEC standards, as well as airline defined proprietary messages.

2.1.2.3 *Airport authority services*

Generally, the airport authority services refers to a set of applications that is used to operate and control the airport. Information on the status of runways, facilities, airport security, etc. is generally considered under this category. Systems and services identified at the time of writing include:

a) FOD debris detection systems;

b) airfield lighting systems;

c) radar, e.g. avian radar;

d) NAVAIDs;

e) runway incursion prevention systems;

f) wildlife detection systems;

g) runway condition reporting systems;

h) in-pavement condition reporting systems;

i) perimeter surveillance;

j) intruder detection;

k) airfield access control systems;

l) audio/video communication with the ground vehicles; and

m) audio/video communication with emergency vehicles.

2.1.3 A**ircraft operational scenario**

2.1.3.1 *Description*

2.1.3.1.1 Aircraft operations at airport terminal areas can be classified under three major scenarios namely:

a) aircraft landing;

b) aircraft parked; and

c) aircraft departure.

2.1.3.1.2 Aircraft operations at hangers can be considered similar to aircraft on the apron scenario in the context of the AeroMACS network.

2.1.3.1.3 These scenarios happen in a sequence of repeated cycles in airports as shown in Figure 5. (En-route communications is not important for the discussion as AeroMACS is not involved in that scenario.)

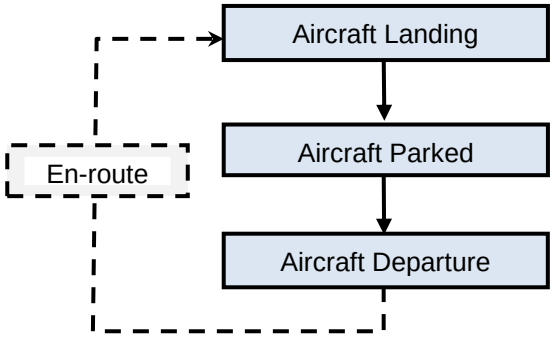


Figure 5. Aircraft operational scenarios

2.1.3.1.4 These sequences happen in continuous cycles for an aircraft during its normal operations (say from 0600 hrs to 2200 hrs (UTC)). Hence in an airport if there are around 200 arrivals and take offs per hour, at least 100 cycles of the above operational sequences occur in that airport in that hour. We can

assume a halting period of eight hours per overnight stay for an aircraft at airports. The individual scenarios are expanded in the following subsections.

2.1.3.2 *Aircraft landing*

2.1.3.2.1 The aircraft landing scenario refers to the operations performed by an aircraft from its touchdown to taxiing till gate. On touchdown, the aircraft establishes data link connectivity with the airport network. (The airport network is based on AeroMACS service.) The services that the aircraft is likely to be connected to are as follows:

a) D-TAXI (data link – taxi) route plan is uploaded to aircraft. (ATC);

b) OOOI (off/out/on/in) status is provided. (AOC);

c) ACM (ATC communications management) transfer of control happens from runway tower to ground tower. (ATC);

d) A-SMGCS (advanced surface movement guidance and control system) surface services are activated in addition to surface surveillance information being provided to aircraft. (ATC);

e) TAXI clearances are provided. (ATC-ground tower); and

f) flight data is downloaded to airline operations/maintenance centres. (AOC).

2.1.3.3 *Aircraft parked*

2.1.3.3.1 The aircraft parked scenario refers to the operation performed when an aircraft is parked at the gates, its engines are switched off and some upkeep operations are being performed. In this scenario, aircraft will be connected to airport, ANSP and airline private networks while exchanging data through the AeroMACS access network. The services that an aircraft is likely to be connected to are as follows:

a) avionics software and database are uploaded. These databases include airport information, navigational data, pilot manuals, terrain data etc.;

b) maintenance data from avionics/engine are downloaded if not downloaded during the aircraft landing above. This data may include both prognostics and diagnostics information;

c) pilot manuals/charts/maps etc., may be uploaded;

d) electronic checklist/electronic flight bag (EFB) updates; and

e) routine maintenance checks.

2.1.3.4 *Aircraft departure*

2.1.3.4.1 In aircraft departure scenario, all operations from pre-departure phase to take-off phase are covered. Aircraft pushes back from the gate, starts engines, taxies to the runway and then takes off Aircraft remain connected to the AeroMACS network until its take-off. The services that the aircraft is likely to be connected to are as follows:

a) flight planning and support services;

b) airport terminal information messages (ATIS),which provides information about the availability of active runways, approaches, weather conditions, NOTAMS, etc.;

c) departure clearance;

d) runway visual range information;

e) hazardous weather and operational terminal information;

f) weight and balance information flight preparations, delays, pilot preferences;

g) OOOI messages; D-TAXI/Push back clearances;

h) TAXI route information and instructions surface surveillance guidance control; and

i) ACM messages or any other information related to the regularity and safety of flight.

2.1.3.4.2 During the take-off phase the aircraft will disconnect from AeroMACS.

2.1.3.5 *Typical scenarios*

2.1.3.5.1 This section describes typical scenarios for the use of the AeroMACS communications system. Within this document, the use of other communications systems such as Mode S and universal access transceiver (UAT) for automatic dependent surveillance-broadcast (ADS-B) messaging and VDL Mode 2 for controller pilot data link communications (CPDLC) is discussed in addition to the use of AeroMACS. This further shows the context in which AeroMACS is intended to be used.

Note.— The following operational scenarios mention a broad range of applications/services. Many States may only operate a subset of these especially when AeroMACS service is introduced.

2.1.3.5.2 The aircraft operator provides gate/stand/hangar information, aircraft registration/flight identification and estimated off-block time to other users (e.g. airport, fixed base operation, corporate operation and ATC) via the ground-ground communications system. The flight crew prepares the aircraft for the flight and, in particular, provides the necessary inputs and checks with the flight management system (FMS). Among their other duties, the pilots power up the aircraft communications systems which include the AeroMACS communications system. The pilots connect their electronic flight bag (EFB) to the communications system ports in the aircraft provided for EFBs to enable updates to all EFB applications. As the various data communications connections are being established, the pilots are performing other duties to prepare the aircraft for the flight. The pilots initiate air traffic control (ATC) voice link and CPDLC to enable transfer of ATC clearances. The flight crew requests the flight plan from aircraft operational control (AOC) for airlines or flight operational control (FOC) for business aviation and enters the provided flight plan data into the FMS. The aircraft begins receiving supporting data from SWIM services via AeroMACS to support trajectory negotiation and other SWIM services (e.g. NOTAMS, PIREPS, AWAS).

2.1.3.5.2 The pilot requests D-ATIS information and receives the response via the AeroMACS system. The flight crew consults relevant aeronautical information services (e.g. planning information bulletins, notices to airmen (NOTAMs), and aeronautical information charts) concerning the flight. Real-time information on the flight's departure is now available in the air traffic services unit (ATSU) automation system. The flight information service (FIS) system response provides all relevant information for the weather, automatic terminal information service (ATIS), and field conditions, plus the

local NOTAMs. The pilots review updated information for appropriate adjustment to information entered in aircraft systems such as the FMS and for coordination with ATC and AOC/FOC.

2.1.3.5.3 The aircraft begins receiving surface vehicle locations on the ADS-B/traffic information system-broadcast (TIS-B) system in the aircraft. Some of the vehicles on the airport surface are equipped with an AeroMACS ADS squitter message (typically non-movement area vehicles such as people movers, tugs, food trucks, baggage carts) while others are equipped with ADS-B squitter message (usually movement area vehicles such as snow plows, fire engines, maintenance vehicles) using Mode S or UAT. Both squitter types of information are transferred to the TIS-B surveillance system. The processed data from the TIS-B surveillance system is transferred to both aircraft and vehicles systems and service organizations (such as airlines, airport authorities, fuel truck companies, fixed base operators (FBOs), and handling organizations) as appropriate for their usage. For aircraft preparing to taxi, the current graphical picture of the ground operational environment is uplinked and loaded using the standard ADS-B/TIS-B links to the aircraft. Some aircraft begin squittering position via the AeroMACS system, as the Mode S system is not yet powered up due to certain aircraft implementation issues (high power transmissions of weather radar which cause personnel safety issues are enabled by the same power switch as the Mode S system on some aircraft).

2.1.3.5.4 The load sheet request is sent to AOC. The load sheet response with the "dangerous goods notification information" and the last minute changes to the weight and balance of the aircraft are sent by the AOC and are automatically loaded into the avionics. The flight crew requests a "start up and push back clearance" via the data link taxi service. The flight crew pushes back and starts up the engines in accordance with airport procedures. The push back sends an "out-off-on-in (OOOI)" message to AOC advising that the flight has left the gate/stand.

2.1.3.5.5 The tug is attached to the aircraft and the tug operator communicates with the pilots using VoIP via AeroMACS to coordinate the pushback of the aircraft. The pilots receive clearance/authorization to push-back and proceed on this snowy day to the de-icing station. As the aircraft pushes back, the surveillance service is activated and continues for the duration of the flight to the destination gate.

2.1.3.5.6 The pilots are aware of the tug position on this snowy day via both visual and TIS-B broadcasts as the tug is squittering its position as are all other vehicles on the surface of the airport (both movement and non-movement areas). As the aircraft approaches the de-icing station, coordination occurs over the AeroMACS VoIP with personnel at the de-icing station. As the de-icing procedure is occurring, the pilots request updated D-ATIS information for review and possible action. Having completed the de-icing procedures, the aircraft receives clearance to proceed to the runway. On the way to the runway, the aircraft passengers and crew prep for take-off. As part of the prep for take-off the pilots stow the EFB. The aircraft is given clearance to take-off. As the aircraft takes off, an out-off-on-in message is generated and sent (or stored for transmission) to AOC that the aircraft is airborne. The aircraft AeroMACS system discontinues transmission starting at take-off while other communications and surveillance systems such as VDL Mode 2 and ADS-B are fully operational.

2.1.3.5.7 As the aircraft proceeds towards its destination, the aircraft collects aircraft engine data and other aircraft information for later transmission. The decision to use the AeroMACS system when reconnected rather than an alternative link during the flight will be due to the aircraft owner policy based on link costs or a need to protect proprietary data. For example, D-ATIS requests for the next leg of the flight (that do not require responses while in the air) could also be held back for communications over the AeroMACS system.

2.1.3.5.8 The flight crew lands the aircraft. After the aircraft lands, the AeroMACS system quickly connects and the stored data and requests are automatically transmitted over the AeroMACS system.

Responses to requests are made available to the requestors. As the avionics detects touchdown the aircraft sends the on-OOOI information to the AOC. As the aircraft proceeds across the airport surface, aircraft ADS-B transmissions are received by the ADS-B ground station at the airport. The ADS-B transmissions received from the aircraft are forwarded to the TIS-B servers via AeroMACS as some of the ground stations do not have direct access to the airport LAN to enable transfer ADS-B squitter information between the TIS-B servers and the ground stations. In addition the multilateration system that tracks aircraft position on the surface of the airport connects via the AeroMACS system to the ATC service provider surveillance system to provide the multilateration sensor data.

2.1.3.5.9 When the aircraft arrives at the gate/stand, the aircraft sends the in-OOOI message to AOC which makes the information available for other users. AOC responds to the OOOI message with a flight log transfer message to inform the crew of the next flight assignment.

2.1.3.6 *Applications supported*

AeroMACS is agnostic to the applications supported, however, message routing and handling will be determined based on the particular applications in the operational scenarios just described. Later sections on routing and discovery and service flows will be discussed in detail.

2.1.4 Routing and discovery

2.1.4.1 The aeronautical communication network comprises multiple independent networks with separate administrative domains interconnected to each other to achieve the overall safety communication infrastructure. Examples of such networks are; air navigation service provider (ANSP) network, airlines network, airport service provider network, OEM network, etc. These networks would be predominantly based on ATN/IPS (IPv6). These are closed networks that are protected against intrusion from the public internet. Hence, the overall aeronautical network can be imagined as islands of closed networks interconnected over public infrastructure to form a closed internet for aeronautical purposes. See Figure 6.

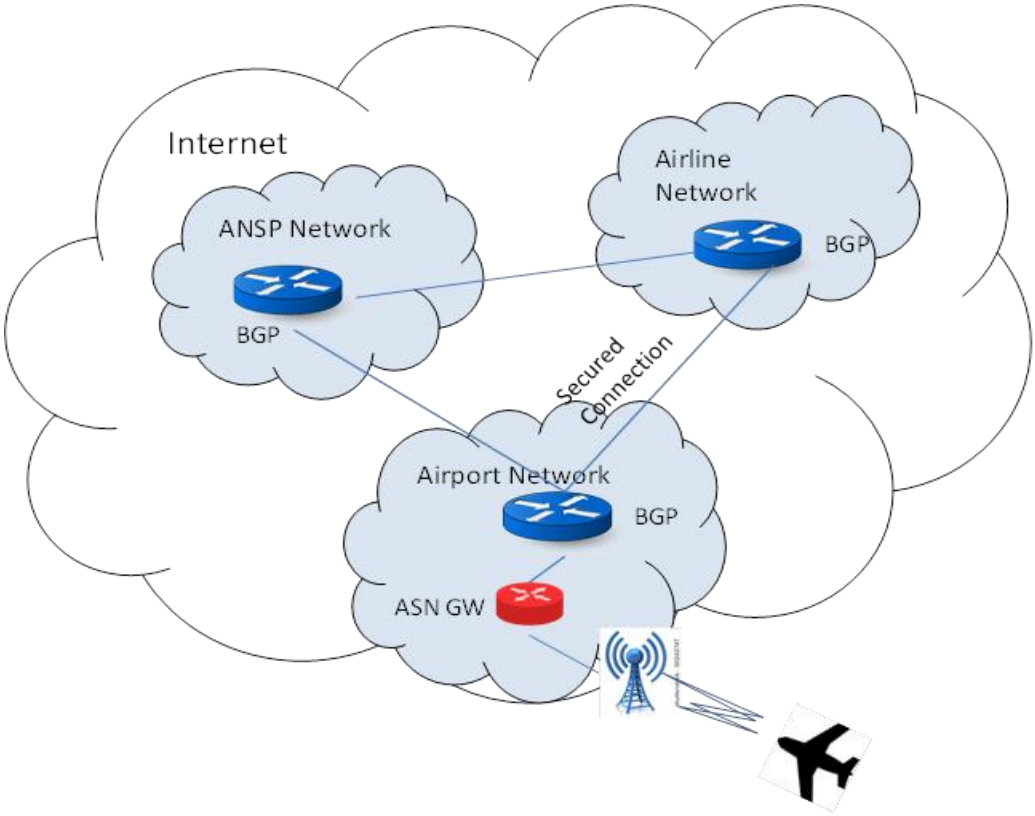


Figure 6. Aeronautical network

2.1.4.2 As per the recommendations of the *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols* (Doc 9896), independent autonomous networks are to be interconnected using inter-domain routers (such as BGP). To maintain abstraction with the public internet, these routers are not exposed to other routers in public domains. Secured links, either based on VPNs or dedicated telecom lines are deployed to interconnect the routers belonging to the aeronautical network. The ingress and egress to safety networks are controlled by routers to ensure complete abstraction from the internet.

2.1.4.3 AeroMACS acts as an access network for the airport domain as shown in the Figure 6. Hence, the AeroMACS ASN Gateway is connected to the core router in the airport domain network. The airport network may obtain its address space from an approved registry such as ICAO or the Internet Assigned Numbers Authority (IANA) and allocates those addresses to its internal networks. For example: if an airport network covers ten different airports, the airport network operator obtains a consolidated address space and suballocates them to the ten airports. Subsequently, each of the airports allocates addresses to its internal network elements. The network edge router advertises the consolidated address space to the external routers.

2.1.4.4 Aircraft may have either global permanent IP addresses allocated to it or may obtain a temporary IP address from the access network at the point of contact. For instance, in case of IPv4 deployment it may not be possible to obtain a permanent global address for aircraft owing to IPv4 address scarcity. However, in case of IPv6, aircraft may be assigned permanent addresses. Depending upon such address allocation schemes, the routing and discovery mechanisms would differ at deployments. In case of temporary IP addresses allocated by the access network, IP mobility implementations such as mobile IP (MIP), proxy mobile IP (PMIP) or any other state of art IP mobile technology may be deployed. In

case of permanent global IP addresses allocated to an aircraft, the aircraft may become an independent autonomous network. In such a scenario, the aircraft may need to have an inter-domain router that connects it to the edge router in the airport network.

2.1.4.5 The routing and mobility concepts are not completely finalized for IPS network. However, these implementations are outside the scope of AeroMACS (access) network. At a minimum, the access network is expected to support both static and dynamic addressing schemes at the link interface for an aircraft.

2.2 FREQUENCY ALLOCATION AND CHANNELIZATION

2.2.1 AeroMACS operates in frequency bands internationally allocated per the aeronautical mobile (route) service (AM(R)S). As a result, AeroMACS, in the internationally allocated bands, is restricted to supporting communications related to safety and regularity of flight. In addition, in accordance with International Telecommunications Union (ITU) Radio Regulations, AeroMACS is limited to supporting surface transmissions at airports.

2.2.2 In general, AM(R)S bands are intended to provide communications between aircraft and ground stations or between aircraft. However, ITU does not preclude operations in frequency bands allocated to a mobile service (like AM(R)S) to support both mobile and fixed/nomadic (i.e. low mobility) applications. As a result, some States plan to utilize AeroMACS also for airport surface communications between ground stations. Finally, some States allow limited use of AM(R)S frequency bands (and by extension AeroMACS) by non-aircraft vehicles; in particular vehicles such as snow ploughs which may mix with aircraft on the airport movement area.

2.2.3 AeroMACS equipment can tune across the band 5 000 MHz to 5 150 MHz, in 250 kHz steps with reference channel of 5 145 MHz. That reference channel is used to identify a channel whose centre frequency is among the centre frequencies that are to be tuned by AeroMACS and it is a reference point for the identification of all other centre frequencies that may be tuned by AeroMACS using the channel step size. The 250 kHz step size will allow AeroMACS to gracefully move away from any interference source such as microwave landing systems (MLS), aeronautical mobile telemetry (AMT), or military users operating in the 5 000 to 5 150 MHz band.

2.2.4 The core or primary AeroMACS band is 5 091 to 5 150 MHz, however, channels can also be assigned in the subbands 5 000 to 5 030 MHz, based on national regulations, and 5 030 to 5 091 MHz depending on frequency planning defined at the ICAO level considering other aeronautical applications.

2.2.5 Due to its limitation to surface transmissions, it is expected that in most cases all AeroMACS channels will be available at all airports (i.e. airport-to-airport coordination is not expected to be necessary). It is also expected, however, that not all airports will have sufficient communications requirements to necessitate use of all the AeroMACS channels.

2.2.6 One constraint on AeroMACS that was considered during the development of the AeroMACS Standards is ensuring compatibility with satellites that share the same operating frequency band. While those Standards were developed using worst-case assumptions, compatibility with the satellites can be enhanced by, for airports which do not require use of all the channels, distributing actually assigned channels across the band. In order to ensure uniformity in that distribution, it is expected that a central authority in each State will control AeroMACS assignments.

2.2.7 To operate an AeroMACS system at an aerodrome, a spectrum license will be required. Spectrum regulations should be well documented prior to any considerations on siting. Any special

permissions when needed, should be investigated. Operators should be aware of any limitations (municipal, State and federal or military) to the use of certain frequency channels.

2.2.8 Further detail on AeroMACS channel assignment criteria and constraints are under development by ICAO. When completed they will be included in Annex 10, Volume V.

2.2.9 AeroMACS is for communication on the airport surface only. Although aircraft on the approach and departure phase of the flight may receive AeroMACS signals while on flight as shown by the glide slopes in Figure 7, aircraft are not permitted to transmit on AeroMACS bands while in flight. Airport systems should be designed to reduce sky-ward emissions through appropriate placement and orientation of the AeroMACS antennas.

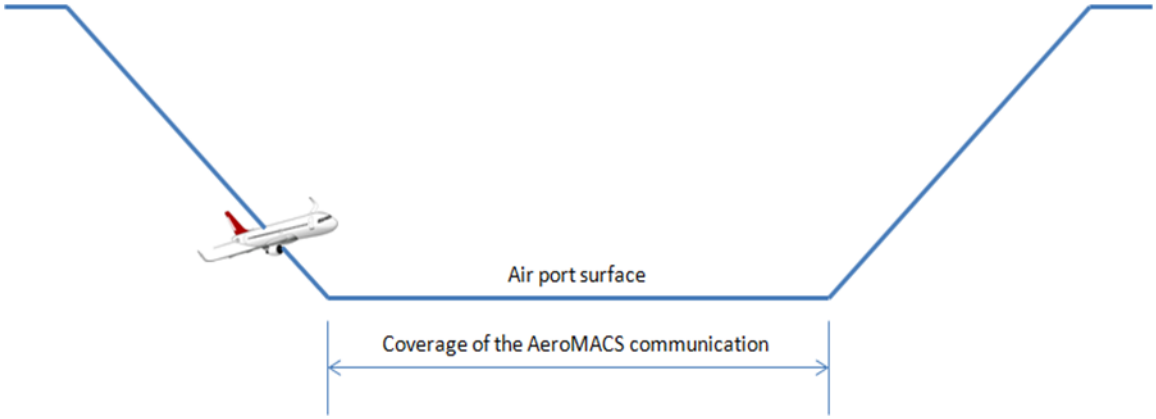


Figure 7. AeroMACS operational environment

2.3 SITING

2.3.1 Base station siting criteria

2.3.1.1 Siting is the process in determining the desirable locations of AeroMACS base station equipment on the airport surface. Siting incorporates a number of considerations and the conclusion of the process is a specification of base station locations, antenna locations, tilt angle and height. Siting takes into account the following:

a) the AeroMACS network architecture such as the physical devices to be deployed;

b) equipment performance such as transmit power, capacity and antenna gain;

c) service requirements such as coverage area and bandwidth;

d) requisite infrastructures such as power and data network points of presence (POPs);

e) buildings and terrain that interfere with line of sight requirements;

f) airport restrictions including no-obstruction areas;

g) airport infrastructures such as landing systems that cannot accept physical or electrical interference;

h) physical access requirements for maintenance; and

i) people and equipment movement.

2.3.1.1.1 An AeroMACS cell network involves BSs and SSs. This document considers the identification of desirable locations for BS. SS locations are not part of the siting analysis but they are implicitly included since a proper BS siting can give service to a number of SS in the coverage area with the expected required performance. In any case, the coverage depends on the link budget between BS and SS, the latter being a mobile device or a fixed station that has been purposely located within the coverage range of a BS part of the siting exercise.

2.3.1.1.2 There is no optimum solution for equipment location. The considerations for siting ultimately result in a compromise that simultaneously meets the network performance objectives and all the other requirements and limitations that are imposed. This section leads the reader through the process of siting, introduces the relevant considerations and lends guidance to the decisions and trade-offs that determine a useful specification of equipment location to meet all the requirements of the AeroMACS network.

2.3.1.2 *Characteristics pertinent to site selection*

AeroMACS MS will be subject to multiple BS to BS handovers. AeroMACS connections must be maintained throughout the airport surface for aircraft ground velocity up to 50 knots (~58 mph). Aircraft network connections in runway, taxiway, ramp and gate areas will be subject to fast fading due to multipath fluctuations of moving aircraft and ground vehicles. While many AeroMACS network connections will be line of sight connections, design considerations must be made for non-line of sight connections for ground handling equipment with lower antenna elevations or sensors placed on the ground, for example.

2.3.1.2.1 Antenna coverage

2.3.1.2.1.1 Base station antennas are typically directional with gain and a characteristic antenna pattern or beamwidth of gain versus elevation and azimuth. Smaller airports may benefit from omnidirectional antenna choices for the base station. Figure 8 establishes AeroMACS limits for EIRP versus elevation for the base station and antenna that antenna choice and tilt orientation must consider. These results were used to validate that AeroMACS global deployments would not violate the ITU WRC-07 requirements of the 2 degree temperature rise at the satellite.

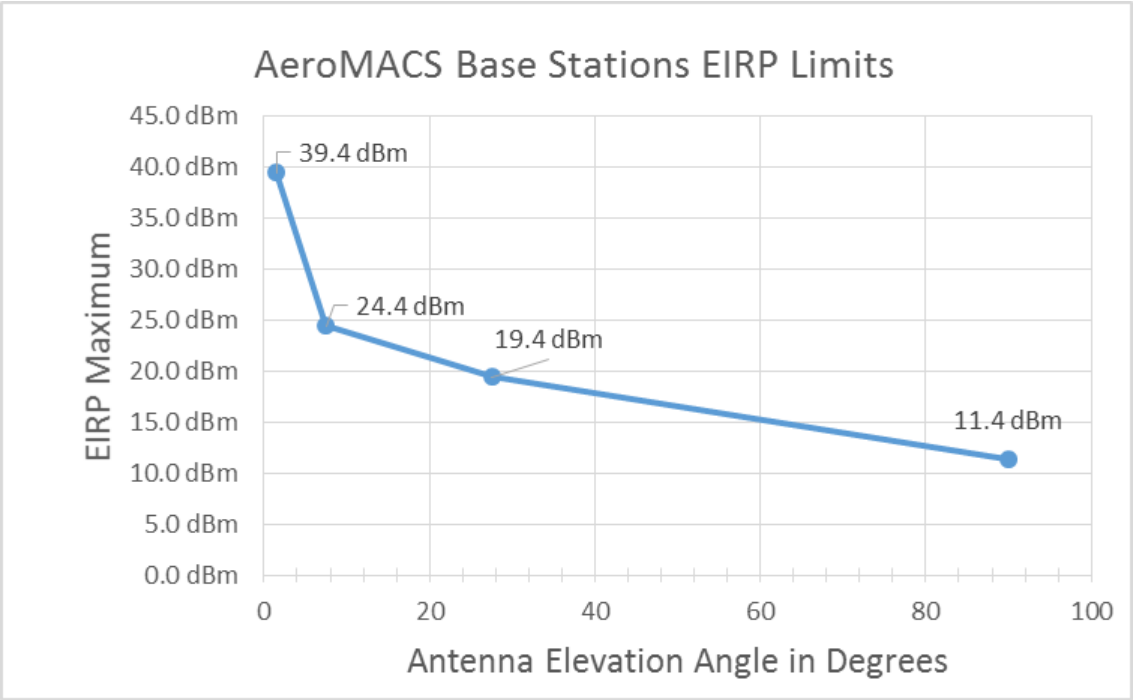


Figure 8. EIRP versus elevation

2.3.1.2.1.2 Subscriber station antennas are typically omnidirectional to allow mobility without concern for antenna orientation relative to the base station. The AeroMACS antenna on the aircraft is typically a single antenna mounted on top of the fuselage near the centreline. Fixed subscriber station antennas may be directional designed for significant gain compared to an omnidirectional antenna to extend range to the base station. These stations may also use multiple-input multiple-output (MIMO) techniques to improve performance.

2.3.1.2.1.3 Changing the antenna radiation pattern and tilt angle will impact the upward radiation and should be considered as part of skyward siting analysis.

2.3.1.1.2 Signal characteristics e.g. QAM, AMC, etc.

In AeroMACS network simulations, receiver characteristics must be considered. Receiver sensitivity typically improves with simpler modulation schemes. Table 1 below summarizes the required receiver sensitivity versus modulation scheme for AeroMACS base stations and subscriber stations.

Modulation scheme using convolutional codes (CC) encoding scheme	Rep. factor	MS RCV sensitivity	BS RCV sensitivity
64 QAM 3/4	1	-74.3 dBm	-74.5 dBm
64 QAM 2/3	1	-76.3 dBm	-76.5 dBm
16 QAM 3/4	1	-80.3 dBm	-80.5 dBm
16 QAM 1/2	1	-83.8 dBm	-84.0 dBm
QPSK 3/4	1	-86.3 dBm	-86.5 dBm
QPSK 1/2	1	-89.3 dBm	-89.5 dBm
QPSK 1/2 with repetition 2	2	-92.3 dBm	-92.5 dBm

Table 1. Receiver sensitivity versus modulation scheme

2.3.1.1.3 Coverage and capacity consideration

This section describes coverage and capacity factors to consider for the airport area being served. AeroMACS service areas include runways, taxiways, ramp areas, maintenance areas, the respective transition points and other special use areas on the airport surface to potentially encompass the entire outdoor airport surface in many instances.

2.3.1.1.3.1 Fixed applications

Fixed applications focus on wireless connectivity for priority standalone applications for "islands" of dedicated network coverage on the airport surface. Fixed applications may or may not share AeroMACS network infrastructure depending on network owner and operation considerations, priority and safety considerations, and deployment timeline considerations. Multilaterlation (MLAT), weather observation (WOI) and video surveillance for security and safety enhancements are examples of fixed applications. Site surveys and radio frequency (RF) planning should minimize the need to re-locate base stations in the future as AeroMACS applications evolve. Some initial base station deployments could be "easily-moveable" or "nomadic" to accommodate unanticipated future AeroMACS application rollout.

2.3.1.1.3.2 Runway/taxiway areas

The service coverage objective is to provide connectivity anywhere and anytime on the airport surface for AeroMACS-equipped aircraft or ground vehicles.

2.3.1.1.3.3 Ramp and gate areas

Gate spacing is typically determined by the wing spans of aircraft. Gate spacing of 80 to 120 meters is a reasonable estimate for airports that serve large jet aircraft. AeroMACS sector range of 1 km will cover eight to twelve gates with an excess loss factor, n = 4. For the capacity discussions that follow, capacity estimates assume eight gates/BS channel with all gates occupied by aircraft, or 8 aircraft per channel. Data payload requirements per aircraft include requirements for necessary support equipment including fuelling and baggage handling equipment, for example. Further, one-half hour is assumed for available time to deliver the required DL data payload per aircraft and to receive the required UL data payload per aircraft and a tentative 67 per cent/33per cent DL to UL payload ratio is incorporated into the data models.

2.3.1.1.3.4 Maintenance and fixed base operators (FBOs)

Maintenance and FBO areas typically serve airline specific operations. High traffic exchanges are expected (GBytes) for EFB updates, software uploads, electronic charts, log downloads and other transactions. These data transactions may happen over long periods of time from hours to overnight.

2.3.1.1.3.5 Airport obstructions and terrain

Airport obstructions, terrain impact and fresnel zone must be identified and anticipated in the system engineering performed for the AeroMACS network plan.

2.3.1.1.3.6 Aircraft and vehicle types

Aircraft and vehicle types must be identified and anticipated in the system engineering performed for the AeroMACS network plan. This is important for SS antennas that are low off the ground.

2.3.1.1.3.7 Types of SS devices

The types of subscriber station devices must be identified and anticipated in the system engineering performed for the AeroMACS network plan. SS devices may include fixed stations and mobile stations with significantly different form factors including PCMCIA cards, PDAs and notebooks/tablet PCs, handheld devices and aircraft radios.

2.3.1.2 *Coverage capabilities*

This section illustrates the propagation models used for different airport locations for both BS and SS to aid in the analytical evaluation. Information for computation and simulation is also provided in this section.

2.3.1.2.1 Link budget

2.3.1.2.1.1 The link budget first calculates maximum allowable link loss by taking into account factors such as transmitter power, receiver sensitivity, antenna gain, cable loss, noise figure, noise floor, modulation scheme and other factors. The link loss is adjusted for fade margin and other margin adjustments to arrive at a link budget. The link budget is an estimate that the system engineer should verify by measurements performed on-site.

2.3.1.2.1.2 The following charts, as shown in Tables 2 and 3, determine the maximum link loss and link budget for an AeroMACS system.

Parameter	DL (BS to SS)	UL (SS to BS)	Comments
Channel BW	5 MHz	5 MHz	
FFT	512	512	
Over-sampling factor	28/25	28/25	
Sampling freq.	5.6 MHz	5.6 MHz	
kTB	-114 dBm/MHz	-114 dBm/MHz	Gaussian noise floor
SNR – QPSK-1/2 coding	2 dB	2 dB	HARQ=2, BER = 10^{-6}
Data + pilot subcarriers	420	408	Partial usage subchannelization (PUSC) permutation
Implementation loss	5 dB	5 dB	
Noise figure	8 dB	8 dB	
Rx sensitivity	92.4 dBm	92.5 dBm	
Rx antenna gain	6 dBi	15 dBi	
Rx diversity gain	0 dB	3 dB	2 Rx antennas on BS
Tx power to antenna	21.4 dBm	24 dBm/20 dBm	Range on UL due to automatic power control
Tx antenna gain	15 dBi	6 dBi	
Tx combining gain	3 dB	0 dB	2 Tx antennas on BS
Maximum link loss	140.8 dB	140.5 dB/136.5 dB	

Table 2. Maximum link loss and link budget

Notes.—

1. *Link budget based on worst-case scenarios, other considerations may be used to improve link budget, where needed.*

2. *Additional margin for HARQ repetitions 6 vs 2, ~5 dB.*

3. *Standard deviation, σ = 8 dB typ. (Std deviation determined by field tests).*

Parameter	DL (BS to SS)	UL (SS to BS)	Comments
System gain	140.8 dB	140.5 dB/136.5 dB	UL RTW/Gate
Margins			
Log-normal fade margin	6 dB	6 dB	Optimistic – actual total fade margins may be as much as 13 dB to 19 dB
Fast fade margin	2 dB	2 dB	
Interference margin	2 dB	3 dB	Frequency reuse of 3
Penetration loss	0 dB	0 dB	
Link budget	130.8 dB	129.5 dB/125.5 dB	UL RTW/Gate

Table 3. Margins for various fading considerations

2.3.1.2.1.3 The following chart, as shown in Figure 9, illustrates various fading considerations to take into account in the AeroMACS system engineering process. Different path fade mechanisms typically dominate link loss depending on the separation of transmitter and receiver.

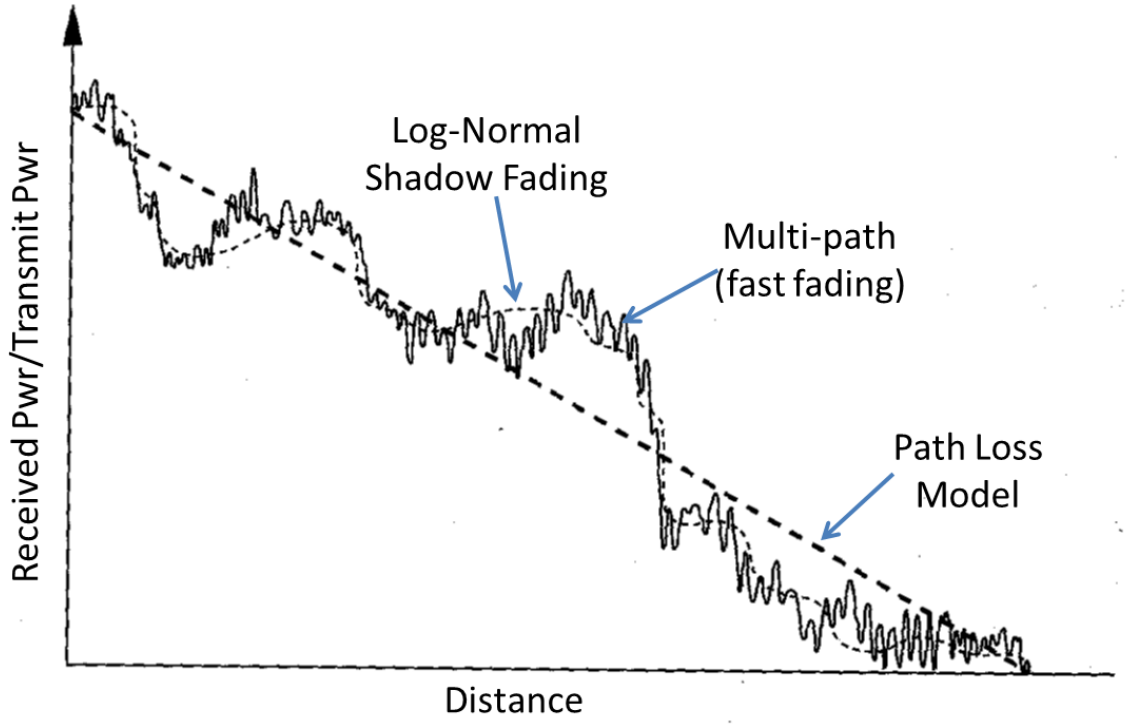


Figure 9. Path loss and fading mechanisms

Notes.—

1. *Every propagation path is subject to time-varying fades:*

a) runway/taxiway areas may be more problematic due to moving aircraft.

2. Mitigation techniques include:

a) MIMO with spatial diversity; and

b) cell to cell coverage overlap.

3. HARQ

a) fade margin allowance in link budget.

2.3.1.2.1.4 The following chart, as shown in Figure 10, plots cell edge availability versus fade margin for various standard deviations and HARQ repetition rates that the link budget takes into account. Note that the total fade margin assumption as illustrated in this chart may be significantly higher than 8 dB with a corresponding reduction in link budget to achieve high availability at the cell edge.

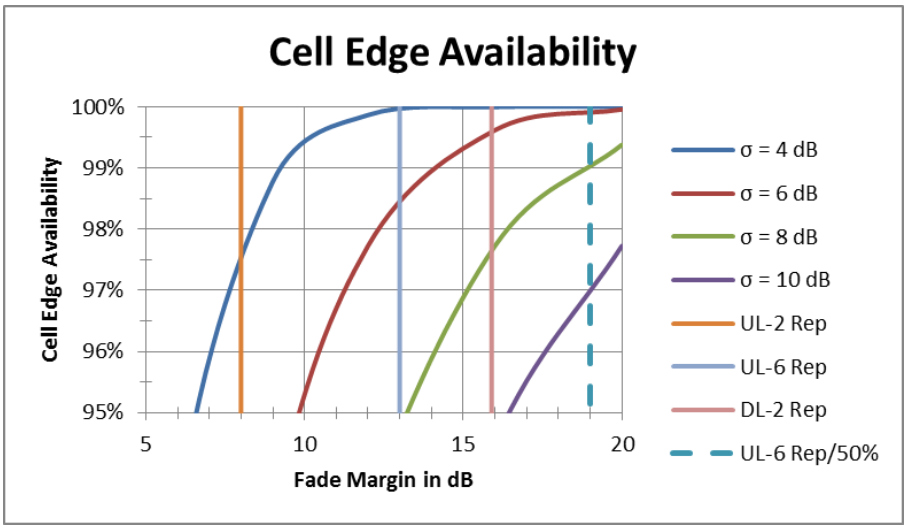


Figure 10. Cell edge availability versus fade margin

2.3.1.2.1.5 The following chart, as shown in Figure 11, predicts path loss for AeroMACS for various loss factors.

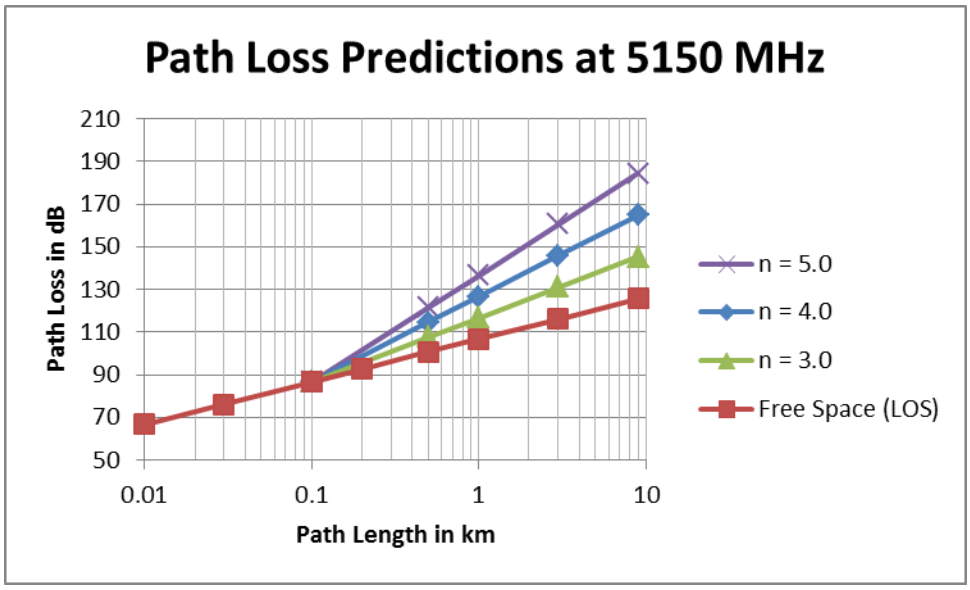


Figure 11. Path loss under various conditions

Notes.—

1. *Many airport areas will have non-LoS some, if not most, of the time.*
2. *Excess loss at 2 km is 10 to 20 dB based on different propagation models.*
3. *Gate areas: High 'clutter':*
   a) *aircraft, jet-ways, service vehicles, terminal buildings; and*
   b) *assume n ~4.*
4. *Runway areas: Less 'clutter':*
   a) *fewer aircraft, no buildings, fewer service vehicles; and*
   b) *can assume n ~3.*
5. *Higher BS and SS antenna height decreases value of n.*

2.3.1.2.1.6 The following chart, as shown in Figure 12, illustrates the impact in availability by increasing cell overlap or decreasing planned cell radius. The plots on this chart represent different total fade margin assumptions at the cell radius D.

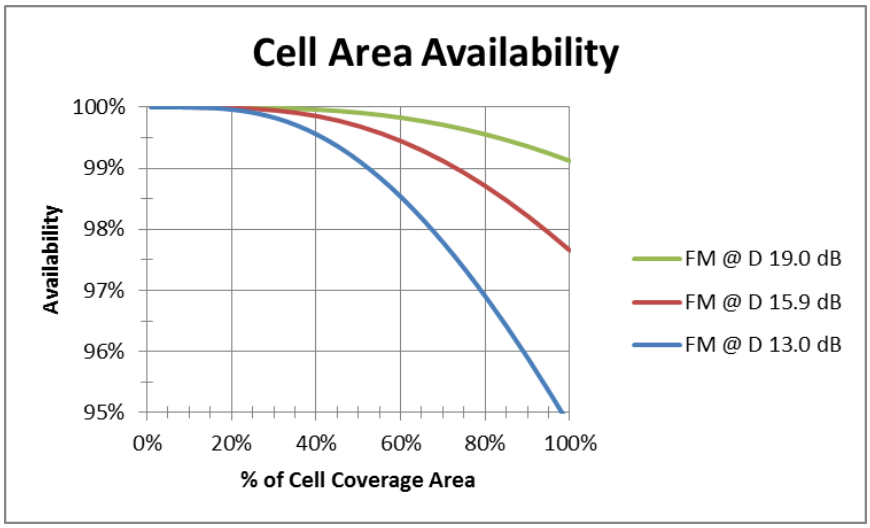


Figure 12. Availability versus cell radius

Note the impact of different fade margin assumptions on cell area for the same availability. The planned cell radius must be reduced by 30 per cent for a 6 dB increase in predicted total fade margin to maintain the same target availability.

2.3.1.2.1.7 If each SS will have access to at least two and many times three BSs, availability improves significantly:

a) main path + 1 alternative path improves availability from 99.0 per cent to 99.99 per cent (99.99 per cent = 52 min/year).

b) main path + 2 alternative paths improves availability from 95.4 per cent to 99.99 per cent (or from 99.99 per cent to >99.999 per cent).

Alternatively for two hops where passive repeaters are used, availability degrades from 99.0 per cent to 98.0 per cent, end-to-end.

2.3.1.2.2 Cell size

2.3.1.2.2.1 Cell radius is the expected distances between BS and SS. Cell area is the area of coverage per sector for a given link budget. In the runway and taxiway areas, the following assumptions are made:

a) excess loss factor: 3;

b) range: ~2.5 km; and

c) coverage: ~6.2^2 km per sector (620 ha/sector), assume 450 to 500 ha/sector to ensure overlapping coverage.

2.3.1.2.2.2 The following chart, as shown in Figure 13, plots coverage for the runway and taxiway area:

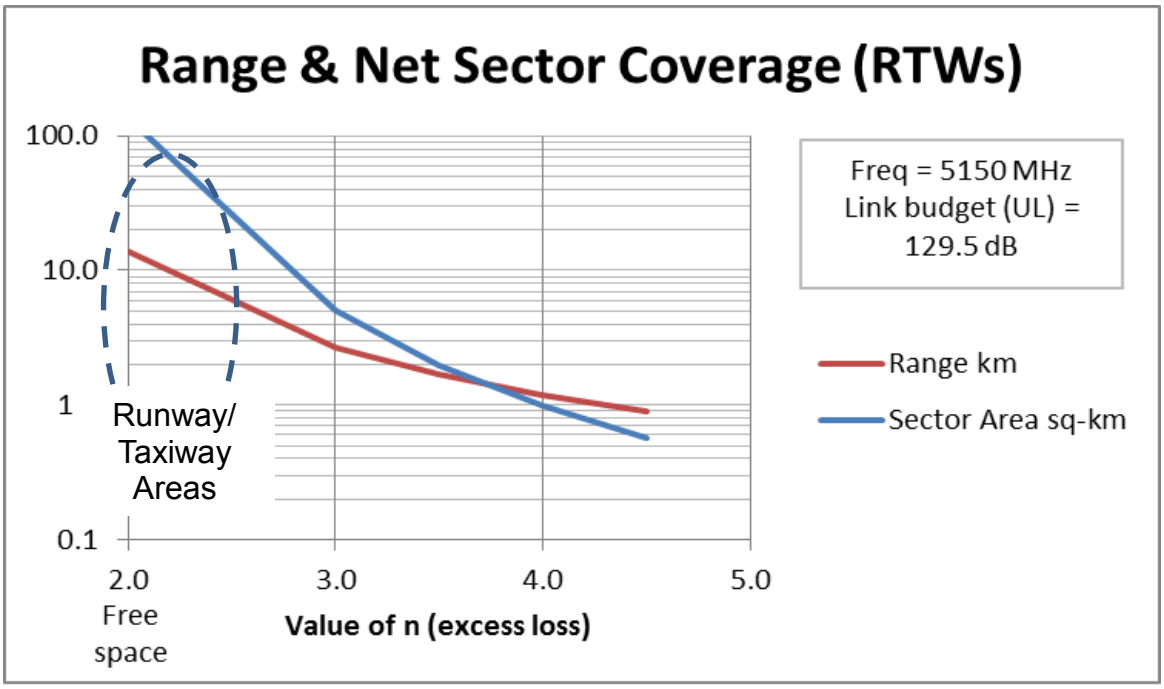


Figure 13. Range and sector coverage for the runway and taxiway areas

Note.— Net sector coverage area for runways and taxiways 1: ~540 ha (assume 500 ha to account for "non-ideal" site placement).

2.3.1.2.2.3 In the gate area, the following assumptions are made:

a) excess loss factor: 4;

b) range: ~1.1 km;

c) coverage: ~1.6 km per sector (160 ha/sector);

d) average gate spacing: 80 to 120 meters; and

e) eight gates per channel/sector.

2.3.1.2.2.4 The following chart, as shown in Figure 14, plots coverage for the gate and ramp area:

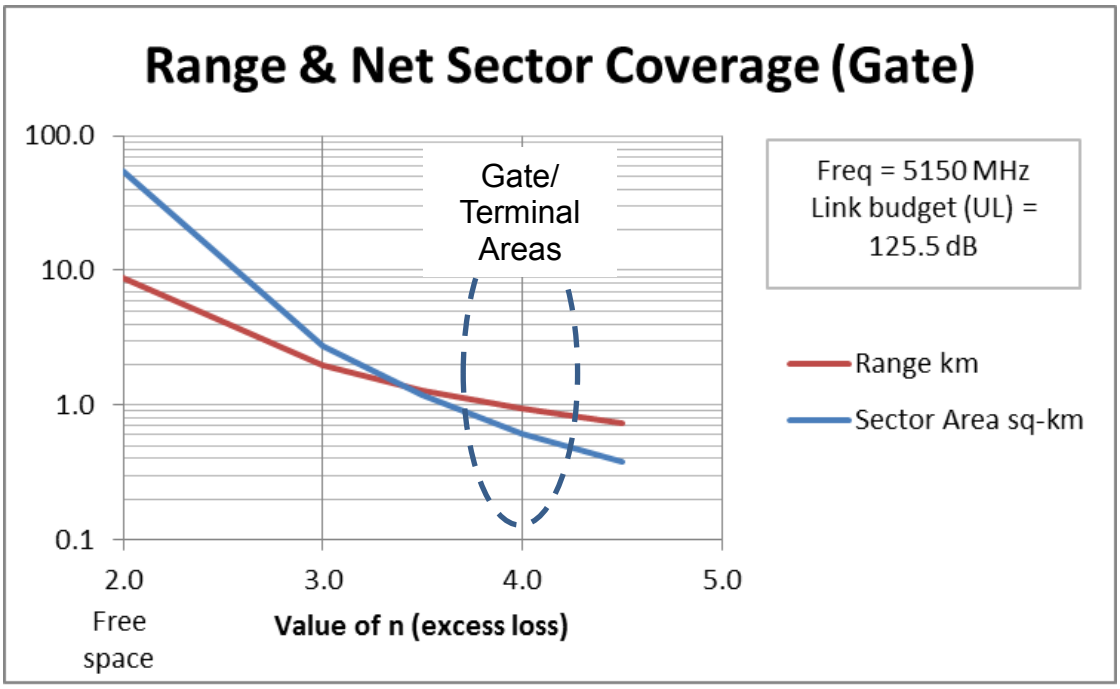


Figure 14. Range and sector coverage for gate and terminal areas

In the two range and net sector coverage charts above, the predicted performance that the plots depict is found in the oval region indicated.

2.3.1.3 *Capacity capabilities*

2.3.1.3.1 Domains and estimated loading

The following chart, as shown in Table 4, summarizes throughput estimates and packet size by domain:

ATC required throughput	
Overall (combined up and downlink) minimum average data load within one cell/sector of runway and taxiway OPS domain	0.6 kps
Overall (combined up and downlink) minimum average data load within one cell/sector of ramp OPS domain	0.2 kps
aoc required throughput	
Overall (combined up and downlink) minimum average data load within one cell/sector of GROUND/TOWER OPS domain	800 kps
Overall (combined up and downlink) minimum average data load within one cell/sector of RAMP OPS domain	1 000 kps
Packet size	
Average ATC message size	190 bytes
Average AOC message size	278 kilobytes

Table 4. Throughput estimates and packet size by domain.

Note.— MASPS offers the potential for more detailed requirements analysis; with respect to packet priorities, packet sizes, relative latency requirements, etc.

The following subsections and explore the data rate and delivery capabilities of the AeroMACS base station equipment. The same base station equipment installed in two different environments will have different rates of throughput as shown in the following tables.

2.3.1.3.2 BS capacity capability at runway and taxiway

The following chart, as shown in Table 5, summarizes the air data rates of the base station at the runway and taxiway for various modulation schemes and distances to the subscriber station.

Parameter	DL	UL	Comments
a) Total subcarriers	512	512	FFT
b) Null subcarriers	92	104	PUSC[1]
c) Pilot subcarriers	60	136	
d) Data subcarriers	360	272	PUSC[1]
e) Symbols	24	24	
f) OH symbols	3	4	
g) Data symbols	21	20	
h) Frame size	5 ms	5 ms	
i) Link budget	130.8 dB	129.5 dB	Lower SS Tx Pwr
j) Peak OTA rate (64QAM-3/4)	6.80 Mbps	3.26 Mbps	= 4.5xDxG/H/1 000
k) Cell edge OTA rate (QPSK-1/2, rep=2)	0.76 Mbps	0.54 Mbps	= 0.5xDxG/H/1 000

Table 5. Possible data rates at runway ends and taxiways

[1] *AMC (adjacent multicarrier) permutation increases data subcarriers in DL ~7 per cent and UL ~40 per cent, PUSC, however, is better for mobility.*

2.3.1.3.3 BS capacity capability at ramp and gate

The following chart, as shown in Table 6, summarizes over the air data rates of the base station at the ramp and gate for various modulation schemes and distances to the subscriber station.

Parameter	DL	UL	Comments
a) Total subcarriers	512	512	FFT
b) Null subcarriers	92	104	PUSC[1]
c) Pilot subcarriers	60	136	
d) Data subcarriers	360	272	PUSC[1]
e) Symbols	24	24	
f) OH symbols	3	4	
g) Data symbols	21	20	
h) Frame size	5 ms	5 ms	
i) Link budget	130.8 dB	125.5 dB	Lower SS Tx Pwr
j) Peak OTA rate (64QAM-3/4)	6.80 Mb/s	3.26 Mbps	= 4.5xDxG/H/1 000
k) Cell edge OTA rate (QPSK-1/2)	1.52 Mbps		= 1xDxG/H/1 000
l) Cell edge OTA rate (QPSK-1/2, rep=2)	N/A	0.54 Mbps	= 0.5xDxG/H/1 000

Table 6. Possible data rates at ramps and gates

[1] *AMC (adjacent multicarrier) permutation increases data subcarriers in DL ~7 per cent and UL ~40 per cent, PUSC, however, is better for mobility.*

2.3.2 Siting procedures

This section presents guidelines on the specific work activities, descriptions and procedures to be followed during the siting process.

2.3.2.1 *Introduction*

The list below outlines a sequential step-by-step checklist recommended to be followed during an AeroMACS network siting process. A detailed description of each step can be found in the following subsections:

a) airport areas to be serviced should be identified and depicted on the proper airport maps and charts;

b) expected volumes and patterns of traffic in specific airport areas should be known and depicted in an application workbook;

c) regulatory restrictions over usable frequency channels and EIRP limits in the area should be identified and supported by regulatory documentation. Take into account the site plan and local regulations that define distance from populated areas;

d) power sources and points of connection to a local ground network accessible by the ASN-GW should be identified;

e) preliminary BS locations are selected following these general guidelines:

1) AeroMACS base station equipment should not be placed in runway safety areas;

2) AeroMACS fixed subscriber station equipment may be placed within the runway safety area if it is collocated with other existing equipment and the existing application allows it;

3) the antenna should be mounted at the highest possible point while respecting height limitations for the specific airport surface location to avoid airspace obstruction. Reception will generally improve with antenna height;

4) ensure minimum obstructions between the antenna and the planned coverage area;

5) ensure a minimum of 55 per cent exposure to the sky (GPS antenna requirement);

6) consider the distance to other antennae or devices that may cause interferences; and

7) base station equipment should be accessible for maintenance; and

f) verify the unit is placed in an area authorized by the corresponding owner of the space and compliant to environment regulation;

g) compute cost of installation (considering additional structural work when needed) and of maintenance should be assessed at the preliminary location and optimized;

h) it is recommended to simulate and optimize the BS locations under the restrictions identified prior to installation. A cell planning tool is recommended for this;

i) perform a site panoramic survey at each candidate site;

j) signal level and carrier to interference plus noise ratio (CINR) at the cell edge should be measured and the expected cell availability measured against the requirements;

k) the effects of the interference, MIMO and sensitivity considerations given in sections 2.5, 2.6 and 2.7 respectively need to be considered;

l) the location of likely handover points also need to be considered in the layout design of an AeroMACS system at an aerodrome. This should be done in such a way that handovers do not occur at locations where communications are anticipated to be critical; and

m) data transmission should be tested at the expected data volumes and latency performance measured against the requirements.

2.3.2.2 *Preliminary data acquisition*

2.3.2.2.1 Coverage requirements

2.3.2.2.1.1 A site survey is required first to identify the areas of the airport to be serviced and the services required. It is critical to match the required services to the geographical areas where they will be served. Working out a workbook of applications stating traffic patterns, required performance

(e.g. latency, ET), and the user profiles authorized is recommended as it will be useful during the siting process to verify the service requirements are covered.

2.3.2.2.1.2 A clear definition of boundaries between airport areas should be stated together with the number of areas to be covered by a BS cell. Cell boundaries do not have to be specified at this moment, however, it may be useful to state the minimum RSSI or CINR values at the cell edge. It may be also useful to point out the preferred handover spots where MS perform handover between cells (recommended to be in spots where a user is expected to run at lower speed).

2.3.2.2.1.3 Traffic patterns should be identified per airport area. These may be related to air traffic volume and patterns (especially in the case of applications served to the aircraft) but not necessarily. Traffic patterns can be defined in terms of user density per surface unit, the number of users per airport area, data rate (bps) density per surface unit, or total data rate per airport area. Note that the data rate needs to be defined for both directions (DL and UL) as it may vary. Dialogues (i.e. instances of an executed service) can also be defined by the number of messages per dialogue, dialogue duration and time between consecutive dialogues.

2.3.2.2.1.3.1 To initiate the evaluation of potential deployment locations on airport property the following will need to be obtained:

a) airport layout drawing and specific information depicting ATC tower location, runway and taxiway configuration, airport terminal buildings, gate location, non-movement areas, maintenance buildings, hangars, cargo operation buildings, fixed base operator locations, fuel storage, and any existing structure that can be used as a host for an AeroMACS system;

b) from the airport authority obtain airport building information including tenant, height, accessibility, services including power and telecommunications;

c) obtain a system design architecture document prescribing the number of base stations to be used in the architecture design document. Architecture design document includes power transmission requirements, recommended antenna system, antenna height recommendations, system diversity and redundancy information;

d) from the air navigation service provider obtain air traffic taxi routes and runway configurations, traffic densities at different times of day, specific configurations used during different seasons such as winter weather operations;

e) from the airline or airport operator obtain gate information including future growth forecasts; and

f) considering system architecture design document and airport layout drawing information, identify candidate locations for base station location that enable service volume coverage specified in the design document. Determine if BSs will be collocated or if there will be two or more base station deployment locations.

2.3.2.2.2 Maps and charts

2.3.2.2.2.1 Prior to conducting a siting exercise, it is important to compile and study current airport maps, obstruction charts, topographical and obstruction data for the airport. Consulting the airport master plans document is an important first step. The airport master plans document represents the airports blueprint for long-term development. This document provides a graphical representation of exiting airport features, future airport development and anticipated land use. Reviewing this document will enable

identification of future obstructions resulting from airport improvements and expansions and enable long-term base station and subscriber station deployment planning.

2.3.2.2.3 Further system architecture considerations

To guide in the design and configuration of an AeroMACS system, detailed performance requirements also need to be considered. These can be found in the AeroMACS MASPS, EUROCAE Doc ED-227.

Note.— These performance requirements given in ED-227 are based on most constraining performance labels specified in ED-228 (RCP130 and RSP160).

2.3.2.3 *Preliminary site selection*

2.3.2.3.1 Airport site investigation

The objectives of an airport site investigation previous to the site selection are to locate and identify available siting property on airport grounds to host BS equipment (and fixed SS equipment, when applicable). Equipment placing is subject to restrictions on:

a) **availability of power interfaces:** Primary and backup power systems, and electrical interfaces appropriate with the BS equipment. Using battery backup systems and electrical protection is recommended to increase the availability of the network;

b) **availability of interfaces to wired communications network:** Provides access to the airport network and connectivity to the ASN-GW. It must not be a public network, but a network owned and operated by the airport or by a third-party telecommunication provider on behalf of the airport. Network interface must be appropriate with the BS equipment (usually Ethernet);

c) **real-estate usage and leasing considerations:** The entity owning the space may be different that the owner of the network. If so, contractual arrangements of the use of space and liability considerations must be taken into account. The usage of the area for antenna siting needs to be authorized by the surface owner and by affected authorities (municipality, airport operator). If the space has to be leased, take into account the leasing cost under operation costs; and

d) **environmental and safety considerations:** All regulations affecting the operation of a radio network need to be complied and documented in terms of environment (introduced pollution, impact to wildlife, visual impact) and safety (radiation health hazard, interference with safety of life operations, accident hazards of components and structure).

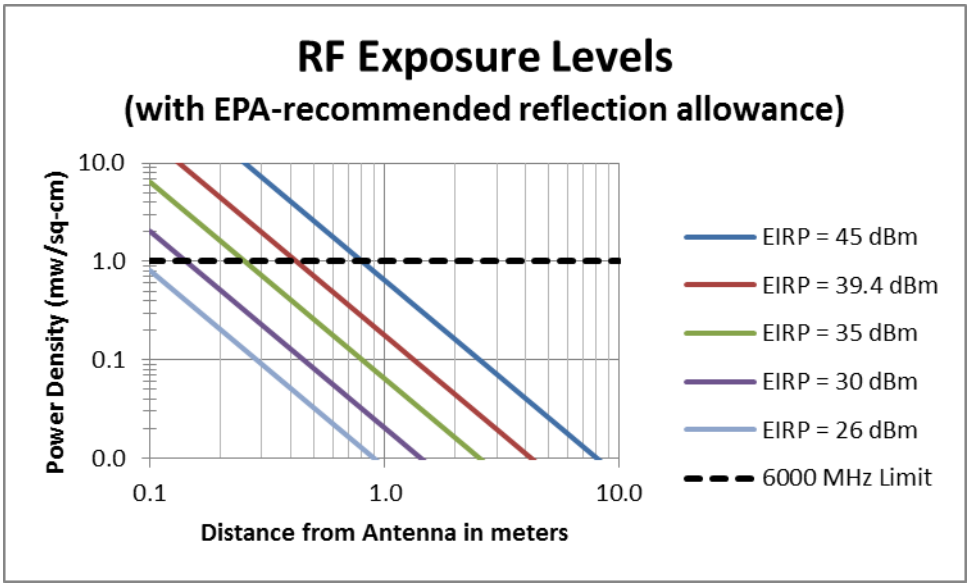


Figure 15. RF exposure levels versus distance from antenna

a) Figure 15 can be found in the United States Federal Communications Commission publication, Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields, OET Bulletin 65, Edition 97-01, August 1997.

b) Site access considerations: Availability of access to the equipment for installation and maintenance needs to be considered and documented. This includes security access requirements, method to access the equipment, and temporary restrictions.

2.3.2.3.2 Preliminary site analysis

The purpose of the site analysis is to determine the most promising candidate site locations for BS and SS, considering if coverage requirements are met, interference with other BS and maintenance accessibility.

2.3.2.3.2.1 Coverage requirements and limitations

Range of a BS on line of sight (LOS) should be maximized by the antenna height and tilt. There should be few obstacles between the antenna and the planned coverage area. Fresnel zone should be respected. Siting consideration requires inclusion of the air operations area (AOA). The AOA includes all areas inside the airport perimeter fence. This includes all areas with restricted access and located outside the airport terminal buildings, including: runways, taxiways, ramps, safety areas, perimeter roads and cargo areas. The AOA consists of the non-movement area and the movement area. Movement areas in the airfield include runways, taxiways and pads. Airport diagrams provide the layout and designations of runways and taxiways. The non-movement area is defined as the taxi lanes and ramp areas not under the control of the air traffic control tower and it consists of aircraft gates, cargo facilities, hardstands (where aircraft often park overnight or for repairs), taxi lanes, perimeter roads, and vehicle drive lanes. This area is also referred to as the ramp, apron, or tarmac. Both aircraft and ground vehicles move on the non-movement area. Specific coverage constraints may be introduced by obstacles on the airport surface, that lead to suboptimal BS locations. It is recommended that such obstacles are well documented in map charts and taken into account in the coverage analysis.

2.3.2.3.2.2 Siting area boundaries

2.3.2.3.2.2.1 Considerations should be given to other BS equipment operating in the same airport and the distance from other BSs that can cause interference should be maximized when possible. At high density sites, in particular, frequency reuse should be used to the maximum extent possible.

2.3.2.3.2.2.2 In order to optimize the number of BSs to be deployed, while achieving an acceptable coverage and capacity performance and minimizing intra-system interference, the use of cell deployment software is encouraged. With such a tool, different configurations of BS siting, antenna direction and frequency reuse plans can be tested.

2.3.2.3.2.2.3 There are two types of service volumes that can be supported by BSs:

a) micro-cells which have smaller service volumes and are typically placed at the gate that provides higher throughput to aircraft and other devices at the ramp area; and

b) macro-cells which have larger service volumes and are typically placed around the airport surface covering more users than a micro-cell and provide less throughput per user.

If users with a heavy throughput requirement are present, such as aircraft stationed at the gates, micro cells could be used to increase throughput.

2.3.2.3.2.3 BS redundancy considerations

In order to increase network availability during the architecture design and overall cell location selection, partial coverage overlap is recommended. AeroMACS SSs follow the IEEE 802.16-2009 threshold-based handover trigger procedures that avoid ping-pong situations. There are a number of instances where cell overlapping creates the potential for path redundancy offering the following advantages:

a) create additional link margin (3 - 6 dB, see section 1.2.1), thus increasing the overall performance of the cell;

b) increased cell area availability, which brings down outage probability especially at the cell edge;

c) introduce an alternative coverage in outage areas due to obstacles on the airport surface blocking LoS from the nearest BS;

d) decrease distance to specific SS with high capacity requirements, thus allowing a higher modulation-coding scheme and increasing throughput; and

e) improve failure mode performance and avoid a single point of failure at the cellular portion of the access network.

2.3.2.3.2.4 Maintenance and installation considerations

BS and SS units should be accessible for maintenance. The cost of installation and maintenance is also an important factor to minimize when possible. If additional structure is required for the equipment installation (e.g. post, wiring, protective structures) it should be taken into account. The following provides a minimum set of considerations for base station installation:

a) **Tower/pole.** Towers and poles should be carefully inspected to ensure they are correctly fabricated with the specified type and size bolts, screws, and fasteners.

b) **Tower grounding, bonding, and lightning protection.** The grounding, bonding, and lightning protection of towers and poles should comply with project specifications and applicable requirements.

c) **Commercial power.** Voltages supplied to the system/equipment should be of acceptable quality and at the correct levels with full loading. Voltages should be satisfactorily regulated and remain within acceptable limits with varying system/equipment loads.

d) **Wiring.** Electrical wiring should be properly installed and of the correct size, type, and colour code.

e) **Lightning protection.** Lightning arresters and surge protectors should be installed on the facility/system/equipment input power circuits, coaxial circuits, control cables, telco circuits, structures, towers, and poles.

f) **Telecommunications (Telco) equipment.** Telco equipment should have been tested for operational acceptability and should meet project specifications. Line quality and levels should be as specified for the facility/system/equipment.

g) **Security.** Locking devices, locks, cores, and keys of the approved types should be installed.

h) **Electromagnetic interference (EMI)/radio frequency interference (RFI).** Proper installation techniques, such as placement of equipment, placement of cables, shielding/grounding of cables, filtering devices, etc., must be employed to the extent practicable so as to ensure that EMI/RFI is held to an acceptable level, i.e. no adverse effect to surrounding facility/system/equipment.

2.3.2.3.2.5 Maintenance

Access to equipment for maintenance is required. Equipment maintenance is required to maximize availability and reliability of air traffic control, communication, navigation and surveillance services. Maintenance personnel require ease of access to electronic equipment to minimize the quantity and duration of interruptions. Additionally, periodic maintenance of communications equipment requires measurement and adjustment of critical parameters for in-service certification and proper access to base station system is required.

2.3.2.4 *Site analysis*

After the preliminary site selection, several candidate spots are chosen. The analysis procedures here should be conducted at each candidate site to select optimum siting locations.

2.3.2.4.1 Site panoramic survey

Once a selection of potential locations has been identified, a panoramic survey is required. The survey needs to focus on the targeted equipment locations with a view to optimizing the direction and orientation of the antenna systems needed to achieve the required performance. The goal of the panoramic surveys is to provide information on potential obstacles, to represent handover areas and support the validation of

the chosen architecture. If the security policy of the airport allows, panoramic photographs will be a useful component of such surveys.

2.3.2.4.2 Coverage analysis

2.3.2.4.2.1 Coverage analysis can be accomplished by utilizing available modelling tools or by analytical link budget calculations.

2.3.2.4.2.2 Link budget calculations can be used to compute analytically whether a specific point at the airport is covered by a BS. Table 3 in section 2.3.1.2.1.3 indicates the maximum signal loss that can be accepted before the point under study is considered in outage. In order to make the calculation, a propagation loss dependent on distance needs to be assumed. A number of propagation loss models can be found in the AeroMACS MASPS (free space, US/LOS, DLR Munich, and SESAR 15.2.7 channel models). It is straightforward to calculate the maximum distance covered by a BS once the parameters above are known.

2.3.2.4.2.3 Computing coverage by analytical link budget calculations has two limitations: a) the propagation loss model is statistics-based and does not take into account losses due to specific obstacles present in or near the line of vision, thus the coverage ranges calculated must be taken as rough estimates; and b) it is not a convenient tool to use to compute resistance to intra-system interference, i.e. differences between desired and undesired signals in reception, from the BS covering the area, and another BS using the same channel (due to frequency reuse) and emitting a non-negligible signal power into the same point of study on the surface.

2.3.2.4.2.4 A radio or cell network modelling software is recommended to use as this allows testing for multiple siting configurations and selecting an optimal solution. The software tool should be able to support propagation loss calculation functions in the AeroMACS spectrum band, ideally for IEEE802.16 or OFDMA frames. The tool should support terrain and obstacle configuration for an accurate airport surface modelling. For multiple cell deployments, the tool should also be able to perform interference computations. Modelling antenna patterns and configuring altitude and pointing angles is also a very recommended feature. The tool should be able to gather statistics on signal quality on reception (CINR, RSSI or equivalent) and ideally per subcarrier/per subchannel signal strength, and peak to average power ratios.

2.3.2.4.3 Traffic analysis

2.3.2.4.3.1 An analysis of capacity constraints in terms of data rate and number of users should be performed at each selected site. The selected base station equipment should satisfy the operational needs identified for the number and type of users at that location.

2.3.2.4.3.2 A limitation is the impact of the asymmetry of the AeroMACS link. Note that using the most symmetric DL/UL ratio (26, 21) in the AeroMACS profile provides a more balanced bi-directional traffic flow. This accommodates at least as much traffic load in the uplink directions as the downlink direction. This is also the desired ratio to maximize the traffic capacity in the uplink direction because other ratios are biased to favour traffic flow in the downlink direction. It is thus recommended to:

a) use appropriate DL/UL ratios in AeroMACS deployments that are expected to use extensively UL capacity; and

b) consider the need to use additional DL/UL ratio links that would support a higher share of the UL capacity. However, this can only be configured for local users that

also support the DL/UL ratio, as interoperability with any device cannot be guaranteed.

2.3.2.4.3.3 Another potential capacity limitation is the size of MAP fields in the DL subframe when the number of users serviced is very high. This can cause the frame to be overpopulated with MAP fields, which have a non-negligible minimum size, and reduce significantly the bandwidth resources dedicated to user services. This effect has not been addressed and requires further study. However, it is worth noting that a certain amount of unbalance in favour of the DL direction may be recommended in order to compensate for this.

2.3.2.4.4 Airport safety area analysis

Deployment considerations near runways and obstacle free zones require careful evaluation. Special siting guidance for runway safety areas and obstacle free zones is provided in publications addressing airport design guidelines. The runway obstacle free zone extends 200 feet (60 meters) beyond each end of the runway and width distances vary depending on approach visibility minimums. For specific information on obstacle free zones refer to Docs 9137, 9157 and 9774.

2.3.2.4.5 Airspace obstruction analysis

Existing airfield buildings and structures have undergone airspace analysis by regulatory authorities to gain deployment approval. Tower or pole structures planned for installations on top of existing building/structures resulting in increased overall structure height require an airspace analysis. For deployments that require construction of new facilities on airfield grounds, an airspace analysis must be conducted to assess if the candidate location complies with existing obstruction regulations. Guidance on obstruction analysis can be found in Docs 9137, 9157 and 9774.

2.3.3 **Case study example**

2.3.3.1 *Information on candidate site*

Objective: Identify suitable locations in airports on airport locations for deployment of base station equipment considering airport wireless architecture design, airport configuration and airport layout plan.

Airport information : Name (withheld)

Number of gates: 65
Number of terminals: 4 (A, B, C and D)
Cargo services: 2
FBO: 1
Airport rescue and firefighting: 1
Hangar facilities: 2
Runway information:

- Runway 6R/24L dimensions: 9 956 x 150 ft./3 035 x 46 m
- Runway 6L/24R dimensions: 9 000 x 150 ft./2 743 x 46 m
- Runway 10/28 dimensions: 6 018 x 150 ft./1 834 x 46 m

Network coverage requirement: Please refer to the following figure (16). The airport operations area (AOA) is shown by a red line and any fixed facilities located within 0.25 miles of the airport perimeter fence are also shown. The blue-shaded regions of Figure 16 indicate coverage challenges where reliable coverage cannot be achieved due to building obstructions, plane and vehicle movement in the immediate area, severe multipath fading and areas that are outside the planned cell radius.

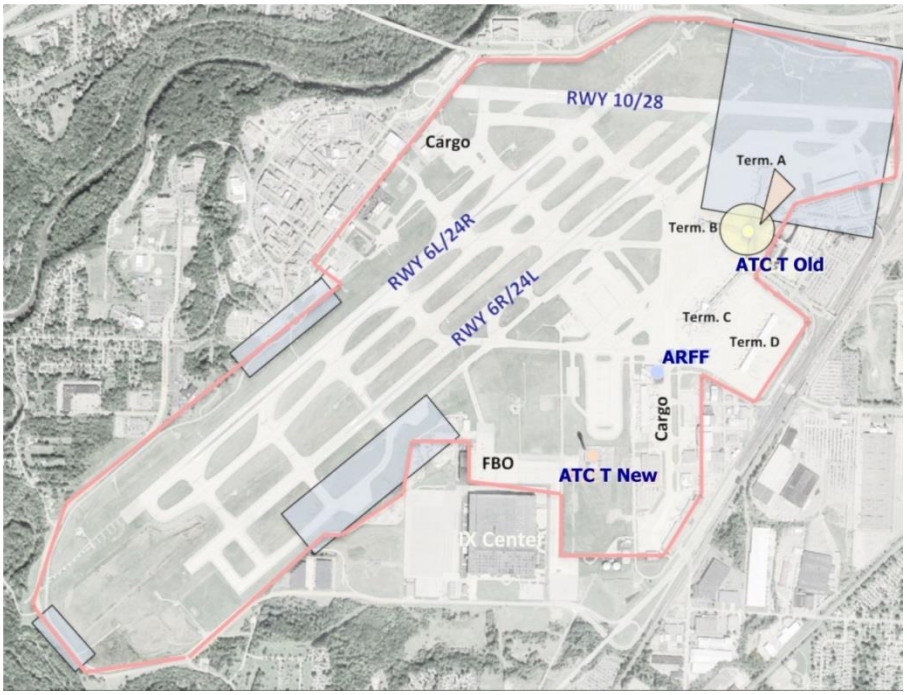


Figure 16. Case study – airport operational areas (AOAs)

Network capacity requirement: Please refer to Figure 17. The AOA area is shown by a red line and the fixed facilities located within 0.25 miles of the airport perimeter fence are also shown. The required capacity of the network for specific locations is indicated by the coloured regions in Figure 17.

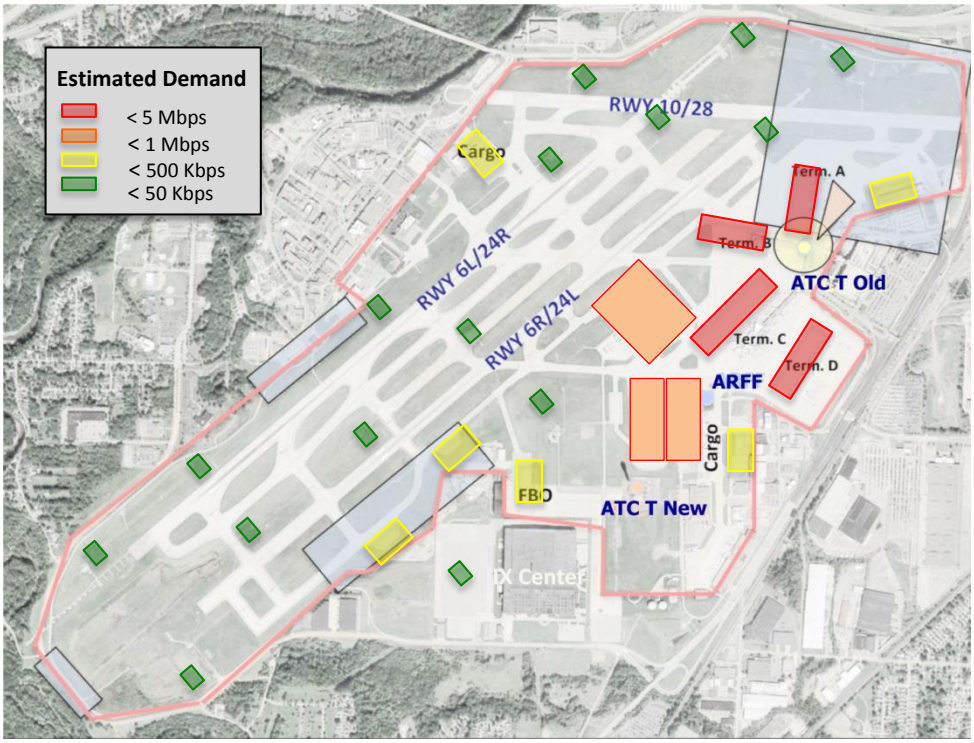


Figure 17. Case study – required capacity at locations within the AOA

2.3.3.2 *Candidate site analysis*

After evaluation of airport layout configuration, coverage requirements, runway and taxiway placement and passenger terminal location, three candidate sites for deployment of base station equipment have been identified. Airport rescue and firefighting, air traffic control tower old (ATCT Old) and air traffic control tower new (ATCT New) have been selected for detail evaluation. The following is a list of specific properties and characteristics for each of the candidate sites:

Location	**ATCT - Old**	**ATCT New**	**ARFF**
Height	198 ft.	324 ft.	60 ft.
Latitude	41D 24’ 40.55” N	41D 24’ 7.35” N	41D 24’ 19.25” N
Longitude	81D 50’ 20.02” W	81D 50’ 53.04” W	81D 50’ 41.72” W
Installation options	Roof - pole structure	Roof - pole structure	Roof
Utility power	Yes	Yes	Yes - not on roof
Standby engine generator	None	Yes	Yes
UPS/PCS/battery backup systems	None	UPS	None

Facility electrical wiring	Yes	Yes	No
Facility/structures grounding	Yes	Yes	No
Lightning and surge protection	Yes	Yes	No
Telco access	Yes	Yes	Yes
Network access	No	Yes	No
Security	Airport badging required	Airport badging required	Airport badging required
Building access	Through terminal building	From street	From street
Access availability	24 hrs	24 hrs	24 hrs
Equipment access	Through tower cab	Through tower cab	Outside ladder
RF antenna colocation	None	VHF, ASDE	None
Installation equipment space - availability	Good	Good	Good
Signal line of sight - movement area	Coverage to all movement area	Coverage to all movement area	
Signal line of sight - non-movement area	Concerns with gates below building	Coverage to all non-movement area	Limited
LoS - obstacles	None	None	Terminal B blocking view of north side of AOA
Future planned construction	None	None	None
Safety	Safety rail available	Safety rail available	None
Radiation health hazard	None	ASDE	None
Lease requirements	Yes	Possible	Yes
Recommended antenna - type			
Reflectors	IX building	IX building	IX building
Notes	Non-movement coverage issue: signal strength immediately below tower structure is a concern.	AOA coverage - excellent	Facility not sufficiently tall to cover AOA

2.3.3.3 *Evaluation and site selection*

ARFF: Coverage investigation of ARFF facility indicates the presence of coverage holes as shown by blue shaded areas in Figure 17. There are four areas in which in both movement and non-movement locations lack signal coverage and this has been determined by measurements conducted. Although there are desirable features in the ARFF building location such as ease of access and security, the facility is not sufficiently tall to cover the full AOA. The optimal installation option is on the roof of the facility and to provide signal coverage to the area of interest, a large tower structure would have to be constructed. Additionally, access to BS equipment for maintenance is difficult given the need to bring an extension ladder for equipment maintenance. Grounding improvements will have to be made to bring facility to code standards.

ATCT Old: Coverage investigation of ATCT Old facility indicates the presence of a coverage hole as shown by the yellow shaded area in Figure 17. Specifically, signal coverage at the base of the building is poor or non-existant. The area of poor coverage includes ramp and gate areas and this deficiency has been identified through measurements. Other areas of the AOA have good line of sight including cargo facilities and perimeter roads. Access to equipment for maintenance or outage restoration is a concern. Maintenance personnel will have to go through airport security to access base station equipment and this may impact equipment time to repair during system outage. A power back up and engine generator is not available at this location.

ATCT New: Coverage investigation of ATCT New facility indicates the presence of a coverage problem as shown by the orange shaded area in Figure 17. Specifically, signal coverage deficiency affects a ramp and gate area in Terminal A. All other AOA areas are well covered. Signal coverage determination has been made through site visits and airport layout analysis. The ATCT New is a state of the art facility providing access to a reliable grounding system and conditioned power. ATCT New is not co-located with the passenger terminal building, thus with proper coordination access to base station equipment for maintenance or restoration is not a challenge.

2.3.3.4 *Recommendation*

Evaluation of airport maps, coverage areas, facility access, maintenance, deployment and others yielded an optimal location for base station deployment at the airport. The ATCT New location has been selected as primary choice for base station equipment deployment with the recommendation of deploying one BS at ATCT Old to improve coverage to the Terminal A area. This configuration will enable redundant coverage in selected areas. The second option for deployment is ATCT Old. Both ATCT New and ATCT Old are very good choices for base station deployment. However, there are a few important factors that elevate ATCT New location as the top candidate. ATCT New is the tallest structure located near the geographical centre of the airport. By design, the top of ATCT New provides optimal line of sight for air traffic controllers and this is also advantageous for signal propagation. Additionally, ATCT New provides the best access to conditioned power, proper grounding, access for equipment maintenance, telco services and provides high facility security. ATCT New meets existing requirements and should be able to accommodate any future site requirements.

2.4 CAPACITY PLANNING

2.4.1 Introduction

2.4.1.1 This section provides the results of a qualitative investigation of the capacity of an AeroMACS access network in terms of the maximum number of users able to be accommodated in such a network under normal conditions. The constraints on the number of users are analysed according to two possible limitations: a) maximum number of registered users in AeroMACS BS and ASN-GW; and b) the number of users considering the maximum throughput supported by the access network and compared to the required throughput per user. This information is provided as guidance for future implementers of AeroMACS systems.

2.4.1.2 Guidance is provided on the overall system capacity and in particular in relation to the number of users that can be supported by an AeroMACS access network under an acceptable level of service.

2.4.1.3 Acceptable level of service is defined here as a situation where the system is not under congested status. In the context of this paper, congestion occurs when the system cannot offer enough capacity for an additional user and it will reject any additional user entry. The level of available capacity reaching congestion differs with the scenarios and the assumptions for the communication requirements of the serviced users.

2.4.1.4 In this analysis, "user" is defined as the application client connected to the AeroMACS service network through a mobile station (MS). Each user runs a number of services described in the scenarios considered in section 3.2. In this analysis, users can be aircraft, surface vehicles and various types of fixed stations.

2.4.1.5 It needs to be noted that this study is a qualitative analysis on the capacity that an AeroMACS access network can provide under a number of assumptions. The objective is not to quantify the absolute maximum number of users that can be supported, neither to derive operational or technical requirements.

2.4.1.6 In general in an AeroMACS network, user access constraints may result from two possible factors:

a) **User registration constraints:** The BS and ASN-GW are the two types of devices that enable the AeroMACS access network. These two devices are limited by design to a number of supported users that are given access service. This limitation depends on the manufacturer design.

b) **Throughput constraints:** Radio access provided by a BS to the MSs covered in the corresponding cell uses the limited throughput resources of the 5 MHz-wide radio channel configured in the cell. Assumptions are taken about the types of MS devices that consume different levels of a throughput and modulation scheme in order to calculate a number of users that allows all the MSs in the cell to be given an acceptable level of service.

2.4.1.7 This section addresses the two constraints mentioned above. For the throughput constraint analysis, a user characterization and scenario definition is worked out before the analytic results are presented.

2.4.2 User registration constraints

2.4.2.1 The maximum number of users that can be supported per ASN-GW and BS is limited due to the size of the database used to register the number of MS (MAC addresses or other parameters). From the ASN-GW perspective, some products are scalable, meaning in number of boards and distributed architecture, hence configurations for thousands of users are possible. Thus, the limitation in number of registered users will probably not be an issue for all systems.

2.4.2.2 BS may impose stricter limits in the number of subscribers registered to operate in the BS radio channel.

2.4.3 Throughput constraints

2.4.3.1 The throughput limitation of the AeroMACS access network occurs at the cell level on each specific radio channel in use; i.e. it is driven by each BS in the network independently. The analysis of this limitation is performed here qualitatively and provides general guidance in the order of magnitude of the throughput limitation given certain assumptions. If a precise result is needed, simulations or field tests should be performed for a specific deployment.

2.4.3.2 In order to calculate the maximum number of users in a cell limited by throughput, a three-step process is followed:

a) first, the throughput needs are defined depending on the type of user and the throughput supported by BS;

b) second, scenarios are defined which specify the ratio of each type of user that is foreseen per BS; and

c) third, results are calculated analytically indicating the maximum number of users supported in each scenario.

2.4.4 User and BS characterization

2.4.4.1 This section defines the average and maximum application level bitrate generated in DL and UL directions per type of user that can be found at the airport, and the maximum bitrate supported by a BS giving access to such users to the AeroMACS access network.

2.4.4.2 The capacity analysis has assumed the following device configurations:

a) **Aircraft at the gate:** Represents modems installed in aircraft. Considering both safety and non-safety applications all identified types of connections are recommended for aircraft except video. The aircraft is at the gate and executing the pre-departure and post-arrival applications necessary for the turnaround process.

b) **Aircraft at hangar, taxiway or runway:** Same as above but the aircraft is executing turnaround processes at the ground movement area or maintenance operations.

c) **Surface vehicle:** Represents devices hosted on all ground support vehicles including passenger vans/buses, dollies carrying cargo, refuel trucks, catering vehicles and push back tugs/ tractors, etc. Generally, most of these vehicles are equipped with PTT phones. In addition, A-SMGCS (advanced surface movement guidance and control system) may require a safety link for exchanging vehicle’s position information on a periodic basis to a centralized control system.

d) **Video sensor:** Represents devices for sending videos during emergency situations.

e) **Ground critical:** Represents devices used to monitor/control ground equipment that are deployed for critical ATS services. Example: landing systems, runway lighting controls, etc.

f) **Ground default:** All other ground equipment falls under this default category.

2.4.4.3 Table 7 provides the average and peak throughput requirements at the application level for each of these types of user. The bitrate for aircraft is based on the AeroMACS MASPS, for the others it is determined based on expected application load and video/audio codec configuration.

	Average [1] application bitrate		**Peak [2] application bitrate**	
	FL (GS->MS)	**RL (MS->GS)**	**FL (GS->MS)**	**RL (MS->GS)**
Aircraft at gate[3]	150 kbps	150 kbps	600 kbps	300 kbps
Aircraft at hangar, taxiway or runway[3]	20 kbps	40 kbps	40 kbps	100 kbps
Surface vehicle	8 kbps	10 kbps	16 kbps	20 kbps
Video sensor[4]	1 kbps	64 kbps	4 kbps	512 kbps
Ground critical	1 kbps	1 kbps	4 kbps	8 kbps
Ground default	1 kbps	1 kbps	4 kbps	4 kbps

Table 7. Device classes

2.4.4.4. In order to calculate the throughput limitations in a BS, the modulation/coding rate and the DL/UL OFDM symbol ratio needs to be derived. Table 8 of the AeroMACS MASPS shows the application data rate (TCP/IP PDU throughput) in a BS depending on the modulation/coding scheme used. Note that these results were obtained by applying (32, 15) DL/UL OFDM symbol rate. The rate (26, 21) is also considered in this study as the most symmetrical DL/UL configuration mandated in the AeroMACS profile. The throughput resulting from this configuration is approximated in Table 9.

1 Using median (50th percentile) is recommended for capacity estimations. Average can lead to wrong conclusion if the traffic demand is not distributed uniformly over time.

2 "Peak" refers to 95th percentile.

3 Aircraft data requirements in line with MASPS.

4 Video works at 360p at 24 FPS and supports compression in low image refresh periods.

MC scheme	Downlink [kbps]	Uplink [Kbps]
QPSK1/2	983.3	532.4
16QAM1/2	2153.52	1235.52
64QAM1/2	3595.04	1758.48

Table 8. AeroMACS expected TCP/IP throughputs vs modulation schemes for DL/UL OFDM symbol rate (32, 15)

MC scheme	Downlink [kbps]	Uplink [kbps]
QPSK 1/2	824.7	698.77
16QAM 1/2	1806.18	1621.62
64QAM 1/2	3015.19	2308

Table 9. AeroMACS expected TCP/IP throughputs vs modulation schemes for DL/UL OFDM symbol rate (26, 21)

2.4.4.5 The same BS can support different types of cells depending on the cell position and desired coverage:

a) A BS supporting a micro-cell is placed at the gate and gives mainly high-capacity to aircraft and other devices at the ramp area with a limited service range (covering about three to five gates). It is assumed that 75 per cent of the users are within range to be serviced by 64 QAM 1/2 and the rest by 16 QAM 1/2

b) A BS supporting a macro-cell is placed around the airport surface and gives high-range coverage to most of the airport surface areas. Table 10 shows the result of the total supported throughput in both directions with the proportion of modulation/coding rates used. It is assumed that 20 per cent of the users are within range to be serviced by 64 QAM 1/2, 40 per cent by 16 QAM 1/2 and 40 per cent by QPSK 1/2.

	Modulation/code scheme	**Supported throughput (Mbps) at (32, 15) DL/UL rate**	**Supported throughput (Mbps) at (26, 21) DL/UL rate**
BS in the micro-cell	64 QAM 1/2 (75 per cent users) 16 QAM 1/2 (25 per cent users)	3.3/1.7	2.7/2.1
BS in the macro-cell	64 QAM 1/2 (20 per cent users) 16 QAM 1/2 (40 per cent users) QPSK 1/2 (40 per cent users)	2/1	1.7/1.4

Table 10. Cell types and maximum throughput

2.4.5 Scenario description

2.4.5.1 This section describes likely scenarios of the AeroMACS access network. Scenarios are defined by the placement of the BS in the airport surface and the proportion of users of each type present on the airport surface. Both factors define the ratio of each user that is present in each BS on the surface.

a) **Scenario 1.** Video surveillance - Represents a scenario in which AeroMACS is used solely to support fixed video surveillance cameras for security control and operation safety monitoring and record.

b) **Scenario 2A.** Integrated surface management system - Represents a scenario in which video, sensor networks and surface vehicles are functioning on the airport surface executing local applications enabling A-SMGCS and surface operation support.

c) **Scenario 2B.** Same as Scenario 2A but without video surveillance sensors.

d) **Scenario 3A.** Surface management and aircraft turnaround - Represents a scenario with local services as above and enables CPDLC and AOC applications with on-board subscribers on the aircraft to support the turnaround process and maintenance. For simplicity it is assumed that aircraft at the gates occupy all the resources of the dedicated micro-cells at the gates.

e) **Scenario 3B.** Same as Scenario 3A but without video surveillance sensors.

2.4.5.2 Table 11 below indicates the proportion of cell bandwidth dedicated to each type of users serviced by a BS in each of the scenarios considered.

AeroMACS Scenarios	Percent A/C at gate	Per cent hangar, taxiway or runway	Per cent surface vehicles	Per cent video sensors	Per cent ground critical	Per cent ground default
Scenario 1	-	-	-	100	-	-
Scenario 2A	-	-	30	50	10	10
Scenario 2B	-	-	80	-	10	10
Scenario 3A	100 (only micro-cells)	50	15	30	2.5	2.5
Scenario 3B	100 (only micro-cells)	70	25	-	2.5	2.5

Table 11: AeroMACS network scenarios considered and percentage of throughput dedicated to each user type

2.4.5.3 The results on capacity are given per BS in this study. In order to derive aggregate capacity in an entire AeroMACS access network, airport categories are based on number of movements and may be used to define the amount of BSs deployed on the airport surface. The following airport size types are assumed for this capacity analysis:

a) small (20 operations/hour) – 3 BS;

b) medium (50 operations/hour) – 9 BS; and

c) large (100 operations/hour) – 15 BS.

2.4.5.4 When calculating the aggregate capacity in the entire AeroMACS network, the limitation of eleven channels available for transmission needs to be taken into account.

2.4.6 **Analysis results (for capacity constraints)**

2.4.6.1 Each scenario is defined by a data rate required per user type and a proportion of user types. The results of the analysis are given in the form of number of users than can be reasonably supported by a BS. Given all the assumptions in the previous sections, the maximum number of users is derived for each scenario based on the user throughput requirements to be able to serve given the user type ratio in the scenarios given in Table 11. The maximum number of users for each case is given in Tables 12 to 21. Note that a margin is left in the form of unused throughput in order to account for a certain amount of peak traffic that may be caused by a user in the cell. The level of margin assumed per cell is based on the peak throughput requirements in Table 10.

2.4.6.2 Tables 12, 13, 14, 15 and 16 below identify the resulting maximum number of users for the different scenarios and different DL/UL ratios considered.

Type of cell	**#Video sensors**	**Remaining throughput (margin)**	
		DL	**UL**
Micro	18	3.28 Mbps (99.5 per cent)	548 kbps (32.2 per cent)
Macro	7	1.99 Mbps (99.6 per cent)	552 kbps (55.2 per cent)

Table 12. Maximum number of users (per channel) - Scenario 1, DL/UL OFDM symbol rate (32, 15)

Type of cell	**#Video sensors**	**Remaining throughput (margin)**	
		DL	**UL**
Micro	24	2.67 Mbps (99.1 per cent)	564 kbps (26.8 per cent)
Macro	13	1.69 Mbps (99.2 per cent)	568 kbps (40 per cent)

Table 13. Maximum number of users (per channel) - Scenario 1, DL/UL OFDM symbol rate (26, 21)

Type of Cell	#Surface vehicles	#Video sensors	#Ground critical	#Ground default	Remaining throughput (margin)	
					DL	UL
Micro	35	9	115	115	2.75 Mbps (83.3 per cent)	544 kbps (32 per cent)
Macro	13	3	45	45	1.8 Mbps (90 per cent)	588 kbps (58.8 per cent)

Table 14. Maximum number of users (per channel) - Scenario 2A, DL/UL OFDM symbol rate (32, 15)

Type of cell	#Surface vehicles	#Video sensors	#Ground critical	#Ground default	Remaining throughput (margin)	
					DL	UL
Micro	50	12	150	150	1.98 Mbps (73.6 per cent)	532 kbps (24.6 per cent)
Macro	20	8	65	65	1.4 Mbps (82.4 per cent)	558 kbps (39.8 per cent)

Table 15. Maximum number of users (per channel) - Scenario 2A, DL/UL OFDM symbol rate (26, 21)

Type of cell	#Surface vehicles	#Ground critical	#Ground default	Remaining throughput (margin)	
				DL	UL
Micro	143	115	115	1.93 Mbps (58.4 per cent)	40 kbps (2.4 per cent)
Macro	87	45	45	1.21 Mbps (60.5 per cent)	40 kbps (4 per cent)

Table 16. Maximum number of users (per channel) - Scenario 2B, DL/UL OFDM symbol rate (32, 15)

Type of cell	#Surface vehicles	#Ground critical	#Ground default	Remaining throughput (margin)	
				DL	UL
Micro	176	150	150	0.9 Mbps (36.7 per cent)	40 kbps (2 per cent)
Macro	123	65	65	586 kbps (34.5 per cent)	40 kbps (3 per cent)

Table 17. Maximum number of users (per channel) - Scenario 2B, DL/UL OFDM symbol rate (26, 21)

Type of cell	#A/C at gate	#A/C at hangar, taxiway, runway	#Surface vehicles	#Video sensors	#Ground critical	#Ground default	Remaining throughput (margin)	
							DL	UL
Micro	9	-	-	-	-	-	1.9 Mbps (59 per cent)	350 kbps (25 per cent)
Macro	-	5	5	2	35	35	1.83 Mbps (91.5 per cent)	552 kbps (55.2 per cent)

Table 18. Maximum number of users (per channel) - Scenario 3A, DL/UL OFDM symbol rate (32, 15)

Type of Cell	#A/C at gate	#A/C at hangar, taxiway, runway	#Surface vehicles	#Video sensors	#Ground critical	#Ground default	Remaining throughput (margin)	
							DL	UL
Micro	12	-	-	-	-	-	900 kbps (33.3 per cent)	300 kbps (14.3 per cent)
Macro	-	11	10	4	35	35	1.3 Mbps (78 per cent)	534 kbps (38.1 per cent)

Table 19. Maximum number of users (per channel) - Scenario 3A, DL/UL OFDM symbol rate (26, 21)

Type of cell	#A/C at gate	#A/C at hangar, taxiway, runway	#Surface vehicles	#Ground critical	#Ground default	Remaining throughput (margin)	
						DL	UL
Micro	9	-	-	-	-	1.9 Mbps (59 per cent)	350 kbps (25 per cent)
Macro	-	8	10	35	35	1.69 Mbps (84.5 per cent)	510 kbps (51 per cent)

Table 20. Maximum number of users (per channel) - Scenario 3B, DL/UL OFDM symbol rate (32, 15)

Type of cell	#A/C at gate	#A/C at hangar, taxiway, runway	#Surface vehicles	#Ground critical	#Ground default	Remaining throughput (margin)	
						DL	UL
Micro	12	-	-	-	-	900 kbps (33.3 per cent)	300 kbps (14.3 per cent)
Macro	-	15	20	35	35	770 kbps (59.2 per cent)	530 kbps (37.8 per cent)

Table 21. Maximum number of users (per channel) - Scenario 3B, DL/UL OFDM symbol rate (26, 21)

2.4.7 Results/conclusions

2.4.7.1 This analysis gives qualitative guidance on the number of users that can be serviced by an AeroMACS access network. The study is based on a number of assumptions on the bitrate requirements by the different users considered and on the cell deployment at the airport surface. Four scenarios are considered based on different assumptions.

2.4.7.2 The analysis does not intend to derive requirements on user service or cell siting. Such aspects of the AeroMACS implementation are left to the discretion of the network owner. This study does provide guidelines on the possible limitations that an access network may have. The main capacity constraints occur in the UL direction in macro-cells. The number of users being serviced in this direction can be significantly dropped especially when servicing video sensors in the cell.

2.4.7.3 The number of users that can be supported is mainly limited by channel throughput constraints. According to the results of this analysis, the maximum number of supported users for the different type of cells can be considered within the following ranges:

a) micro cells: up to 24 video sensors, or up to 170 surface vehicles, or up to twelve aircraft stationed at the gate and about 300 sensors.

b) macro cells: up to 13 video sensors, or up to 120 surface vehicles, or up to eleven aircraft and about 130 sensors.

2.4.7.4 Note that throughput margins should be left available in a BS, as was done in the scenarios considered in this paper, in order to cope with peak traffic. Video peak traffic can be particularly high and requires a large margin of available throughput (512 kbps assumed).

2.4.7.5 The analysis shows that micro cells are best suited to cover an area with many users within a small range (such as the gate area), while macro cells cover larger areas with less users (such as airport movement or maintenance areas).

2.4.7.6 If users transmitting a heavy bitrate are present, such as video sensors or aircraft stationed at the gates, micro cells can be used to increase capacity to two to three times compared to the capacity provided using macro cells. However, this is subject to restrictions on:

a) number of BSs intended to be deployed (including frequency reuse limitations);

b) availability of BS sites in the required areas (note that the micro cell has a limited range); and

c) availability of network connections in the required sites.

2.4.7.7 Another technique to increase the cell throughput is to reduce the BS range (applying cell siting) in order to increase the likely modulation code and thus increase the overall capacity of the cell. This can be done via cell coverage overlap and load balance. In such a case, attention must be paid to the limitation in the number of available channels which may lead to frequency reuse and increased interference between cells.

2.4.7.8 When a large number of users transmitting a low bitrate is present (such as sensors), the limitation is not the cell throughput but the maximum number of users allowed to be registered in the BS equipment.

2.4.7.9 Another relevant conclusion of this analysis is the impact of the asymmetry of the AeroMACS link. Note that, using the most symmetric DL/UL ratio (26, 21) in the AeroMACS profile the number of users supported increases significantly. This is due to the fact that the UL direction has at least as much traffic load as the DL direction in the scenarios of this analysis. This situation may occur in operational deployments, especially if video sensors or aircraft are present. It is thus recommended to:

a) use appropriate DL/UL ratios in AeroMACS deployments that are expected to use extensively UL capacity; and

b) consider the need to identify additional DL/UL ratio links (possibly in a future revision of AeroMACS standards) that would support a higher share of the UL capacity.

2.5 SPECTRAL MASK AND EMISSIONS

2.5.1 Section 7.4.5 of the SARPs provides the Standards for the spectral mask and emissions.

2.5.2 The appendix to this manual provides a test procedure to ensure that these requirements are met. The test procedure is included in this manual as it shows key steps, such as:

a) how to avoid deterioration of testing accuracy caused by characteristics of the IF filter provided in the spectrum analyser; and

b) how to set up the 0dB reference for the spectrum mask measurement.

2.6 MANAGEMENT OF INTERFERENCE

2.6.1 Interference avoidance measures for AeroMACS

2.6.1.1 The ITU allocated the band, 5 030 to 5 150 MHz to AM(R)S. Currently, the 5 091 to 5 150 MHz band is the primary band targeted for AeroMACS implementation worldwide. In addition, AeroMACS networks can also operate in the 5 000 to 5 030 MHz band on a regional basis. The number of channels available for each airport system implementation will depend on the international and regional channel allocation rules. The number of channels available for each system may be limited due to potential interference with the Globalstar satellite system and/or policies and procedures specific to a host State. For example, the CAA may or may not allow combining ATC and AOC traffic on the same network or the same set of channels. Should the requirement to separate ATC and AOC traffic onto different channels be imposed, the number of channels available for each network would be further limited.

2.6.1.2 The number of BSs required for each AeroMACS implementation will depend on the size of the geographic area to be covered and the volume of traffic the system needs to support. A system or part of a system may be implemented with sectorized coverage where the region around a BS is divided into sectors of coverage through the use of directional antennas and an AeroMACS transceiver for each antenna.

2.6.1.3 Implementation of frequency reuse will be required if the number of BSs exceeds the number of available channels or if there is a need to support higher volumes of traffic, thus placing more than one channel on each BS. A frequency reuse scheme, i.e. how often each frequency is reused, will depend on a specific system implementation and will require managing intra-system interference.

2.6.1.4 Interference must be managed if the system is to comply with the requirements outlined in the AeroMACS SARPs. This will likely translate into avoiding adjacent channel assignments on different sectors of the same site in a sectorized scenario. Co-channel assignments will need to be separated as far as feasible avoiding overlapping coverage.

2.6.1.5 Various interference mitigation techniques are available to a system designer and operator including, but not limited to, antenna downtilt, transmit power reduction, antenna height variations, and careful site placement taking advantage of signal attenuation and blocking. Smaller sites, i.e. smaller coverage areas, would make signal propagation easier to control but would result in a greater number of BSs per airport thus necessitating increased frequency reuse. Additionally, mobility management techniques are available to minimize potential interference effects.

2.6.2 AeroMACS planning against interference

2.6.2.1 *AeroMACS planning method*

2.6.2.1.1 AeroMACS service areas should be planned on the basis that the desired signal power level (in dBm) at the receiver input inside a service area should exceed the AeroMACS receiver sensitivity by the quantity 10log(1+(I/N)):

Desired signal level ≥ Sensitivity + 10 log (1+ (I/N)).

where:

a) I is the cumulative mean interference power, adjusted to the selectivity of the RF and IF sections of the AeroMACS receiver;

b) N is the total mean noise power in the IF bandwidth; and

c) in the above expression, both I and N are expressed in non-logarithmic units (mW) and are referred to the receiver input.

2.6.2.1.2 It should be noted that the total mean noise power (N) in dBm equals the level of thermal noise (N_{th}) plus the receiver's noise figure (NF). The thermal noise in dBm is:

$$N_{th} = 10\log(KTB) + 30,$$

where K is Boltzmann's constant (1.38 × 10-23 J/K), T is the absolute temperature of the receiver (in Kelvin) in and B is the bandwidth of the receiver (in Hz).

For a 5 MHz bandwidth, N_{th} = -107.0 dBm and for NF = 8 dB, the level of the total mean noise power equals N=-99.0 dBm.

2.6.2.1.3 The ratio I/N equals the relative increase (ΔT/T) of the receiver noise temperature due to interference. Because the quantities I and N contain the effect of filtering, the ratio I/N can be thought of as applying to the IF output as well.

2.6.2.2 *Application of the planning method*

2.6.2.2.1 The first choice the network designer has to make is over the maximum value of the ratio I/N.

2.6.2.2.2 The greater the value of this ratio, the more tolerant will be the AeroMACS network to interference. Caution needs to be exercised on increasing the value of this ratio as the greater the value of this ratio, the higher the required level of the desired signal at the AeroMACS receiver. Consequently for a given maximum BS EIRP, the higher the desired signal at the receiver, the smaller the effective range of the base station.

2.6.2.2.3 It needs to be emphasized that "I" represents the cumulative interference. Hence the network designer has to consider all possible interference sources that may affect simultaneously the most vulnerable point of the network. In particular the cumulative interference "I" includes the co-channel and adjacent-channel interference due to other AeroMACS emissions.

2.6.2.2.4 The existence of AeroMACS deployments in nearby airports (current or future planned) should be investigated. It is recommended that local airports at a distance within the radio horizon are considered and, if an interference level is deemed relevant, readjustments are made to the channels available in each deployment.

2.6.2.2.5 The next step would be to allocate weights p_j to the various concurrent interference threats where:

$$\Sigma_j \, p_j = 1.$$

2.6.2.2.6 For each individual interference threat, the power threshold I_j (in dBm) at the input of an AeroMACS receiver, when adjusted to the selectivity of the RF and IF sections of the AeroMACS receiver, is then calculated as follows:

$$I_j = I + 10\log(p_j) = N + 10\log(I/N) + 10\log(p_j),$$

where in the term 10log (I/N), I and N are expressed in non-logarithmic units.

2.6.2.2.7 The individual power threshold I_j can be subsequently utilized for the determination of the threshold of the unadjusted interference power at the input of an AeroMACS receiver and thus for the calculation of the required separation in terms of distance and/or frequency between the AeroMACS receiver and the source of interference.

2.6.2.2.8 As an illustration, suppose that the choice I/N=1 is made for a given option of the modulation (QAM) scheme and that there exists interference from (a) one AeroMACS adjacent channel, (b) an off-channel telemetry application and (c) an MLS facility in the same airport.

Suppose that the choices for p_j are :

$$p_{AeroMACS} = 0.4,\ p_{ATM} = 0.3,\ p_{MLS} = 0.3$$

The interference thresholds in dBm corresponding to each threat would then be:

$$I_{AeroMACS} = I + 10\log(p_{AeroMACS}) = I - 4.0 = N - 4.0 = -103.0 \text{ dBm},$$
$$I_{ATM} = I + 10\log(p_{ATM}) = I - 5.2 = N - 5.2 = -104.2 \text{ dBm},$$
$$I_{MLS} = I + 10\log(p_{MLS}) = I - 5.2 = N - 5.2 = -104.2 \text{ dBm}.$$

2.6.2.2.9 As for the determination of the unadjusted interference power threshold due to AeroMACS adjacent-channel emissions, it is noted that for I/N = 1 one can benefit directly from the implications of the AeroMACS adjacent-channel performance requirements because they are valid subject to the same condition (I/N=1). In this case, if the only source of interference is an AeroMACS transmitter on the adjacent channel, the power of the adjacent-channel transmission at the receiver input, which is required to produce I=N, equals the power of the desired transmission (sensitivity + 3dB) plus the so called adjacent-channel rejection R. In reference to the above example, there follows that the power level P_{adj} of the adjacent-channel transmission at the receiver input that is required to produce an adjusted-by-filtering value of $I_{AeroMACS} = N - 4 = -103.0$ dBm, is given by:

$$P_{adj} = \text{sensitivity} + 3\text{dB} + R - 4\text{ dB} = \text{sensitivity} + R - 1\text{ dB}.$$

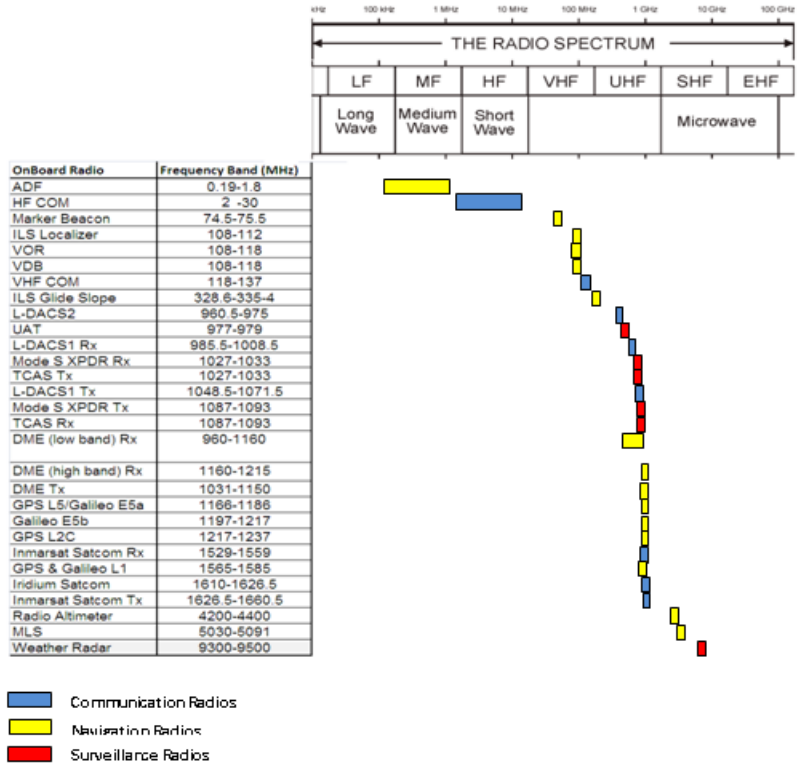
2.6.2.3 *Sensitivity under mobility conditions and impact on interference planning*

2.6.2.3.1 When a mobile station moves with velocity *v*, the errors in the decoding of received signals come not only from the noise and the interference at the receiver but also from the doppler effect. The amount of noise at the receiver does not change with the motion. However, the error is increased in comparison with the static situation as a result of inter-symbol interference due to the doppler effect. If for instance we chose to allocate the same rms doppler error as for the noise, it would be necessary to double the power of the desired signal compared to its level in the static case, so that the ratio of the total rms error to the amplitude of the desired signal remains as in the static situation. Hence in this case the sensitivity of the receiver would be higher by 3 dB and this should also be considered in the planning against interference. The need for a higher desired signal at an AeroMACS receiver to account for doppler effects would further decrease the range of an AeroMACS BS (assuming the same maximum EIRP level as in the static case). It is noted that a higher allocation of error to the doppler effect in order

to cover the mobility requirements would necessitate a further increase in the level of the desired signal at the receiver.

2.6.2.4 *Interference from/to AeroMACS to/from avionics*

2.6.2.4.1 The RF interference environment applicable to the AeroMACS radio is comprised of onboard RF transmitters whose RF emissions may have an impact on the design and performance of the AeroMACS radio receiving function and other onboard RF receivers whose performance may be affected by RF emissions from the AeroMACS radio. The following figure provides a list of those transmitters and the frequencies on which they operate.



OnBoard Radio	Frequency Band (MHz)
ADF	0.19-1.8
HF COM	2 -30
Marker Beacon	74.5-75.5
ILS Localizer	108-112
VOR	108-118
VDB	108-118
VHF COM	118-137
ILS Glide Slope	328.6-335.4
L-DACS2	960.5-975
UAT	977-979
L-DACS1 Rx	985.5-1008.5
Mode S XPDR Rx	1027-1033
TCAS Tx	1027-1033
L-DACS1 Tx	1048.5-1071.5
Mode S XPDR Tx	1087-1093
TCAS Rx	1087-1093
DME (low band) Rx	960-1160
DME (high band) Rx	1160-1215
DME Tx	1031-1150
GPS L5/Galileo E5a	1166-1186
Galileo E5b	1197-1217
GPS L2C	1217-1237
Inmarsat Satcom Rx	1529-1559
GPS & Galileo L1	1565-1585
Iridium Satcom	1610-1626.5
Inmarsat Satcom Tx	1626.5-1660.5
Radio Altimeter	4200-4400
MLS	5030-5091
Weather Radar	9300-9500

Figure 18. Aeronautical radio spectrum used by aircraft

2.6.2.4.2 Radios that require transmission of RF signals to provide the required service generate out-of-band emissions which affect the performance of the functions of other onboard RF receivers. Therefore whenever a new RF system that includes an RF transmitter and/or receiver is added to an aircraft installation, it is important to evaluate the impact that the new RF transmitter will have on the performance of the other onboard RF receivers and the impact that other onboard RF transmitters will have on the new RF receiver.

2.6.2.4.3 Figure 19 provides an illustration of various radios that may be installed to provide each of the functional categories of services described below.

Fig-X

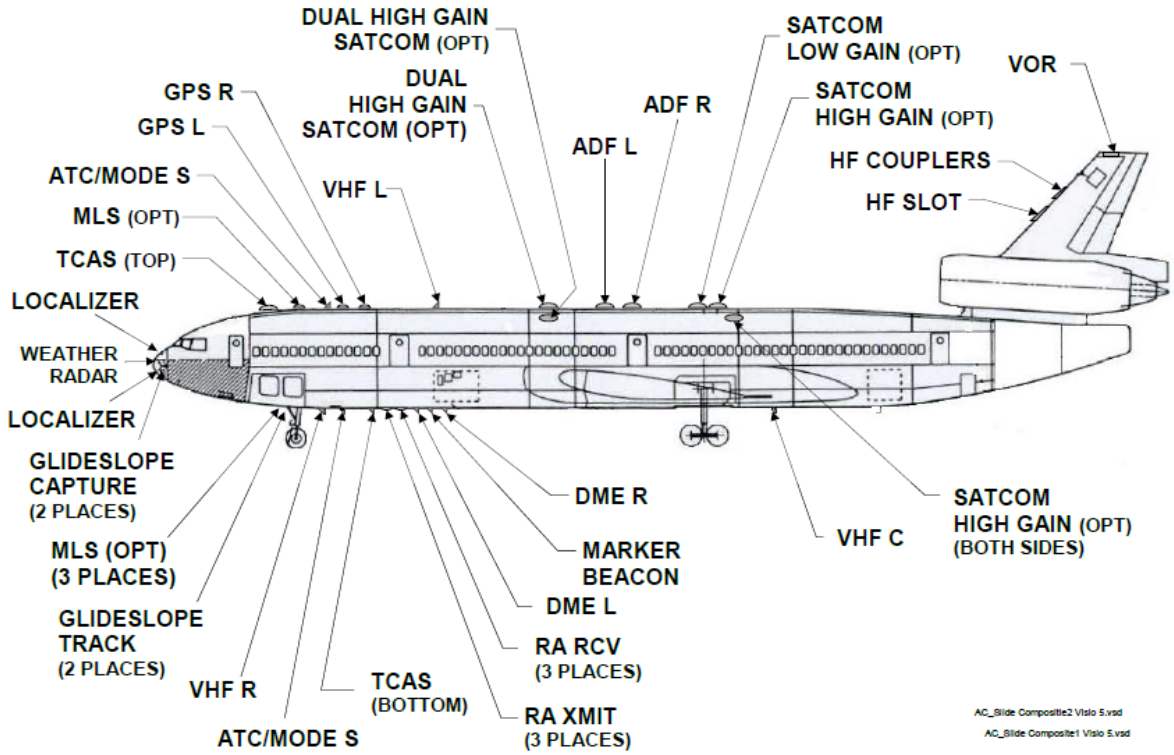


Figure 19. Typical aircraft antenna farm

2.6.2.4.4 An analysis done on the electromagnetic compatibility issues of installing an AeroMACS radio on aircraft equipped with other on-board communications, navigation and surveillance radios concluded on the following points:

a) AeroMACS spurious and broadband emissions that are merely compliant with the emissions mask defined in the AeroMACS profile [2] will produce interference levels requiring more than 110 dB of isolation between the AeroMACS transmitter and other onboard receivers such as GNSS receivers, COM and surveillance radio receivers. It is highly difficult to achieve that much isolation between the AeroMACS antenna and other Rx antennas on the aircraft. Hence, additional reduction of 5 to 70 dB in the AeroMACS emissions below 2 GHz is recommended; and

b) another important observation is that the minimum isolation required between an AeroMACS receiver and L-Band transmitters like Mode S, transponders and TCAS are also very high at 113 dB and 114 dB[1] respectively. It may be difficult to achieve such isolation at the aircraft only by spacing AeroMACS antenna away from the Mode S and TCAS antennas. Hence, TCAS and Mode S transmissions may have some impact on AeroMACS radio performance. Since the interference is due to the broadband emissions that fall within the operating range of the AeroMACS receiver, it is impossible to evade such interference from these two systems using any filtering mechanisms. However, since the Mode S and TCAS transmissions are of short

[1] IEEE Paper - 978-1-4577-0557-1/12 ©2012 IEEE & Honeywell Inc: Aircraft Installation & Operational Aspects of the Aeronautical Mobile Airport Communications System (AeroMACS) – Aloke Roy et al.

duration and their duty cycle is very low (less than 1 per cent), the fraction of the time that AeroMACS reception will be interfered with will also be low.

2.6.2.4.5 The AeroMACS radio will have to be certified for compliance with RF radiated and conducted emissions out of the radio enclosure(s) and cabling connected to the unit, and for compliance with RF susceptibility to radiated and conducted interference coupled via the cabling connected to the AeroMACS radio per applicable industry standards.

2.6.2.5 *Other systems occupying the spectrum*

2.6.2.5.1 The AeroMACS unwanted emission (i.e. out-of-band and spurious emissions) levels are specified in section 3.5 of the AeroMACS SARPs. Those levels are consistent with that required of commercial IEEE802.16 devices.

2.6.2.5.2 AeroMACS operates in the AM(R)S, across at least the frequency 5 030 to 5 150 MHz (see sections 2.1 and 3.2.1 of the AeroMACS SARPs). The expected initial operating band is 5 091 to 5 150 MHz.

2.6.2.5.3 During development of the AeroMACS SARPs it was noted that No. 5.443C of the ITU Radio Regulations places additional requirements on AM(R)S operations in the 5 030 to 5 091 MHz band to protect radio navigation satellite systems (RNSS) in the adjacent 5 010 to 5 030 MHz band. The footnote was considered when developing the AeroMACS unwanted emission level requirements.

> ***5.443C*** *The use of the frequency band 5 030 - 5 091 MHz by the aeronautical mobile (R) service is limited to internationally standardized aeronautical systems. Unwanted emissions from the aeronautical mobile (R) service in the frequency band 5 030 - 5 091 MHz shall be limited to protect RNSS system downlinks in the adjacent 5 010 - 5 030 MHz band. Until such time that an appropriate value is established in a relevant ITU-R Recommendation, the e.i.r.p. density limit of -75 dBW/MHz in the frequency band 5 010 - 5 030 MHz for any AM(R)S station unwanted emission should be used. (WRC-12).*

2.6.2.5.4 In particular, the following points were noted:

a) 5.443C does not apply to AeroMACS operation in 5 091 to 5 150 MHz where near-term operations will occur. Though AeroMACS is capable of operating in 5 030 to 5 091 MHz, that band in ICAO is currently planned for control and non-payload communications (CNPC) for remotely piloted aircraft systems (RPAS; termed unmanned aircraft systems or UAS in ITU). RPAS CNPC will utilize a completely different radio system;

b) the -75 dBW/MHz level in 5.443C is provisional and based on protection of RNSS service links under certain conditions. Such RNSS service links do not currently exist. Also the scenario utilized to derive the limit did not consider on-aircraft interference from AeroMACS-to-RNSS. Such aircraft integration is beyond the purview of ITU; and

c) RNSS feeder downlinks do exist in the 5 010 to 5 030 MHz frequency band, however, they were not studied in the development of the -75 dBW/MHz provisional limit. As a result, the level necessary to protect those systems is not known. It should be noted that such feeder link receivers are usually associated with large dish antennas and usually located in areas away from airports, while AeroMACS is limited to operating on the surface of an aerodrome.

2.6.2.5.5 Given the available information, the decision was taken to keep the unwanted emission levels contained in section 3.5. If in the future AeroMACS is operated in 5 030 to 5 091 MHz, operating RNSS systems will be protected as necessary. This may result in additional attenuation to AeroMACS unwanted emissions below 5 030 MHz, and/or reduced AeroMACS operating power. This too could also apply to other non-RNSS satellite systems as explained in the next section.

2.6.2.6 *Interference to satellite systems*

2.6.2.6.1 The potential of AeroMACS interference to the satellite fixed services transmissions (FSS) has been debated in ITU at the WRC-07, as part of the agreement to allow AeroMACS to have an AM(R)S allocation in the 5 GHz band.

2.6.2.6.2 The agreement at the WRC-07, constrains the AeroMACS usage on the airport surface, requiring specific limitations (notably a maximum of a 2 per cent increase in the satellite receiver noise temperature) to be met. Following this agreement, additional studies and investigations have been carried out in Europe and the United States in particular to demonstrate that AeroMACS meets these requirements.

2.6.2.6.3 The undertaken analysis considered future dense deployments of AeroMACS in all regions of the world in order to simulate worst case scenarios (which will not be realized in the early deployment of AeroMACS). In addition the analysis considered potential hot spots considering dense simultaneous deployment both in Europe and the United States.

2.6.2.6.4 This section summarizes the analysis undertaken in one of the above studies and presents as an example the assumptions and outcome of calculating aggregated emissions from all expected future AeroMACS deployments so that AeroMACS implementations:

a) are compliant with the ITU co-interference requirements (WRC-07); and

b) do not adversely affect the Globalstar satellite feeder links.

2.6.2.6.5 This material is provided in the AeroMACS Manual as guidance and explanatory material to capture some relevant implementation considerations. It is important to note that in WRC-15 some of the limitations agreed in WRC-07 were reconsidered (i.e. the 2 per cent limit was increased to 5 per cent which adds margin in the implementation considerations.

2.6.2.6.6 In the WRC-07 discussions the threshold interference power level for Globalstar at low earth orbit (LEO) has been established at -157.3 dBW corresponding to a maximum 2 per cent increase of the satellite receiver's noise temperature.

2.6.2.6.7 In order to establish power limits for AeroMACS base station transmitters and to avoid interference with the Globalstar uplinks, the AeroMACS base stations with sector antenna transmitters were modelled at 6 207 airports in Europe, the United States and the rest of the world. The following assumptions were applied related to large, medium and small size category airports of the simulation:

a) large size airports:

1) US categories: 35 operational evolution partnership airports (OEP 35);

2) Europe: 50 largest European airports according to Wikipedia list.

b) medium size airports:

1) 123 US category Class C airports;

2) Europe: 50 medium category airports according to Wikipedia list rank 51 to 100;

c) small size airports:

1) all other airports in open flights database.

2.6.2.6.8 In the model used in the investigations, each large airport is assigned six 120° sector antennas, each medium airport is assigned three 120° sector antennas and each small airport is assigned one 120° sector antenna. Several simulation runs were applied with different random antenna directions. This is equivalent to assume a horizontal omnidirectional station pattern as a mean.

2.6.2.6.9 The simulations assumed that large airports will use all eleven 5 MHz channels, medium airports will use six 5 MHz channels and small airports will use one 5 MHz channel. Small airports are only allowed transmitting half as much power per sector as the medium and large airports. This takes into account that at smaller sites it is expected that AeroMACS is not permanently running.

2.6.2.6.10 Finally, the following assumptions for EIRP, MIMO system and antenna pattern have been applied:

a) EIRP is the sector transmit power at the antenna input plus antenna gain;

b) maximum allowable EIRP in a base station sector must be the sum of both transmit power amplifiers in a 2-channel MIMO system; and

c) base station sector patterns are defined to be ITU-R-F-1336-2 reference patterns with 120° 3 dB beam width toward the horizon.

2.6.2.6.11 Based on the simulations, the analysis concluded that under the assumptions considered the AeroMACS deployment will be meeting the ITU WRC-07 requirements, when the worldwide deployment of AeroMACS base stations observe the following emissions limitations:

a) the total base station EIRP in a sector was assumed not to exceed:

1) 39.4 dBm for elevation angles up to 1.5 degrees;

2) 39.4 dBm linearly decreasing (in dB) to 24.4 dBm for elevation angles from 1.5 to 7.5 degrees;

3) 24.4 dBm linearly decreasing (in dB) to 19.4 dBm for elevation angles from 7.5 to 27.5 degrees;

4) 19.4 dBm linearly decreasing (in dB) to 11.4 dBm for elevation angles from 27.5 to 90 degrees;

b) the total mobile station EIRP is not assumed to exceed 30 dBm.

Note.— The above ground antenna elevation pattern is contained in ITU-R F.1336-2.

2.6.2.6.12 The antenna pattern identified in the above analysis is one that has been shown via simulations to meet the WRC-07 requirements. However, it is not specified or recommended to be included in the requirements as other patterns may also be suitable.

2.6.2.6.13 The information in this section aims to raise the awareness of the AeroMACS implementers that in eventual dense (end-state) AeroMACS deployment, the antenna pattern of the (ground) base stations and the antenna tilt, need to be carefully considered to avoid any impact to FSS systems and to continue meeting any applicable ITU requirement.

2.6.2.6.14 However, this issue (minimization of impact to FSS) cannot be addressed locally at the level of a single airport or in one region only, as it is the global aggregate interference impact that is important.

2.6.2.6.15 In order to minimize impact to FSS, it is also important that, particularly in the case of smaller airports, potentially using a limited number of channels, the choice of the channels is spread among different airports to avoid some channels being over assigned (and over used) while others being under assigned (and under used).

2.6.2.7 *Interference to/from other AeroMACS systems*

2.6.2.7.1 The existence of AeroMACS deployments in nearby airports (current or future planned) should be investigated. It is recommended that local airports at a distance within the radio horizon are considered and, if interference level is deemed relevant, readjustments are made to the channels available in each deployment.

2.7 ANTENNAE/MIMO

2.7.1 Multiple-input multiple-output (MIMO) is a system with plural antennas to improve the system coverage or throughput [1].

2.7.2 There are two types of MIMO modes. One is MIMO matrix A (MIMO-A), the other is MIMO matrix B (MIMO-B). MIMO-A employs two transmitting (Tx) antennas and one or two receiving (Rx) antenna to improve coverage by sending the same data via Tx antennas and combining them at the receiver. MIMO-A can be implemented in onboard MS with only one receive antenna.

2.7.3 On the other hand, MIMO-B employs two Tx antennas and two Rx antennas to increase throughput by dividing a single data stream and sending the resulting streams over two antennae in parallel.

2.7.4 AeroMACS should support downlink MIMO-A.

Note.— When applications demand the greater throughput provided by MIMO-B, this may be considered for aircraft.

2.7.5 MS installed on ground vehicles or other use cases except for aircraft is recommended to support both MIMO-A and MIMO-B to obtain better throughput.

2.7.6 BSs are recommended to support both MIMO-A and MIMO-B. BS will accept many MSs with various types of MIMO mode simultaneously. MIMO-B is available only when both BS and MS support it.

2.8 SENSITIVITY

2.8.1 The sensitivity level is defined as the power level measured at the receiver input when the BER is equal to 1*10-6.

2.8.2 The computation of the sensitivity level for the AeroMACS system is based on the following formula:

$$RSS = -114 + SNR_{Rx} - 10 \times \log_{10}(R) + 10 \times \log_{10}\left(\frac{F_s \times N_{used} \times 10^6}{N_{FFT}}\right) + ImpLoss + NF \qquad (1)$$

Where:

*	-114:	is the thermal noise power term in dBm, referred to 1 MHz bandwidth and 300 K temperature.
*	SNR_{RX}:	is the receiver SNR , it can be defined as the SNR necessary , at the demodulator input, to get the desired BER for the given modulation and coding rate.
*	R:	is the repetition factor.
*	Fs:	is the sampling frequency in Hz.
*	NFFT:	is the FFT size.
*	Nused:	is the number of subcarrier used (FFT size – number of guard-band subcarriers – DC carrier).
*	ImpLoss:	is the implementation loss, which includes non-ideal receiver effects such as channel estimation errors, tracking errors, quantization errors, and phase noise. The assumed value is 5 dB.
*	NF:	is the receiver noise figure, referenced to the antenna port. The assumed value is 8 dB.

2.8.3 The SNRrx depends on the modulation and coding scheme selected (a QPSK 1/2 needs a lower SNR than a 64 QAM 3/4 to get the same BER); in case of convolutional coding the values defined are:

Receiver SNR		
Modulation	**Coding**	**Receiver SNR (dB)**
QPSK	1/2	5
QPSK	3/4	8
16-QAM	1/2	10.5
16-QAM	3/4	14
64-QAM	1/2	16
64-QAM	2/3	18
64-QAM	3/4	20

Table 22. Receiver SNR

2.8.4 Using the above parameters in the formula (1) and applying them to Table 22, we get the sensitivity values listed in Table 22.

Modulation Scheme	Rep. Factor	Sensitivity
64-QAM 3/4	1	-76.37 dBm
64-QAM 2/3	1	-78.37 dBm
16-QAM 3/4	1	-82.37 dBm
16-QAM 1/2	1	-85.87 dBm
QPSK 3/4	1	-88.37 dBm
QPSK 1/2	1	-91.37 dBm
QPSK 1/2	2	-94.37 dBm

Table 23. AeroMACS receiver sensitivities: RSS

2.9 SYSTEM ARCHITECTURE

2.9.1 General

2.9.1.1 Figure 20 provides a logical representation of the overall networks at an airport.

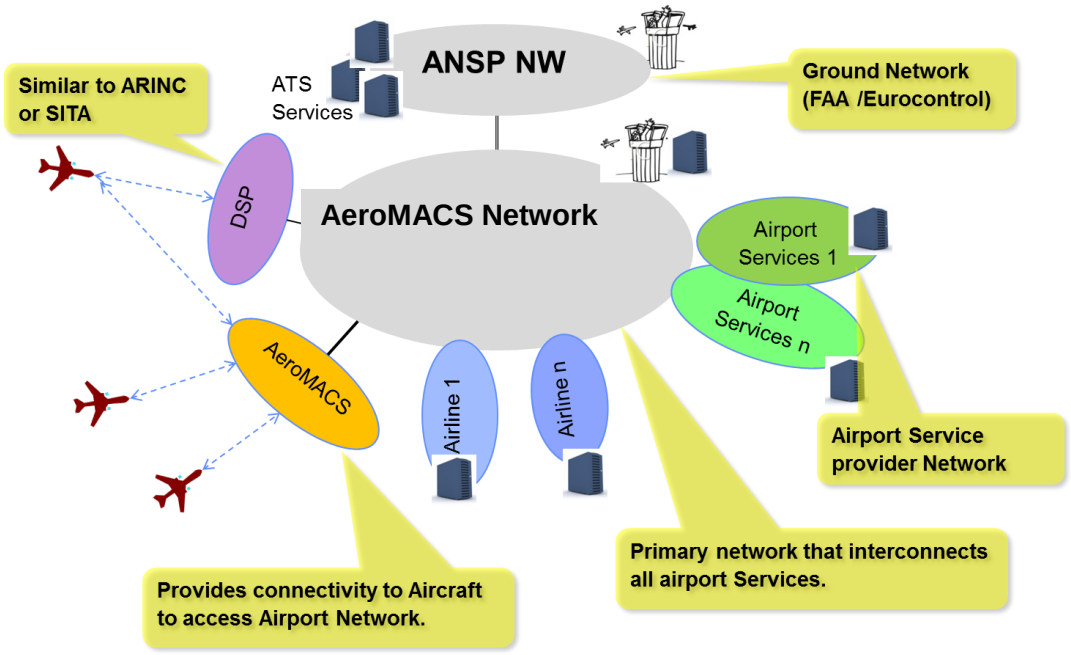


Figure 20. Network at a typical airport

2.9.1.2 The aviation internet (IPS) may comprise various networks with different administrative domains as explained below:

a) ANSP stands for air navigation service provider, the entity that manages the flight traffic in a region or in a State. ANSPs have their networks deployed to support the air traffic applications. ANSP networks belonging to various regions are interconnected to each other and thus provide a global network for data link services.

b) Airport network supports various airport services. Airport network may provide infrastructure for airport service providers to register and host its airport services in global or site-local domains. Site-local services will be available within the airport network only while global services will be available to anyone in the global aviation internet. An example of a site-local application could be the real-time broadcast of surface vehicle position information. Such real-time information need not be broadcasted in the global domain.

c) AeroMACS network, in the context of aircraft, provides mobile connectivity to aircraft to access airport network. It has the infrastructure to support dynamic connections, to handle subscriptions for mobile users and to ensure authenticity and privacy needed for aircraft's safety communications. It corresponds to AeroMACS ASN and CSN in the reference model. AeroMACS network may also offer other fixed link services for interconnecting various networks within the airport domain.

d) ASP/airline networks should be considered as private enterprise networks. An airport is expected to have multiple ASP networks. ASPs can host its servers/applications that are required to be accessed by external entities in the perimeter network (in a de-militarized zone (DMZ)), while the internal network elements should be kept inside the closed aviation network. For example, consider a weather service provider network at an airport. The network may comprise sensors installed at various places

of an airport, servers to collect and process information from various sensors, routers, networking devices, personal computers for staff, internal mail servers etc., placed in the closed network, while the dispatch server that provides consolidated weather information to aircraft kept in the de-militarized zone (DMZ).

2.9.2 Network overview and architecture

This section provides an overview of the AeroMACS network based on the network reference model describing the functional blocks and reference points of the access service network (ASN) and connectivity service network (CSN). Secondly, an end-to-end AeroMACS service network architecture is proposed based in the network reference model.

2.9.2.1 *Network reference model (NRM)*

2.9.2.1.1 General

2.9.2.1.1.1 The network reference model (NRM) does not necessarily define physical entities but instead groups the functions to be performed into functional blocks with a simple logical interface between them.

2.9.2.1.1.2 The NRM is a general logical representation of the network architecture, including AeroMACS, based on the IEEE standard (7). The NRM identifies functional entities and the reference points (RPs) over which interoperability is achieved between them. Each of the entities, SS, BS, ASN and CSN represents a grouping of functional entities. A reference point represents a conceptual link that connects different functions of different functional entities. RPs are not necessarily a physical interface. These functions make use of various protocols associated with an RP. Figure 21 introduces overall interoperability reference points between AeroMACS functional entities.

2.9.2.1.1.3 The intent of the NRM is to allow multiple implementation options for a given functional entity while achieving interoperability among different realizations of functional entities. Interoperability is based on the definition of communication protocols and data plane treatment between functional entities, to achieve an overall end-to-end function, for example, security or mobility management. Thus, the functional entities on either side of a reference point represent a collection of control and bearer plane end-points. In this setting, interoperability may be verified based only on protocols exposed across an RP which would depend on the end-to-end function or capability realized (based on the usage scenarios supported by the overall network).

2.9.2.1.1.4 The NRM specifies the normative use of protocols over an RP for such a supported capability. If an implementation claims support for the capability and exposes the RP then the implementation needs to comply with this specification. This avoids the situation where a protocol entity may reside on either side of an RP or the replication of identical procedures across multiple RPs for a given capability.

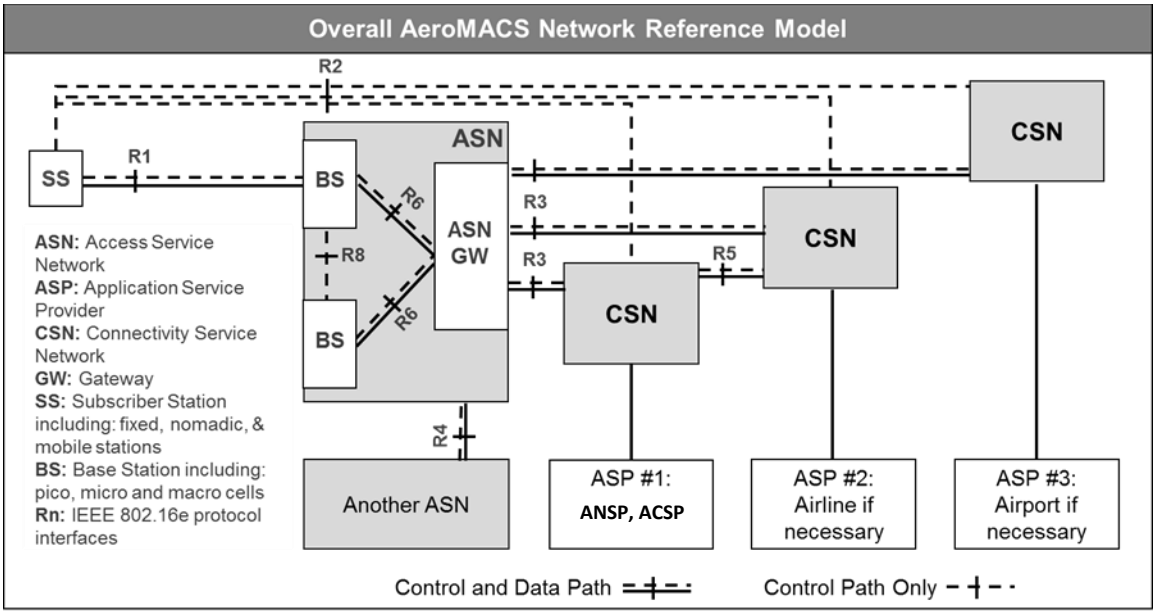


Figure 21. Overall network reference model

2.9.2.1.1.5 All protocols associated with an RP may not always terminate in the same functional entity, i.e. two protocols associated with an RP need to be able to originate and terminate in different functional entities.

2.9.2.1.1.6 The normative reference points between the major functional entities are the following:

Reference Point R1

Reference Point R1 consists of the protocols and procedures between an SS and a BS as part of the ASN air interface (PHY and MAC) specifications (see also ASN reference model outlined later in this section). Reference Point R1 may include additional protocols related to the management plane.

Reference Point R2

Reference Point R2 consists of protocols and procedures between the SS and CSN associated with authentication, services authorization and IP host configuration management. This reference point is logical in that it does not reflect a direct protocol interface between SS and CSN.

The authentication part of Reference Point R2 runs between the SS and the CSN operated by the home NSP, however the ASN and CSN operated by the visited NSP may partially process the aforementioned procedures and mechanisms.

Reference Point R2 may support IP host configuration management running between the SS and the CSN (operated by either the home NSP or the visited NSP).

Reference Point R3

Reference Point R3 consists of the set of control plane protocols between the ASN and the CSN to support AAA, policy enforcement and mobility management capabilities. It also encompasses the bearer plane methods (e.g. tunnelling) to transfer user data between the ASN and the CSN. One of the protocols foreseen on this RP is RADIUS.

In section 2.9.1.3.8.6 concerning deployment scenarios, some particular internetworking relationships will be described between ASN and CSN for:

a) sharing an ASN by multiple CSN; and

b) providing service to roaming SS.

Reference Point R4

Reference Point R4 consists of the set of control and bearer plane protocols originating/terminating in various functional entities of an ASN that coordinate SS mobility between ASNs and ASN-GWs. R4 is the only interoperable RP between similar or heterogeneous ASNs.

Reference Point R5

Reference Point R5 consists of the set of control plane and bearer plane protocols for internetworking between the CSN operated by the home NSP and that operated by a visited NSP. This reference point will only exist between CSNs that have an institutional or business relationship which requires such internetworking.

Reference Point R6

Reference Point R6 consists of the set of control and bearer plane protocols for communication between the BS and the ASN-GW. The bearer plane consists of intra-ASN data path between the BS and ASN-GW. The control plane includes protocols for data path establishment, modification, and release control in accordance with the MS mobility events. R6 also serves as conduit for exchange of MAC state information between neighbouring BSs except when protocols and primitives over R8 are used. The main protocol often used in this interface is an IP-in-IP tunnelling protocol, named GRE (generic encapsulation protocol).

Reference Point R8

Reference Point R8 specifies the information exchange between BS belonging to the same ASN for resource management or load balancing purposes.

Note.— Reference Point 7 has been deleted by the IEEE, however, remaining numbering has been maintained.

2.9.2.1.2 ASN reference network

2.9.2.1.2.1 General

2.9.2.1.2.1.1 The ASN defines a logical boundary and represents a convenient way to describe an aggregation of functional entities and corresponding message flows associated with the access services. The ASN represents a boundary for functional interoperability with AeroMACS clients, AeroMACS connectivity service functions and aggregation of functions embodied by different vendors. Mapping of functional entities to logical entities within ASNs as depicted in the NRM is informational.

2.9.2.1.2.1.2 The ASN reference model is illustrated in Figure 22. An ASN shares R1 reference point (RP) with an SS, R3 RP with a CSN and R4 RP with another ASN. The ASN consists of at least one instance of a base station (BS) and one instance of an ASN Gateway (ASN-GW). The R4 reference point is the only RP for control and bearer planes for interoperability between similar or heterogeneous ASNs. Interoperability between any type of ASN is feasible with the specified protocols and primitives exposed across R1, R3 and R4 reference points.

2.9.2.1.2.1.3 It is highly desirable that inter-ASN mobility is supported in an airport to minimize latency outages on the airport surface.

2.9.2.1.2.1.4 For the inter-ASN mobility applicable protocols and procedures should comply with the Reference Point R4.

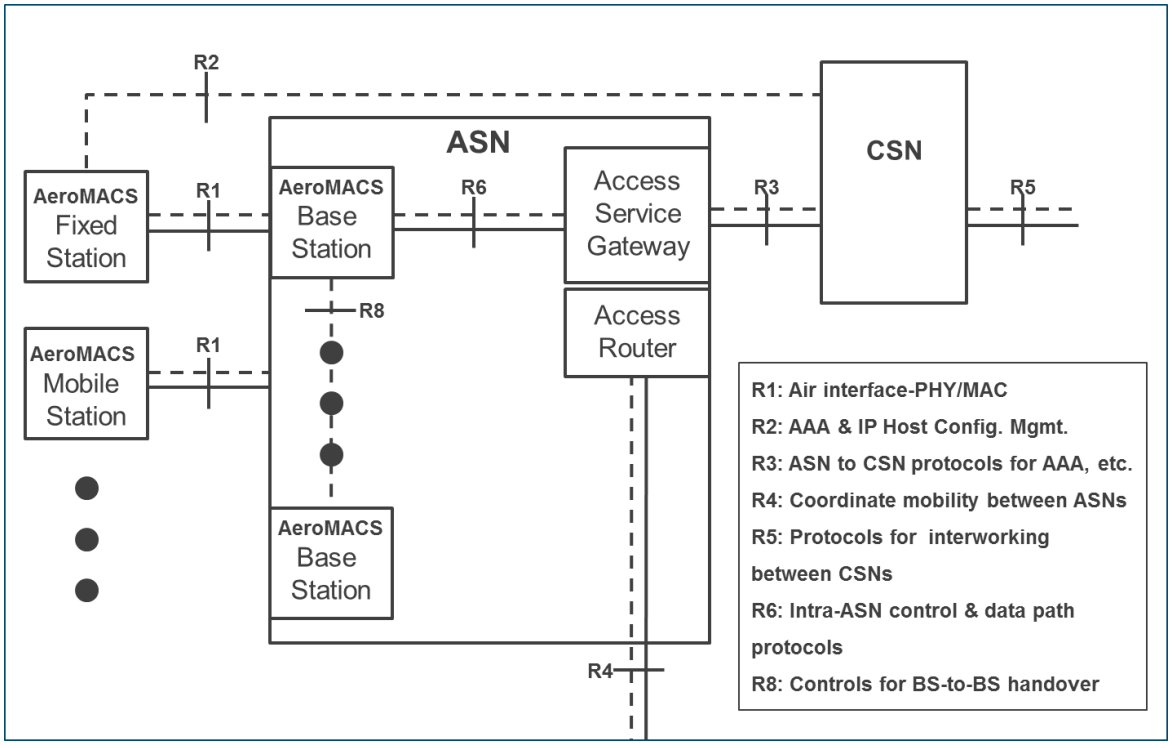


Figure 22. Detailed AeroMACS ASN reference model

2.9.2.1.2.2 SS and BS definition

2.9.2.1.2.2.1 The SS and BS are specific AeroMACS entities that manage the user and control planes of the physical and medium access layers of the subscriber node and the access network, respectively. Their functions are fully described by IEEE 802.16-2009 Standard.

2.9.2.1.2.2.2 The AeroMACS base station (BS) is a logical entity that embodies a full instance of the MAC and PHY in compliance with the AeroMACS specifications.

2.9.2.1.2.2.3 A BS instance represents one sector with one frequency assignment. It incorporates scheduler functions for uplink and downlink resources, which will be left for vendor implementation and are outside the scope of this document.

2.9.2.1.2.3 ASN gateway definition

2.9.2.1.2.3.1 As explained in 2.2.1.1.1, the ASN is not necessarily a physical entity but a functional block performing the following functions.

2.9.2.1.2.3.2 The ASN gateway (ASN-GW) is a logical entity that represents an aggregation of control plane functional entities that are either paired with a corresponding function in the ASN (e.g. BS instance), a resident function in the CSN or a function in another ASN. The implementation of the ASN-GW is outside the scope of this document.

2.9.2.1.2.3.3 The ASN-GW is the main actor on the network topology on which rely most of the management and control procedures to support the data link and its interconnection with the backbone. Figure 23 summarizes the functions attributable to the ASN-GW.

2.9.2.1.2.3.4 One ASN-GW is expected to be deployed per access service network. As depicted, the main interfaces for the ASN-GW are: the R6 reference point which connects it to the BSs and the R3 reference point which deals with the interconnection to the CSN. In the cases such as a small airport with a single ASN and where the ASN-GW and BSs are integrated into one physical entity, nonetheless the R6 interface is to be exposed.

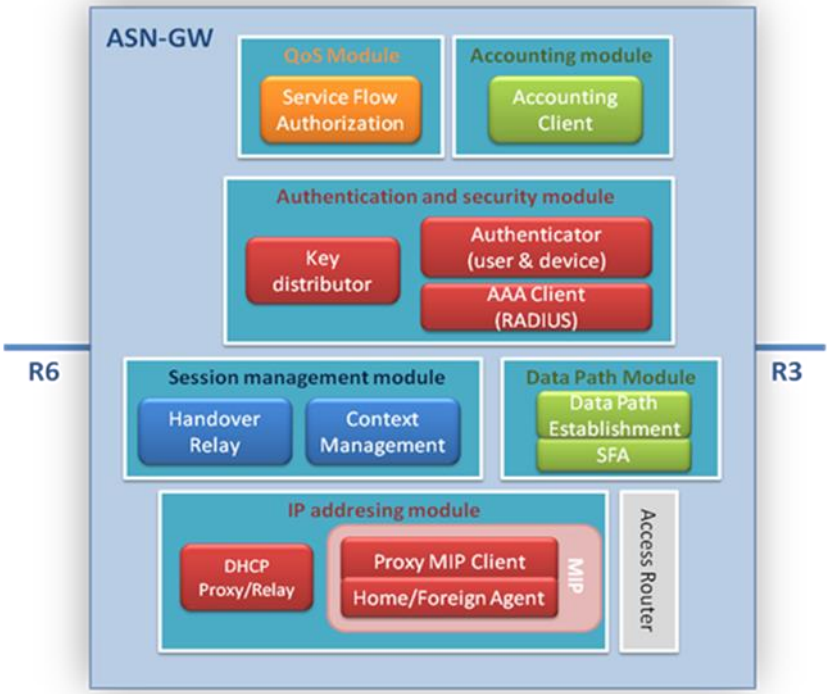


Figure 23. Main functionalities of AeroMACS ASN-GW

Note.— IP addressing model and access router functions are implementation options and may reside outside the ASN-GW.

2.9.2.1.2.3.5 According to the AeroMACS network architecture reference model, a generic ASN-GW covers the features/functionalities shown:

a) AeroMACS Layer 2 (L2) connectivity with SS;

b) relay functionality for establishing IP connectivity between the SS and the CSN;

c) network discovery and selection of the AeroMACS subscriber's preferred NSP;

d) subscriber IP address allocation by querying the DHCP server for network establishment and DHCP DISCOVER messages forwarding;

e) IP forwarding to/from the backhaul via MIP foreign agent (FA);

f) connection admission control to ensure service quality and different grades of service commitment and provision;

g) AAA proxy/client. AeroMACS ASN-GW will trigger the exchange of susceptible subscriber information and transfer AAA messages of AeroMACS subscriber's visited NSP for authentication, authorization and accounting to the home NSP;

h) context management. Transfer of subscriber credentials (it can store user's profiles or just cache them). Consequently, key distribution between entities;

i) user profile management. After the authorization phase and key exchange, the user profile is handled in order to create corresponding SFs;

j) data path establishment and service flow authorization (SFA). ASN-GW creates one data path per SF. According to a predefined profile, ASN-GW will receive the mapping of CID to SFID from the BS. If GRE tunnelling is used, then there will be one GRE tunnel per SF; and

k) mobility management and handover control.

2.9.2.1.2.4 AeroMACS ASN profile

2.9.2.1.2.4.1 While the grouping and distribution of functions into physical devices within the ASN is an implementation choice, the AeroMACS architecture specification defines one ASN interoperability profile.

2.9.2.1.2.4.2 A profile maps the ASN functions into the BS and ASN-GW so that protocols and messages, over the exposed reference point, are identified. The following text describes WiMAX forum ASN Profile C based on [3].

Note.— The depiction of a function on either the ASN-GW or the BS in Figure 22 below, does not imply that the function exists in all manifestations of this profile. Instead, it indicates that if the function existed in a manifestation it would reside on the entity shown. Identification of the ASN Profiles was done for the specific goal of providing a framework for interoperability among entities inside an ASN.

2.9.2.1.2.4.3 According to Profile C, ASN functions are mapped into ASN-GW and BS as shown in Figure 24. The key attributes of Profile C are:

a) handover (HO) control is in the base station;

b) radio resource control (RRC) is in the BS that would allow radio resource management (RRM) within the BS. An “RRC relay” is in the ASN GW, to relay the RRM messages sent from BS to BS; and

c) ASN anchored mobility among BSs is achieved by utilizing R6 and R4 logical connections.

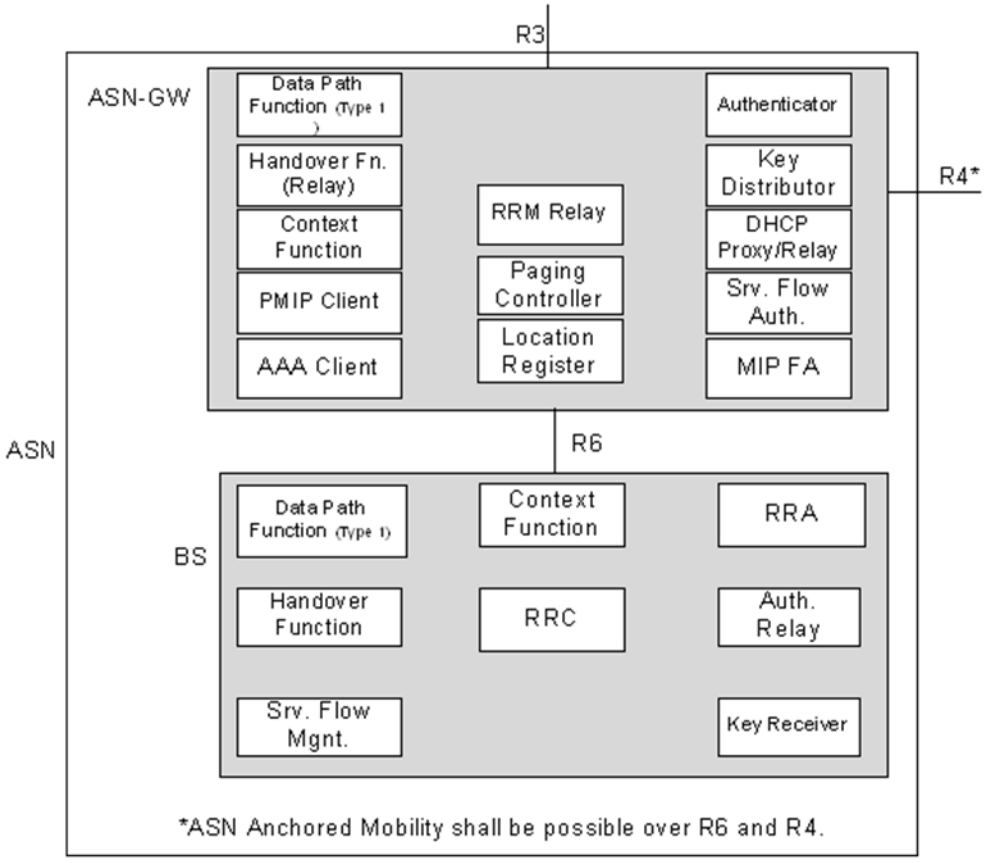


Figure 24. WMF ASN Profile C

For more details refer to [2].

2.9.2.1.2.5 CSN reference network

The CSN, as shown in Figure 25, is the network that provides end-to-end connectivity to AeroMACS subscribers with network entities and enables the provision of services by AeroMACS application service providers (ASP). CSN main functionalities are AAA server and DHCP server. The applicable RP are R3 (CSN with ASN) and R5 (between two CSN). CSN internal reference points are out of scope of this specification.

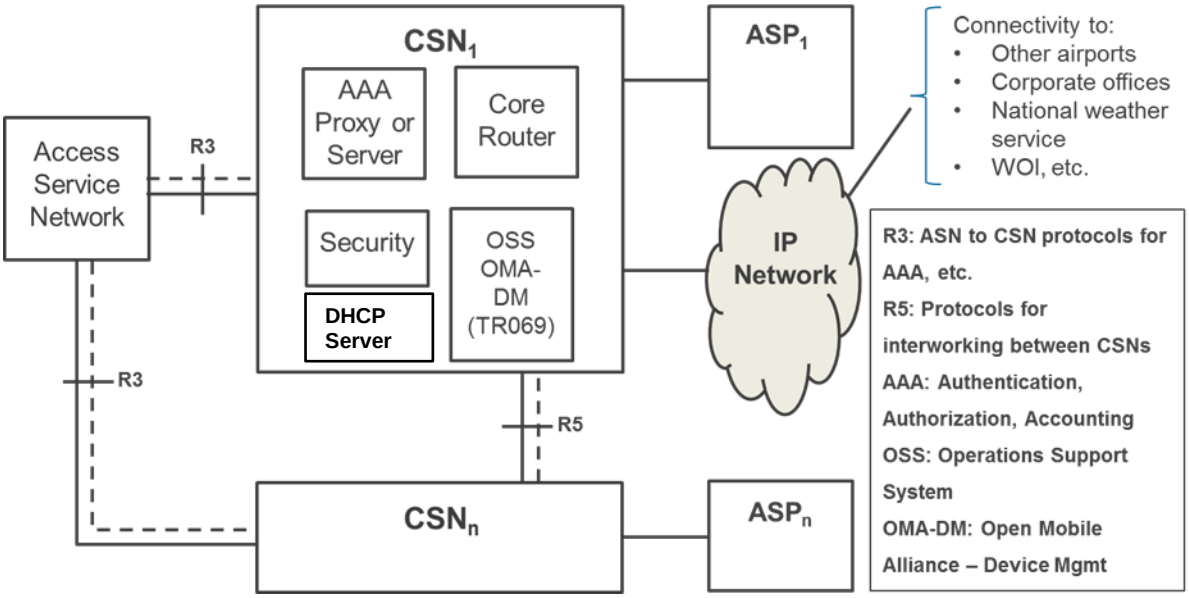


Figure 25. Detailed AeroMACS CSN reference model

2.9.2.1.2.6 AAA proxy/server

2.9.2.1.2.6.1 During logon aircraft credentials are presented to the AeroMACS CSN AAA server. AAA server verifies the credentials and checks the policy database in the context of aircraft before authorizing it. The AAA then informs the ASN about the successful completion of authentication, the SS authorization profile (i.e. assigned service flows and associated QoS parameters) and the required security context (i.e. MSK and its lifetime) to be used.

2.9.2.1.2.6.2 Local users in an airport (e.g. handling vehicles) will be managed by an airport AAA server via the ASN-GW. For non-local users (such as an aircraft) the likely scenario will involve a AAA proxy in the airport that will send queries and requests to the H-NSP, which will manage airborne user authentication and policy function (PF). AAA proxy covers the following functionalities:

a) support network entry when required, in case MS connects to V-NSP;

b) simplify connection to several CSN; and

c) security capability that allows authentication of MS locally.

2.9.2.1.2.6.3 AAA servers deployed at each airport can be connected via a proxy network. This allows authentication of subscribers beyond the region of the service in the airport. However, the mechanisms to establish this proxy network are out of the scope of this document.

2.9.2.1.2.6.4 By default, the IETF RADIUS protocol is supported as the main protocol for AAA purposes.

2.9.2.1.2.6.5 Key exchange using PKMv2 will rely on the fact that in AeroMACS user (subscriber) authentication is required. EAP-TLS framework is the defined suite to give support to user authentication. The aircraft router will use X.509 certificates for EAP-TLS authentication. A C/N (common name) realm, such as an airline name (as network domains are currently defined by ICAO), or any PKI provider name

can be used for EAP-TLS. The H-NSP AAA server will receive authentication traffic with the username realm, which implies that the airport proxy AAA will need to map the realm value to the H-NSP AAA address.

2.9.2.1.2.6.6 ASN-GW makes use of RADIUS protocol to support service authorization. AAA server is also involved in checking the QoS policy for a given SS and consequently creation of a service flow authorization (SFA) by ASN-GW in response to a service flow initiation request from the SS.

2.9.2.1.2.6.7 AAA servers will depend on the core network managed by the network service provider. AAA server databases could belong to the visited network of each airport; they could belong to the same virtual segment of network as AeroMACS or be held remotely in a different facility of the operator and therefore in another network (namely, the home network).

2.9.2.1.2.6.8 IPsec support for the transport of all connections is envisaged. Moreover, the use of VPN tunnelling is encouraged to secure all the connections to the remote elements of the backbone of the network. This is a local implementation issue and out of scope of this document.

2.9.2.1.2.7 DHCP server

The DHCP server resides in the local CSN, which could be operated by the visited or home NSP. IP address assignment will be done after the SS has performed full network entry if dynamic addressing is used. Alternatively, static addressing can be utilized.

2.9.2.2 *AeroMACS network architecture*

2.9.2.2.1 General

2.9.2.2.1.1 The network reference model is valid to support the integration of AeroMACS data link within the IPS backbone and give the corresponding service support. The overall principles followed to specify AeroMACS end-to-end network architecture are:

Functional decomposition: The proposed architecture allows that required features are decomposed into functional entities. The reference points are means to provide multivendor interoperability. For interoperability purposes, special care must be paid to the Reference Points R1 and R6 of the ASN reference model. Intra ASN mobility will imply full support of R6 control messages.

Modularity and flexibility: The modularity of the proposed architecture gives the means to adapt to different AeroMACS deployments, and the interconnection to the ground infrastructure. As an example, the interconnection of different CSN topologies with just one single access network is permitted. The architecture also enables the scalability of the network in case after initial deployment the number of BSs installed within the airport needs to be increased in order to support more users.

Decoupling the access and connectivity services: This architecture enables full mobility with end-to-end QoS and security support, making the IP connectivity network independent from the AeroMACS radio specification. In consequence, this allows for unbundling of access infrastructure from IP connectivity services.

Support to a variety of business models: AeroMACS architecture supports the sharing of different aviation business models. The architecture allows a logical separation between the network access provider (NAP), the entity that owns and/or operates the access network, the network service provider (NSP) and the application service providers (ASP).

2.9.2.2.1.2 The reference points can represent a set of protocols to give control and provide management support on the bearer plane. On any deployment, functional entities here depicted could be matched to more than one physical device. In a similar manner, most of the reference points are left open. The architecture does not preclude different vendor implementations based on different decompositions or combinations of functional entities.

2.9.2.2.1.3 Figure 26 presents an example of a high-level functional architecture to support communication with ground vehicles (airport operation) and aircraft (ATC, AOC). In such a case, at the airport, in addition to AeroMACS specific systems (base stations and ASN gateway), AAA server and DHCP server need to be deployed to enable communication with airport vehicles. The airport operator network would thus act as the home network for airport vehicles.

2.9.2.2.1.4 For ATC and AOC service provision, the airport network would act as visited network, the home network being implemented at regional or global scale for aircraft. The airport AAA server would thus act as an AAA proxy for aircraft relaying authentication and authorization requests from the ASN gateway to the home-NSP, which is the administrative authority that can operate one or more home agents (HA). Regarding IP connectivity, it is possible that IP addresses will be assigned directly by an H-NSP or a global DHCP. However, the most likely case is that an IP address will be assigned locally to the MS and, in the case of an aircraft with a permanent IP address, it will be announced to the network. The ASN gateway would also relay a DHCP request to the aircraft home network DHCP server. For global connectivity and mobility support, the ASN will rely on a HA operated by an H-NSP.

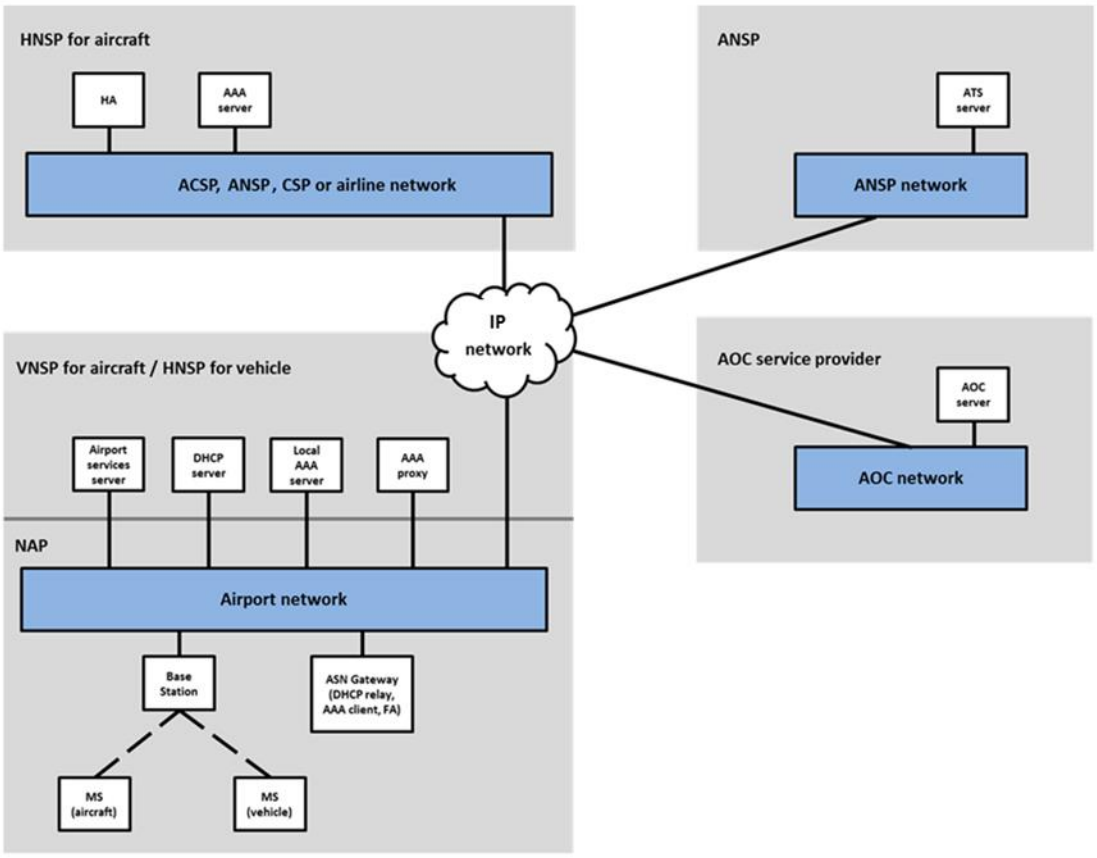


Figure 26. Typical AeroMACS network entities at an airport offering ASN and CSN functions

2.9.2.2.2 Mobility

2.9.2.2.2.1 Doc 9896 identifies mobile IPv6 as the mechanism to provide global mobility among access networks in the ATN. This is currently under review as the IPS requires the use of bidirectional tunnelling, i.e. routing packets from source to destination through the HA in both directions, which may lead to suboptimal routes.

2.9.2.2.2.2 It is foreseen that global IPv6 addresses will be assigned to specific aircraft or on-board data link equipment such as AeroMACS. This can be done via static IP addresses or dynamically via mobile IP mechanisms. The support of dynamic IP addresses allocation (DHCP) and roaming for aircraft needs the support of global IP mobility and contractual agreements between NSPs or network access providers (NAPs) in order to allow the global identification and operation of airborne devices. Subscriber and home agents (HA) will implement the mobility solution to be specified in Doc 9896. According to [9], an IPS MSP operates one or more home agents.

2.9.2.2.2.3 The redirection of an incoming packet to the home network from the visited network where the aircraft is currently in is done through a tunnel established between HA and forwarding agent (FA) or access router (AR).

2.9.2.2.2.4 HA location could vary in a real scenario and can be centralized or decentralized, whereas the AAA is expected to act as a proxy only in the V-NSP. This foreseeable scenario is depicted in Figure 27.

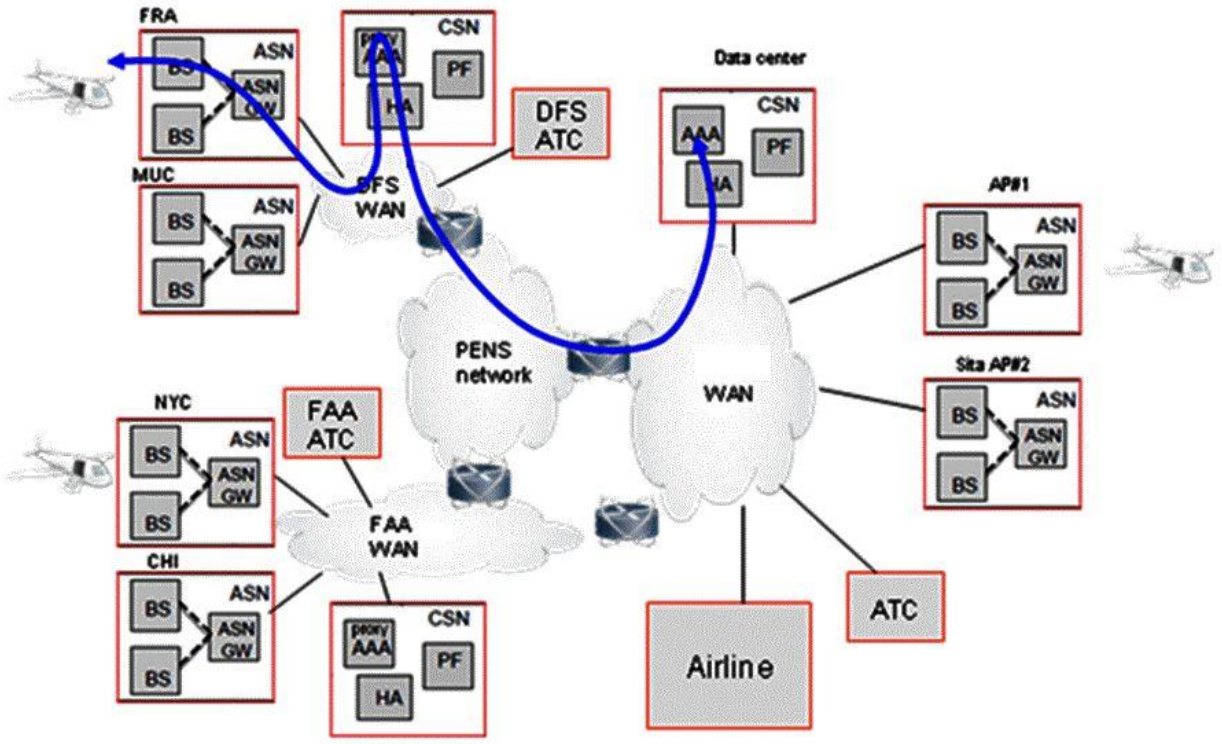


Figure 27. AeroMACS AAA and HA deployment scenario

2.9.2.2.2.5 Several options for the location of the FA/AR are envisaged, namely:

a) physically inside the ASN-GW equipment (as in Profile C) and dedicated to mobility functions only for the MSs in the ASN;

b) as a separate entity in the local airport network and dedicated to mobility functions only for the MSs in the ASN; and

c) as a separate entity in the local airport network and able to perform mobility functions for any node in the local network, including one or more AeroMACS ASN and other IP end nodes.

Note.— The FA/AR will not, in any case, operate to provide IP connectivity and mobility functions to other data links other than AeroMACS.

2.9.2.2.3 IP address configuration

2.9.2.2.3.1 An AeroMACS service provider may choose to have a centralized CSN managing multiple ASNs in different airports.

2.9.2.2.3.2 Alternatively, ASN gateway (acting as a DHCP proxy) contacts the airport network gateway (which acts as DHCP server) to get IP address for aircraft's AeroMACS connection. This IP address is expected to be unique in the scope of global aviation internet. If the aviation internet (IPS) supports dynamic DNS service for aircraft, aircraft registers its new IP address with the DNS services.

2.9.2.2.3.3 Following the network entry procedure, an AeroMACS SS can reach the connection establishment state and belong to a broadcast domain (Layer 2), thereby getting access to network elements beyond the BS which at data plane level is just bridging air and wireline media. Therefore, once Layer 2 is granted, the question on who is listening to the SS broadcast messages to obtain an IP comes up. The forthcoming procedures depend on the type of IP version convergence sublayer established in the previous phases.

2.9.2.2.3.4 For IPv6, from the AeroMACS SS perspective the first hop router is the access router in the ASN-GW.

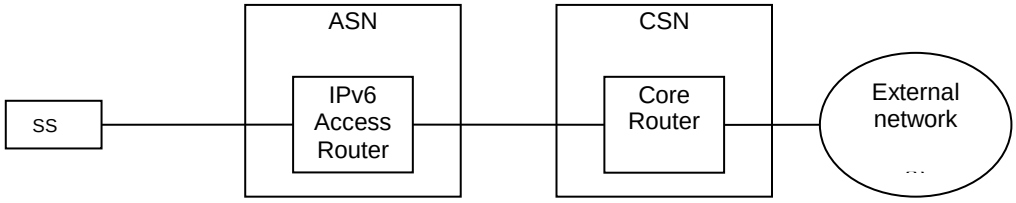


Figure 28. AeroMACS IPv6 data connectivity network elements

2.9.2.2.3.5 The SS performs initial network entry to activate the initial service flows. The establishment of the IPv6 initial services flows enables the sending and receiving of IPv6 packets between the SS and the access router. Then router advertisement and address assignment procedures are initiated.

2.9.2.2.3.6 The information contained in the router advertisement message is learnt by the ASN from the attributes present in the RADIUS authentication accept message sent by the authentication server during the network authentication phase. That content will depend on the network operator access policies.

2.9.2.2.3.7 Then the ASN advertises an IPv6 prefix from a preconfigured pool of prefixes belonging to the attached CSN. In case of NAP sharing, the ASN may have several different prefix pools associated with different CSN. In such case, the ASN uses the realm part of the network address identifier (NAI) to select an appropriate pool to set in the IPv6 router advertisement messages to send to the incoming SS [5].

2.9.2.2.3.8 The message sequence chart in Figure 29 describes the sequence of protocol messages exchanged between the SS and the network during the IP address allocation phase.

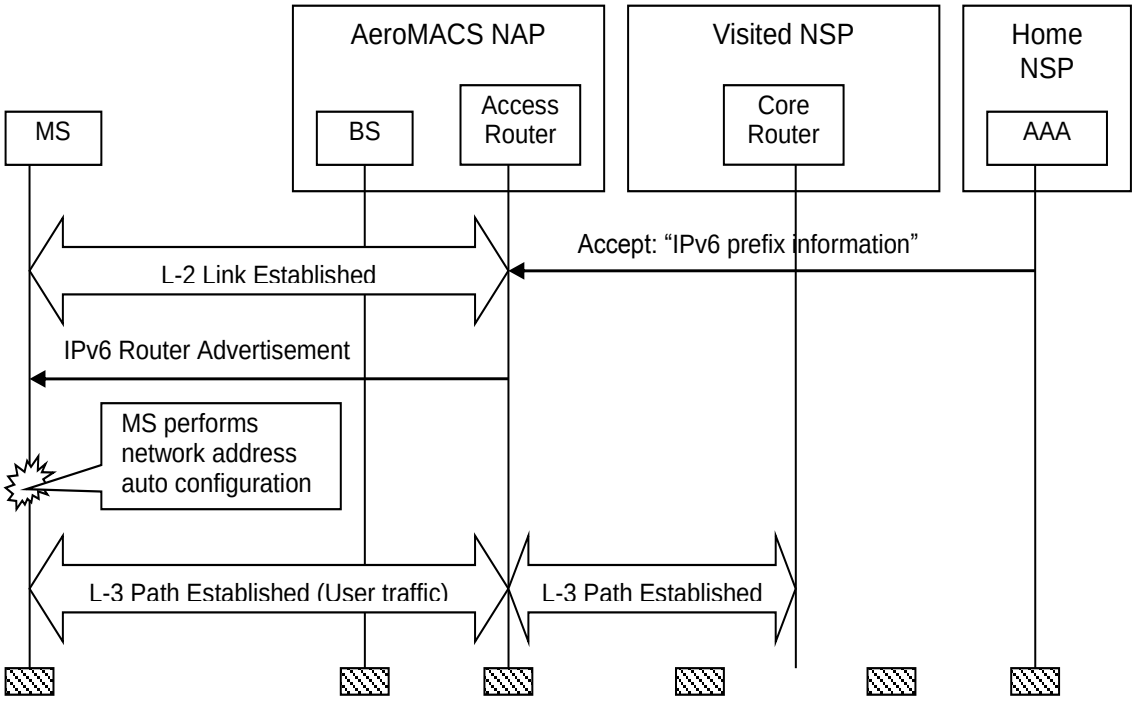


Figure 29. AeroMACS IPv6 data connectivity establishment message sequence chart

2.9.2.2.3.9 After the Layer 3 path is established the following diagram model is in place for a typical deployment scenario:

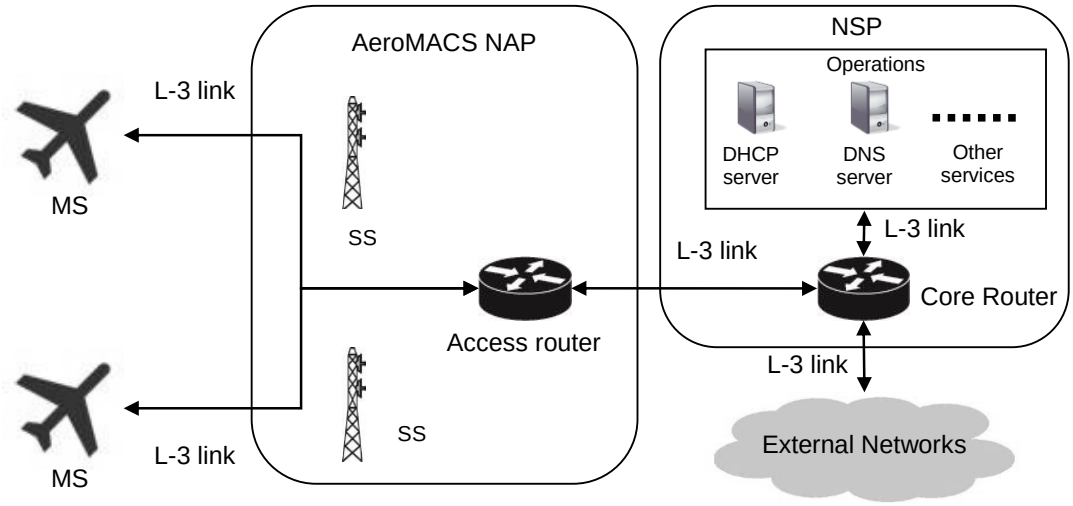


Figure 30. AeroMACS data plane typical deployment

2.9.2.2.3.10 All operations services at Layer 3 are reachable by the MS. This model supports the extension to any service such as IMS, SNMP management, TFTP configuration server, subscriber/policy management, etc. The external networks can be any of these: other network service providers (NSPs), a corporate VPN (airline network), aeronautical internet or any other application partner.

2.9.3 Network deployment scenarios

2.9.3.1 *Business relationships in AeroMACS*

2.9.3.1.1 The NAP is the entity that owns and operates the access network providing the radio access infrastructure to one or more NSPs. Similarly; the NSP is the entity that owns and provides the subscriber with IP connectivity and services by using the ASN infrastructure provided by one or more NAPs. An NSP can be attributed as a home NSP or a visited NSP from the subscriber's point of view. A home NSP maintains service level agreements (SLA), authenticates, authorizes, and charges subscribers. A home NSP can establish roaming agreements with other NSPs, which are called visited NSPs and are responsible to provide some or all subscribed services to the roaming users. Within the aeronautical environment, the following actors could make use of AeroMACS business entities:

a) ANSP (air navigation service provider) as the owner and operator of the national navigation service network;

b) airport authorities may offer AeroMACS services to aircraft. The subscription may offer a combination of network access and airport services provided by that airport authority;

c) airlines may have their dedicated AeroMACS service for their aircraft exclusively. Large airlines may even have their own AeroMACS infrastructure deployed at airports to service their aircraft;

d) ACSP (aeronautical communication service provider) e.g. AVICOM, SITA, ARINC, ADCC may offer AeroMACS services as part of their overall data link service offerings. ACSPs can own AeroMACS networks extending their service at airports; and

e) new/other global CSP (communication service providers). An independent service provider may offer AeroMACS service at an airport providing connectivity to the aviation internet.

2.9.3.1.2 The network on an airport can be connected to the end-user and H-NSP networks using inter-domain routing protocols so that it becomes a part of the aviation internet. Thus it offers global access to airport services, anywhere from the aviation internet for supporting future air traffic management concepts. Aircraft connected to any part of the H-NSP network should be able to reach the airport network and access services offered at any airport through the aviation internet.

2.9.3.1.3 In order to access the services provided by the network, first an entity needs to provide connectivity to the subscriber. This is done by the provision of access service, IP configuration service, AAA service and mobility service. Aviation business models and contractual agreements between parties can have an impact on the network topology that supports the AeroMACS service provision. Figure 31 depicts the overall contractual case and entities involved on behalf of provisioning services to the subscribers. AeroMACS architecture supports the discovery and selection of one or more accessible NSPs by a subscriber.

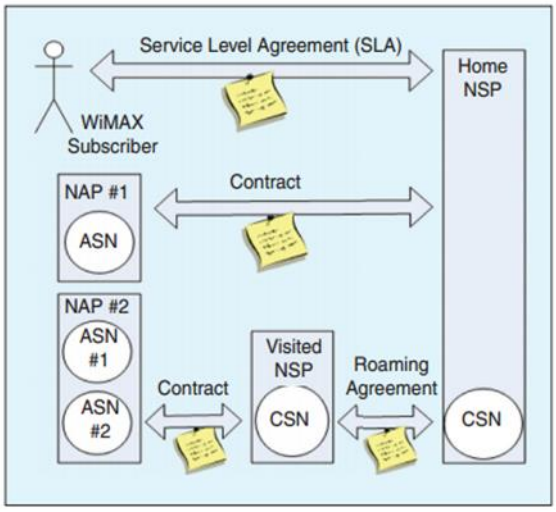


Figure 31. Overall relations between AeroMACS business entities

2.9.3.1.4 A summary of NAP/V-NSP/H-NSP services and possible actors is depicted in Table 24 below.

	Airport authority	**ANSP**	**ACSP**	**CSP**	**Airline**
NAP	X	X	X		X
V-NSP	X	X	X	X	X
H-NSP	X (for vehicles)	X	X	X	X

Table 24. Possible actors for NAP/V-NSP/H - NSP functions

2.9.3.2 *NSP and NAP deployment models*

This section describes the foreseen deployments of NSP and NAP in an AeroMACS network. The models affect the number of possible NSPs and NAPs serving a given airport (one or several) and the role of the potential AeroMACS service providers.

2.9.3.2.1 NAP sharing by multiple NSP

2.9.3.2.1.1 This deployment model for mobile services in aircraft and vehicles is shown in Figure 32 and proposes the existence of one access service network per airport (owned and/or operated by a single entity) shared by multiple NSPs over a single NAP. It is also the most cost-effective solution to have both ATC and AOC services in the aircraft (using a single antenna and MS), and is in line with future IPS ground/airborne architecture supporting traffic segregation. AeroMACS allows the existence of multiple network service providers for a given airport, and there is a defined method for the selection of the NSP by a given MS upon network entry.

2.9.3.2.1.2 This deployment model is the preferred solution by NSP and NAP in order to simplify infrastructure, ease cell planning at a given airport, and reduce harmful interference on legacy systems (e.g. Globalstar) with probably less base stations due to a more efficient use of the spectrum.

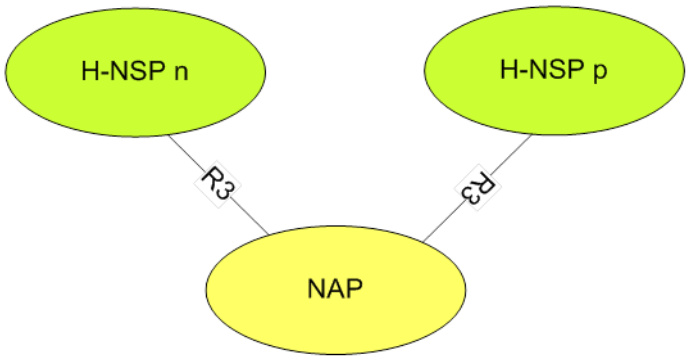


Figure 32. Single NAP - multiple NSP

2.9.3.2.1.3 Several CSNs might share the same ASN.

2.9.3.2.1.4 The NAP deploys and provides the access network to ARINC, SITA, AVICOM, etc. and manages the relationship with airports on behalf of the airlines. Airlines could act as H-NSP or have contractual agreements with a different H-NSP.

2.9.3.2.1.5 In this scenario, the ASN-GW will advertise for incoming new MSs on the access network that there are different NSPs, enabling the MS to establish data communication to its NSPs through AeroMACS ASN and relay the messages to reach the final end user.

2.9.3.2.2 Single NSP providing access through multiple NAPs

2.9.3.2.2.1 This deployment model shown in Figure 32 is foreseen by NSP to extend its coverage at regional scale in relying on local NAP (e.g. extension to several airports by one service provider like SITA or ARINC).

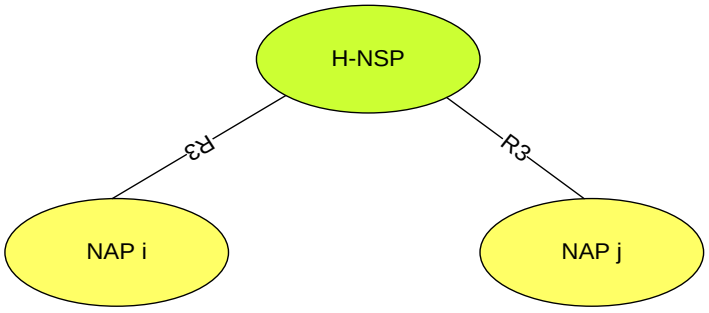


Figure 33. Multiple NAP - single NSP

2.9.3.2.2.2 If one NAP cannot provide full coverage for an NSP in a given area, the NSP can have agreements with multiple NAPs. This model is compatible with the previous one, i.e. multiple NAPs can be serviced by multiple NSPs and vice-versa.

2.9.3.2.2.3 There is a difference within this model depending on whether the NAPs served by a single NSP are collocated in the same airport or not. In the first case, the deployment option of placing the sensitive servers needed (mainly AAA and DHCP) locally would be possible and there would be no need to enable VPN end-to-end connectivity, packet forwarding or relay functions, thus simplifying the rollout and operation of the network. In the latter case, connectivity to the global network would be necessary.

2.9.3.2.3 Greenfield NAP plus NSP

2.9.3.2.3.1 This deployment model, as shown in Figure 34, is foreseen for manufacturers and operator since they leave the flexibility to the NSP to act or not as NAP, depending on local issues.

2.9.3.2.3.2 This model is more suitable to CSPs, ACSPs or airlines in areas where they will be allowed to act as NAP. A single NSP, corresponding to the same CSP or ACSP, operates the network.

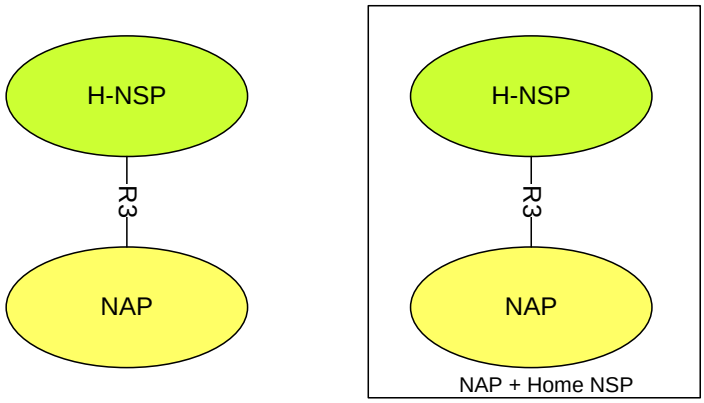


Figure 34. Greenfield NAP plus NSP

2.9.3.2.3.3 Therefore, ACSPs or airlines could be deploying themselves on the airport ground network side acting as the same entity for the NAP plus NSP on the business model. An aircraft coming from a different aircraft operator will be served by its H-NSP, while this Greenfield NAP plus NSP is providing access.

2.9.3.2.3.4 The likely deployment scenarios are illustrated in Table 25.

Use case N°	Description	Subscriber station type	NAP	V-NSP	H-NSP	Deployment model
1	Local services	Fixed vehicle	Airport telco ANSP ACSP	Airport telco ANSP ACSP/CSP	Airport telco ANSP ACSP/CSP	Greenfield NAP plus NSP.
2	Safety and non-safety services on same channels	Fixed vehicle airline A/C	Airport telco ANSP ACSP	Airport telco ANSP ACSP/CSP	Airport telco (vehicle/fixed) ANSP ACSP/CSP	NAP sharing by multiple NSPs. One NSP providing access through multiple NAPs.
3	Safety services on specific channels	Fixed vehicle airline A/C	Airport telco ANSP ACSP	Airport telco ANSP ACSP/CSP	Airport telco (vehicle/fixed) ANSP ACSP/CSP	NAP sharing by multiple NSPs. One NSP providing access through multiple NAPs.
	Non-safety services on specific channels	Vehicle airline A/C	Airport telco ACSP airline	Airport telco ACSP/CSP airline	Airport telco (vehicle) ACSP/CSP airline	One NSP providing access through multiple NAPs.
4	Non-safety services in airline hub	Vehicle airline A/C	Airport telco ACSP airline	ACSP/CSP airline	ACSP/CSP airline	One NSP providing access through multiple NAPs. Greenfield NAP plus NSP.
5	Safety services managed by ANSP	Fixed vehicle airline A/C	ANSP	ANSP	ANSP	One NSP providing access through multiple NAPs. Greenfield NAP plus NSP.

Table 25. Potential AeroMACS deployment scenarios

2.9.3.2.3.5 In each deployment scenario the role of the H-NSP has an impact on the AAA framework, the subscriber management and the route optimization.

2.9.3.2.3.6 If the H-NSP is the airport authority (or an airport telco operator), performing these local functions in the local airport is straightforward. It also allows quick and secure access to local safety services without the need of a VPN since it does not use the ground network infrastructure beyond the airport, which most likely dispenses with the need for a VPN, however, this will also depend on the service provider security policy. The assignment of H-NSP to the airport authority is suited to provide service to local equipment (sensors, handling vehicles, etc.).

2.9.3.2.3.7 If the H-NSP is an ANSP, it can provide a nation-wide mobility anchor point and IP address pool for aircraft flying in the domestic airspace. The ANSP, being the network operator, can manage the safety and performance requirements of the ATC services provided. ANSP could either own the access network at some or all of the nation's airports (Greenfield model) or contract the use of the airport access network, which will act as a V-NSP under a roaming agreement. The AAA proxy from the ASN would send queries and requests to a database operated by the ANSP that will manage airborne user authentication and policy function (PF). Airline services can be provided to contracting airlines under network leasing or SLA agreements. It becomes more challenging when a domestic aircraft flies to foreign airspace since a roaming agreement needs to exist with the V-NSP that manages the aircraft connectivity in the foreign airport. In addition, routing optimization should be used in this case in order to avoid data access between the aircraft and ASPs to be routed through the HA belonging to the ANSP since it could introduce additional latency.

2.9.3.2.3.8 If the H-NSP is an airline, it may operate a global infrastructure of AOC centres providing airline services around the world regions that the airline covers. In such a situation, the airline may set up a global home agent – home agent (HAHA) system in which the route for data access is optimized using the regional HA in each case. As in the case of the ANSP, the access network would rely on local airport authorities or telco operators acting as V-NSP. For certain applications (e.g. maintenance), the airline could own an AeroMACS access network and set up a Greenfield deployment model. The model implies that the provision of ATS services is managed by airlines under SLAs with the ANSPs. Another issue may be the additional latency incurred in AAA exchanges and data access in general, if a route optimization algorithm is not in place.

2.9.3.2.3.9 Finally, if the H-NSP is an ACSP, the ACSP can operate a global infrastructure facilitating the optimization of HA utilization depending on the location of the aircraft. The ACSP may own the AeroMACS access network in certain airports (Greenfield model) and use a third party infrastructure in others, as V-NSP. The AAA proxy from the ASN would send queries and requests to a database operated by the ACSP that will manage the airborne user authentication and policy function (PF). ACSP can sign SLAs with the corresponding ANSPs, airlines and other ASPs for the provision of their services under certain safety and performance levels. A potential issue with this approach is the large amount and complexity of agreements that the ACSP needs to establish with all other service providers. Another issue may be additional latency incurred in AAA exchanges and data access in general, if a route optimization algorithm is not in place.

2.9.3.3 *Network entry and NAP/NSP selection*

Several considerations on the NAP and NSP selection by the MS are described above. Manual or automatic selection of NAP/NSP is left as an open item.

2.9.3.3.1 Overview of network entry

2.9.3.3.1.1 An aircraft MS network entry process is as follows:

During the scanning process the aircraft needs to be able to determine if it is on a channel of a NAP providing aircraft communication services:

a) if the NAP is providing aircraft communication services, the aircraft can either check that its H-NSP is connected or decide to authenticate directly;

b) if the authentication is successful, it means that the NAP/V-NSP is able to contact the H-NSP;

c) then the MS can perform NET entry and be allocated a CoA (care of address);

d) MS establishes MIP tunnel to the H-NSP home agent; and

e) MS can then be contacted using its home IP address through the home agent on the H-NSP.

2.9.3.3.1.2 In the case of an airport handling vehicle, the node is attached to the local network and, thus, the network entry process is largely simplified:

a) during the scanning process the device needs to be able to determine if it is on a channel of a NAP providing airport services;

b) the H-NSP is based locally so the device can perform authentication directly; and

c) if authentication is successful, the MS performs NET entry and the H-NSP grants the device a local IP address.

2.9.3.3.2 AeroMACS discovery procedures

2.9.3.3.2.1 The AeroMACS profile allows two discovery procedures:

a) NAP discovery gives means to the MS, after scanning and decoding the "operator ID" element for DL_MAP, to select a particular operator to connect to; and

b) NSP discovery is mandatory in the profile. The MS will dynamically discover all NSPs in the airport during the network entry procedure. In order to accomplish that, the MS will be listening to the broadcast message with the NSP IDs sent by the BSs (SII-ADV MAC message advertisement).

2.9.3.4 *Roaming scenarios*

2.9.3.4.1 Overview

2.9.3.4.1.1 Roaming is the capability of wireless networks via which a wireless subscriber obtains network services using a "visited network" operator's coverage area. At the most basic level, roaming typically requires the ability to reuse authentication credentials provided/provisioned by the home operator in the visited network, successful user/MS authentication by the home operator and a mechanism for billing reconciliation and optionally access to services available over the Internet services.

2.9.3.4.1.2 In a possible roaming scenario, an aircraft landing on an airport network is managed by an NSP that is different from the aircraft home NSP (H-NSP) and thus acting as a visited NSP (V-NSP). Figure 35 shows the entities participating in roaming.

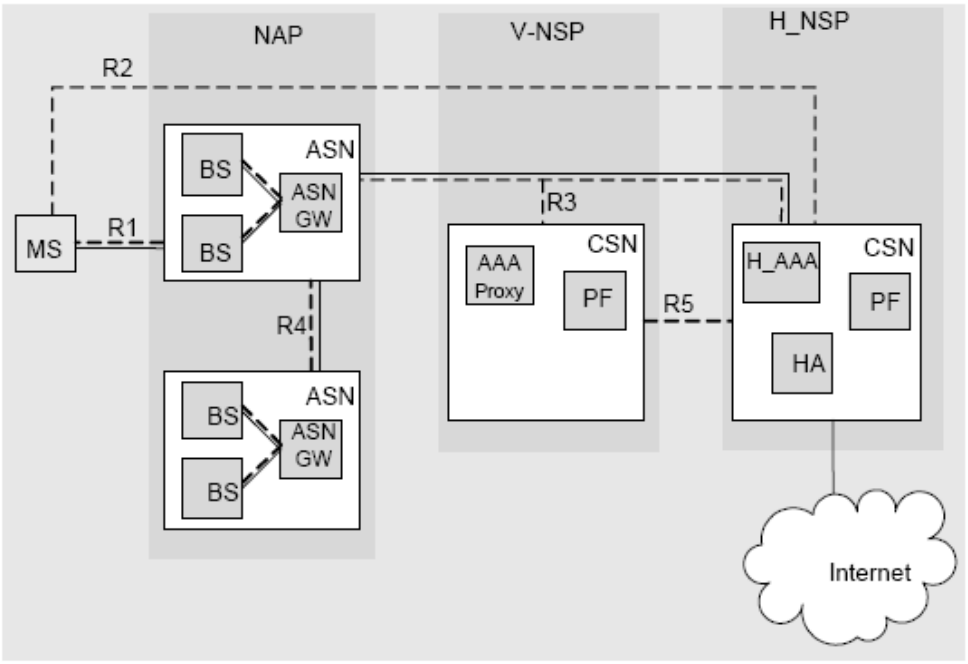


Figure 35. AeroMACS roaming architecture

2.9.3.4.1.3 The second foreseeable scenario is the use of one AAA server, shared by all the NAPs and outside the H-NSPs. As a consequence, no roaming scenario will occur.

2.9.3.4.2 Route optimization scenarios

2.9.3.4.2.1 Upon network entry, an MS selects an NSP that manages the connectivity of the subscriber to the network. In order to be able to access services from application service providers (ASP) present in other networks, data access needs to be established between the corresponding communication endpoints. Different mechanisms may be used for data access between communication endpoints that reside in networks managed by different NSPs, as depicted in Figures 36 and 37, which depict two different route optimization scenarios. In Scenario 1, the aircraft is attached to the home network (which is a global network managed by an ACSP or other), while in Scenario 2 the aircraft is attached to a visited network (e.g. a local ACSP in an airport or an ANSP network) through roaming. The following scenarios are deemed relevant for aviation purposes:

a) **Data access via home NSP:** This is the classic deployment where the H-NSP manages the HA function which establishes the paths between the mobile router (MR) behind the MS on the aircraft and the correspondent nodes (CN) in the ATM ground network. As a consequence, the application flow to the end node is relayed from/to the mobile node care-of-address in the foreign network to the HA and later to the CN.

b) **Data access via correspondent router:** This deployment model provides the opportunity to the mobile node to establish an optimized path directly with the correspondent router (CR). This leads to the benefit of optimizing performance and having direct access to the CN and the ATM ground network (which can be located in the local access network), rather than having all traffic flowing to a central HA located in a remote location (shown in Figure 37).

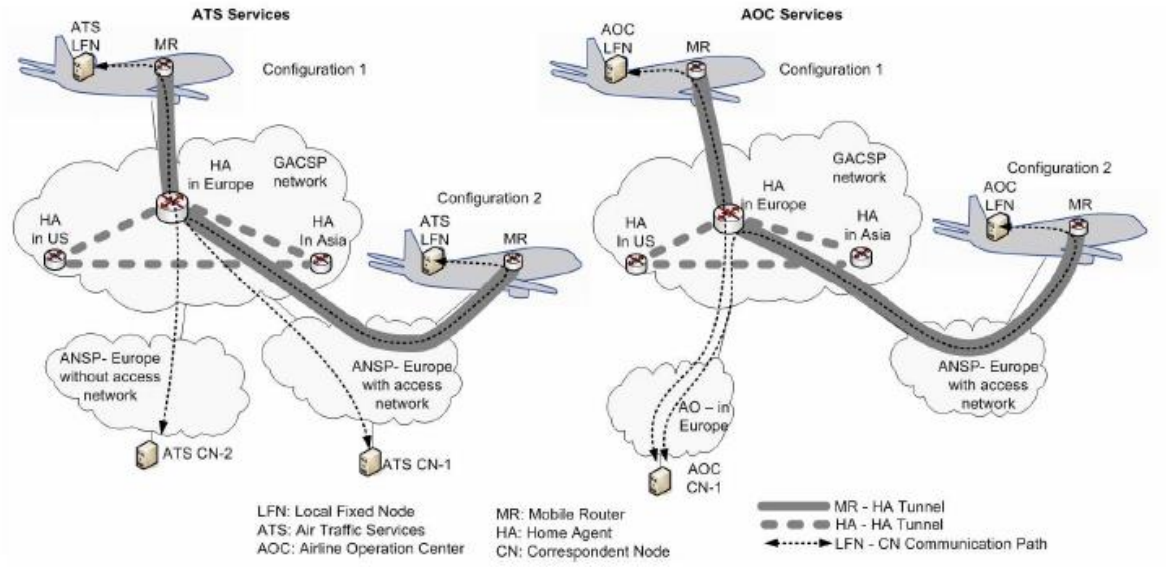


Figure 36. Route optimization Scenario 1 - Data access via home NSP

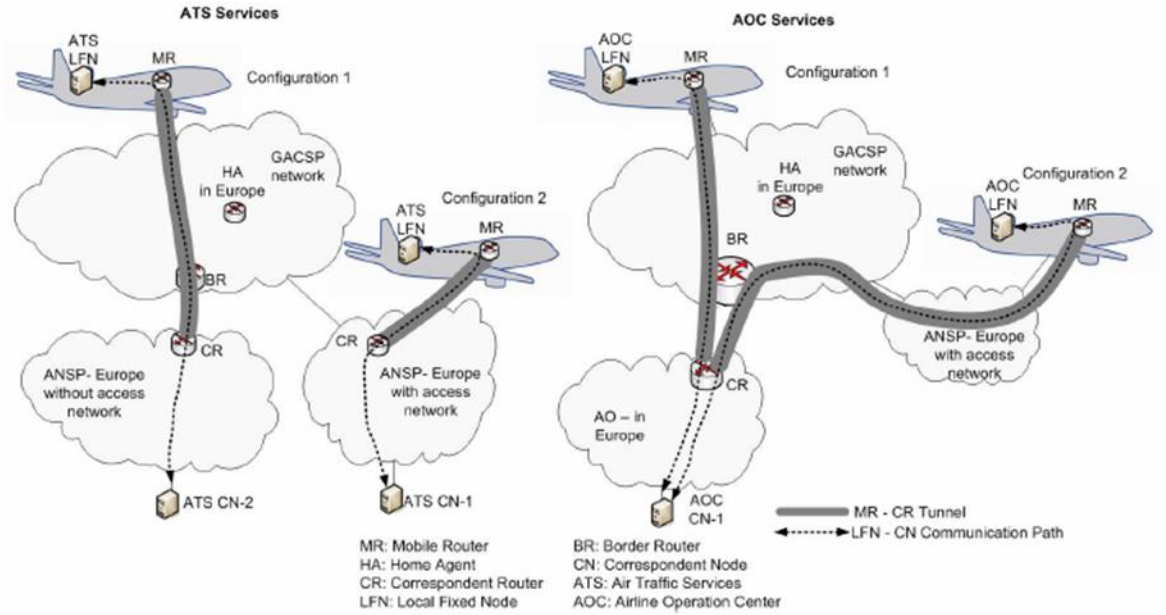


Figure 37. Route optimization Scenario 2 - Data access via correspondent router (CR)

2.9.3.4.2.2 Several technical solutions are undergoing definition to handle route optimization (RO with mobile IP). One option is the global HAHA, where local home agents can be deployed as illustrated in Figure 36, the other corresponds to the use of correspondent routers (CR) operated locally by ANSPs. In all cases, a global home agent must be accessible at all times.

2.9.3.5 *Application service provider (ASP) deployment models*

2.9.3.5.1 In an airport, AeroMACS service may offer seamless connectivity for aircraft to access the airport network and its services, ANSP network as well as airline or service partner operational centres to access data link applications. AeroMACS may also be used to extend private networks that are owned by different airport service providers within airport premises or to interconnect networks within airport regions. Figure 38 provides the overall context of AeroMACS network in the airport.

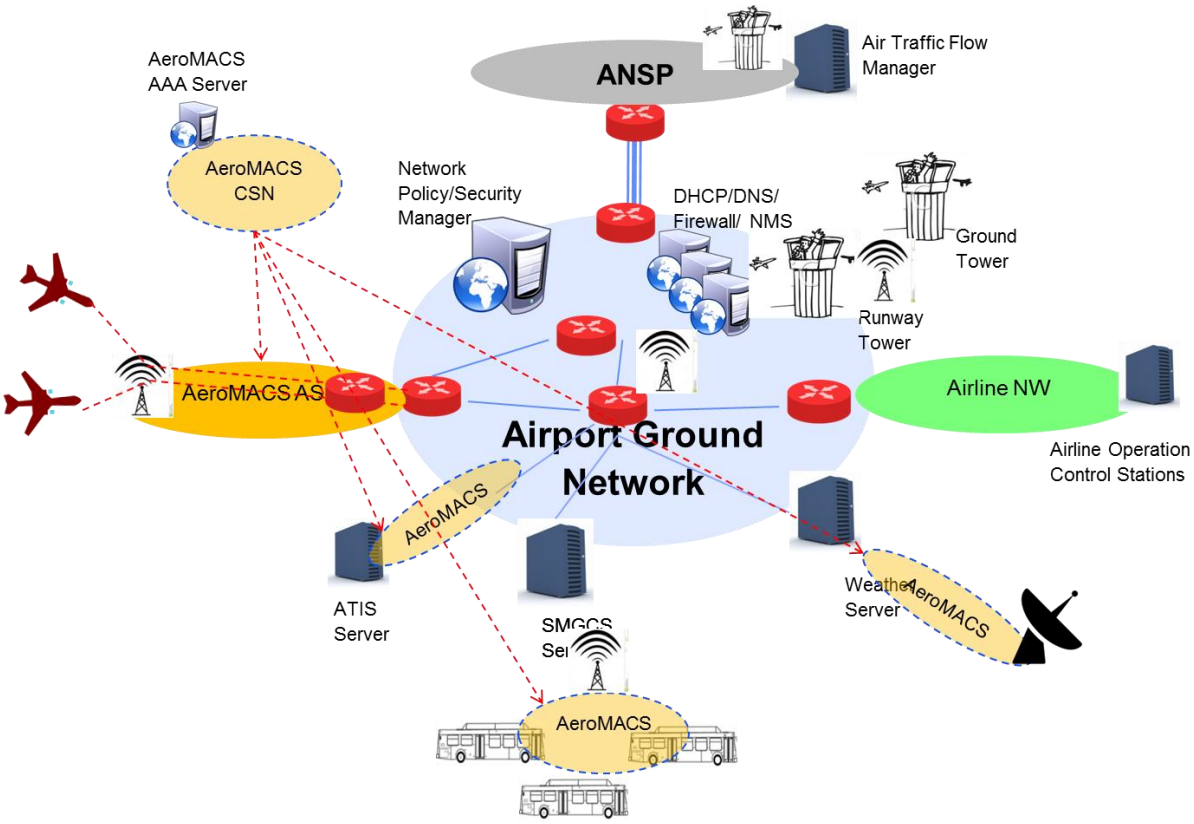


Figure 38. AeroMACS network from overall perspective

2.9.3.5.2 In Figure 38, AAA should be able to appropriately distinguish aircraft (aviation internet) users from the other users and authorize appropriate service flows to the users accordingly. This can be accomplished by using different profiles of digital certificates for different users.

2.9.3.5.3 If AeroMACS networks are deployed to support both aircraft traffic and other private network traffic, AeroMACS ASN should be able to identify and route the traffic belonging to different networks respectively.

2.9.3.5.4 Figure 39 shows various traffic flows through an AeroMACS network, when it is deployed to interface with multiple networks.

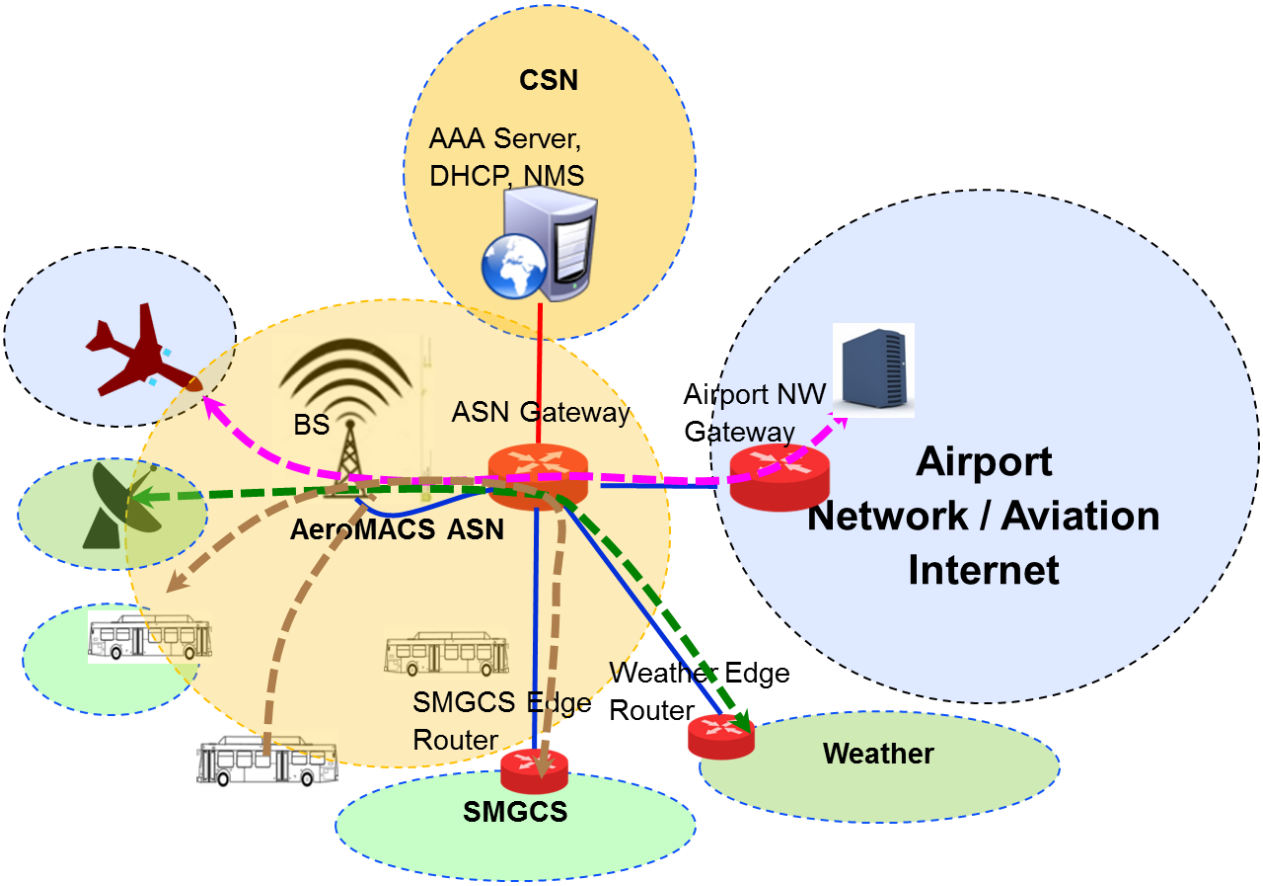


Figure 39. Various traffic flows through AeroMACS

2.9.3.5.5 In the above figure:

a) aircraft uses AeroMACS to connect to aviation internet;

b) weather service provider uses AeroMACS as a point to point link to connect a weather sensor to its network; and

c) SMGCS uses AeroMACS to contact vehicles in an airport.

2.9.3.5.6 In this scenario, the ASN handles traffic from all the three independent networks, hence it becomes a common medium to transport packets for multiple networks. Therefore, considering aviation safety internet, its security perimeter is limited to the airport network gateway as ASN handles multiple network traffic. To mitigate such risks, a secured pipe should be extended from edge router to edge router, when an AeroMACS ASN infrastructure is shared with multiple networks. Other private networks may also choose to have their own security mechanisms over a shared AeroMACS network to safeguard their network traffic.

2.9.3.6 *Deployment scenarios*

2.9.3.6.1 The deployment scenarios of an AeroMACS network are analyzed in this section. As an example of a trans-oceanic roaming operation, Figure 40 shows the scenarios of AeroMACS services offered through a dedicated network and also a shared network in the John F. Kennedy (JFK) and Charles de Gaulle (CDG) Airports. The JFK Airport is shown with a dedicated ASN infrastructure installed by the

NSP/MSP exclusively for aircraft connectivity. The CDG Airport is shown with the MSP using a shared AeroMACS network provided by a third party network access provider (NAP). Assume that the local service provider uses an AeroMACS network to offer both an aviation internet service as well as local network connectivity services (shared network).

2.9.3.6.2 At the JFK Airport, the AeroMACS network is exclusively deployed for MSP subscribers. Both the ASN and CSN networks belong to MSP. Hence, the CSN AAA server (belonging to MSP) acts as the final authenticator approving aircraft to log into the AeroMACS ASN network. During logon digital certificates are exchanged between the AAA server (under MSP administrative network) and aircraft for mutual authentication. A common certification authority should have either signed the certificates of the AAA server and the aircraft, or should be available in the trusted path of the certificate authorities to establish the authenticity of the entities. On successful verification, the data connections are established with aircraft at the ASN. The ASN gateway is connected to the MSP gateway which offers connectivity to aviation internet. Aircraft access ANSP services or airport services through the aviation internet as shown in Figure 40. In this configuration the ASN is exclusively used for aircraft communications and hence the safety network boundary extends up to the aircraft.

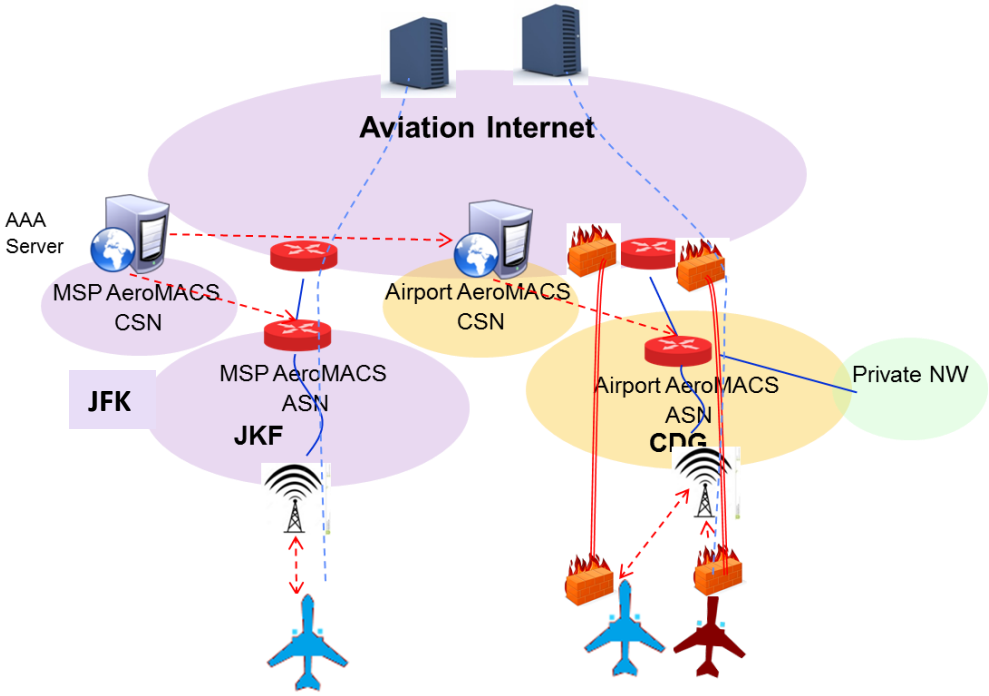


Figure 40. AeroMACS offered by NSP/MSP

2.9.3.6.3 At the CDG Airport, the ASN/CSN infrastructure is deployed by a third party service provider. When an aircraft, having MSP subscription, tries to log into the network, the CSN (belonging to a third party local network) will not have MSP subscriber account details. In this case, the AAA server at the CSN network will act as a proxy and contact the AAA server at the MSP network to authenticate the aircraft. The aircraft is required to use the AeroMACS attribute–value pair (AVP) and operator name to indicate its preferred network operator. As a prerequisite, MSP and the particular airport network service provider would have a prior business agreement and the AAA servers are connected to handle this back end authentication. On approval from the MSP AAA server, access to the airport network/aviation internet is granted to the aircraft. In this scenario as the airport network ASN is shared across multiple networks, the security boundary for the aviation internet can be considered only up to the airport network gateway as ASN handles multiple network traffic. Hence, to ensure security a VPN connection is

established between the aircraft edge router to the airport network gateway to transport packets safely through the ASN network. Message flows between various network elements in the AeroMACS network is provided in Figure 41.

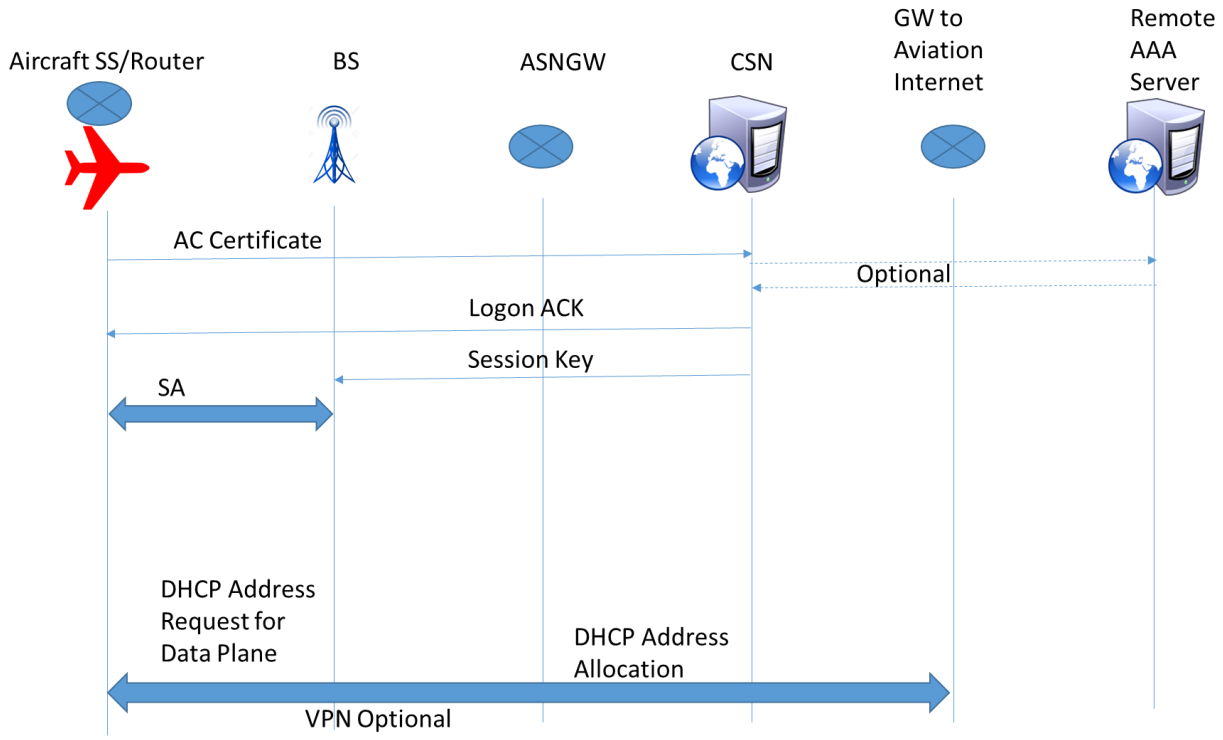


Figure 41. Message flows in the AeroMACS network

2.10 AVIONICS ARCHITECTURE

The use of AeroMACS is relevant to both the ACD and AISD domains, to support ATM and AOC applications. In this section various AeroMACS communication architectures and scenarios assuming current and future ACD and AISD are given with each one representing a possible airborne AeroMACS implementation.

2.10.1 ARU "on/off" control

2.10.1.2 Operation of the AeroMACS radio unit (ARU) RF transmitter is only allowed while the aircraft is on the ground. This characteristic defines an ARU interface to control the "on/off" mode of the ARU RF transmitter. The "on/off" control logic should be implemented within the ARU to supply (or not supply) power to the AeroMACS RF transmitter based on the aircraft status (airborne or not airborne) as indicated by the discrete inputs.

2.10.1.3 The ARU should provide two standard open/ground discrete inputs to allow remote switchable on/off control of the device, such as from the weight-on-wheels (WOW) air/ground strut switch or from other avionics or flight deck switch. The ARU RF transmitter should be powered up **only** when both "on/off" control discrete inputs are in the grounded state thus indicating that the aircraft is on the ground. When either discrete input is open then the ARU RF transmitter should be powered down. Other functions within the ARU, such as BIT or health monitoring/reporting, may remain powered up during flight as long as all RF transmissions are inhibited.

2.10.2 **ACD and AISD**

2.10.2.1 There are two data domains of interest with respect to AeroMACS; the aircraft control domain (ACD) and the airline information services domain (AISD). The AeroMACS domain does not include the passenger information and entertainment services domain (PIESD) and the passenger owned devices domain (PODD) which are to be physically separate from the AeroMACS domain.

2.10.2.2 The ACD data includes FANS-1/A, ARINC 623, and FMC AOC applications such as winds aloft, etc. ACD also includes ACARS AOC data from the CMU such as the OOOI message, crew info, etc., as well as data from other LRUS such as CMC, ACMS, cabin terminals, IFE ACARS data and EFB ACARS data. In the future, ACD will expand to include future air traffic services applications defined under ATN.

2.10.2.3 The AISD data consists of IP-based messaging from an AISD IP router. IFE and EFB with IP connections to the AISD IP router may be part of the AISD network. In addition, AISD data may include navigation databases, maps and charts, graphical weather and services available through system-wide information management (SWIM).

2.10.2.4 The AeroMACS radio unit should be designed to support and interface with the future IPS router envisioned to be installed in the ACD at a longer term.

2.10.2.5 If the ARU has the appropriate security capabilities then the ARU could simultaneously be connected to the ACD and the AISD domains. This approach is very similar to solutions currently envisaged for easing introduction of/transition to new IP-based satellite communication services in the ACD (Iridium and Inmarsat-SBB).

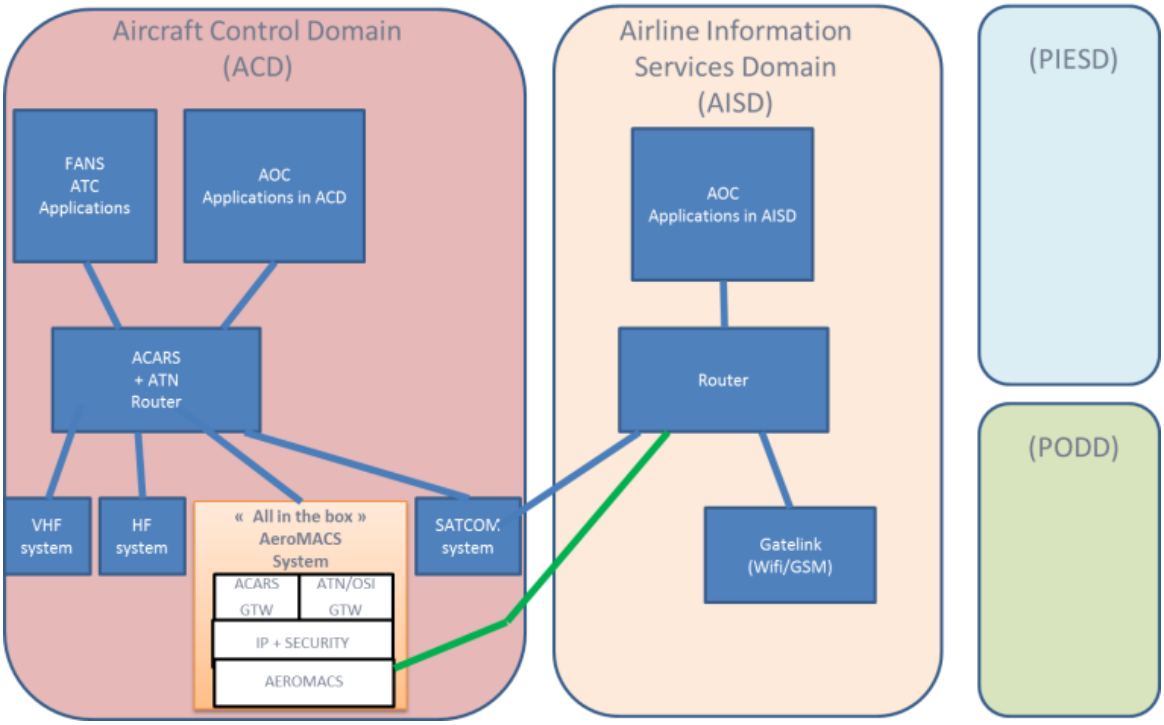


Figure 42. AeroMACS radio unit integration into aircraft

2.10.2.6 Since AeroMACS is a native-IP Layer-2 device, it could be connected directly to the IP router through the IP convergence sublayer within the AeroMACS device. On the other hand, connectivity to non-IP ACARS+ATN router in the ACD would be possible by implementing an appropriate subnetwork dependent convergence function layer and gateway depicted in Figure 42. A similar solution has been already tested and validated under the SANDRA Project, allowing interoperability between ARUs and OSI routers.

2.10.2.7 An additional security capability, on top of the AeroMACS security framework, should be implemented at the ARU if simultaneous connectivity to IP routers in the ACD and AISD is supported to segregate the ACD from the AISD domain hence preventing the open IP world having access to the ACD domain.

2.10.2.8 It has to be noted that the needed security requirements to be guaranteed by this scenario increase the complexity of the AeroMACS unit (AU), while maintaining the advantage of having a single AeroMACS unit (AU) connecting both ACD and AISD users.

2.10.3 Scenario 1A – Installation of the AeroMACS unit (AU) in the AISD

2.10.3.1 Scenario 1A, as shown in Figure 43, assumes that an AU could be introduced as an additional communication media of the AISD domain, attached to the existing AISD IP router, as a complement or alternative technology to the current or upcoming data link technologies.

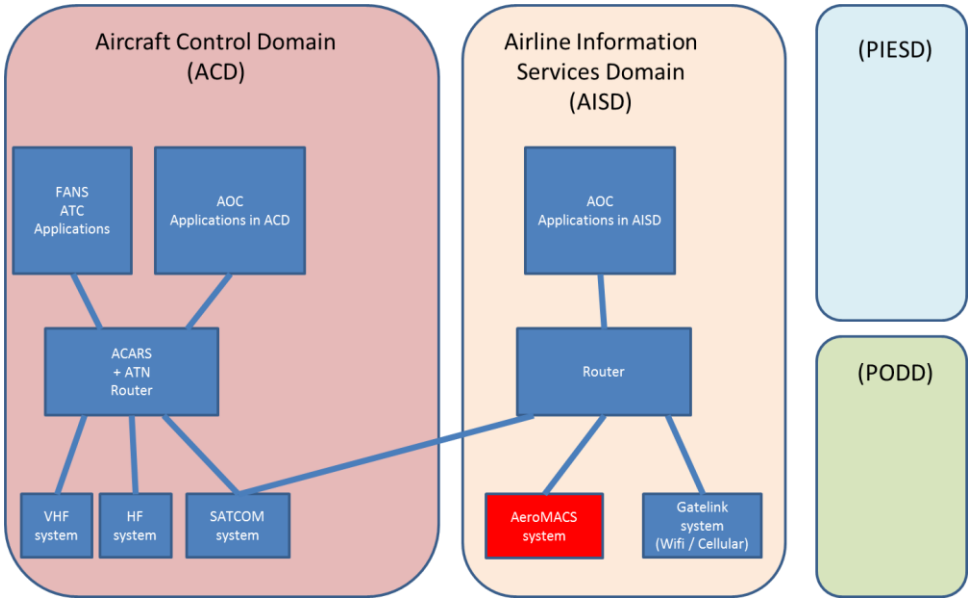


Figure 43. AeroMACS radio unit integration into aircraft - Scenario 1A

2.10.4 Scenario 1B – Installation of the AeroMACS unit (AU) in the ACD domain

2.10.4.1 Scenario 1B assumes, in the short- medium-term, the availability of an AeroMACS unit connected to the AISD domain but designed and pre-installed to be hosted in the ACD domain in preparation of the longer term Scenario 3A/B described farther below. In terms of initial capabilities and supported services this AeroMACS unit is the same as the one shown in Scenario 1A in the longer term.

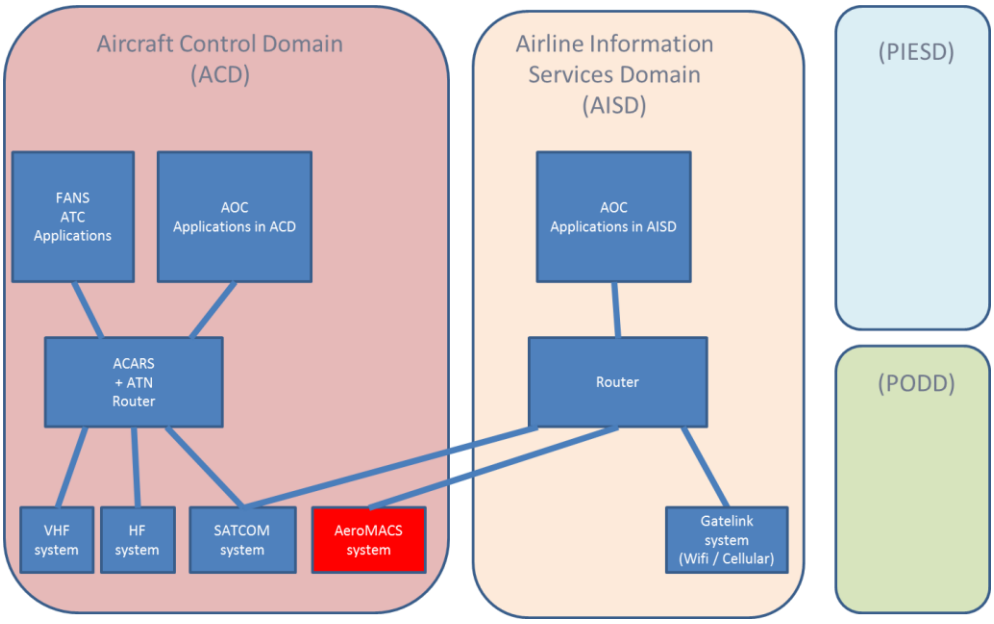


Figure 44. AeroMACS radio unit integration on aircraft - Scenario 1B

2.10.5 Scenario 2A – Installation of the AeroMACS unit (AU) in the ACD

2.10.5.1 Scenario 2A assumes that the AeroMACS unit (AU) could be developed and certified as a more global equipment providing in the same "box" the following capabilities: 1) the AU (mobile station) functions; 2) an initial IP router function; 3) a (optional) security function at IP level; 4) a function allowing the encapsulation of ACARS messages over IP (and AeroMACS); and 5) a function allowing the encapsulation of ATN/OSI messages over IP (and AeroMACS). The difference with Scenario 1 is that an AeroMACS unit in this scenario would be designed to directly interface with the ACD airborne network and with peripheral ACD avionics systems. In particular, the AeroMACS unit could be designed with the physical inputs/outputs modules (e.g. ARINC 429, AFDX, etc.) necessary to interface with the ACD systems generally involved in the monitoring, control, and maintenance of ACD radio communication systems (e.g. to support possible interfaces with an ACD radio management panel (RMP) or multi-purpose display unit (MCDU), with the failure warning computer (FWC), with the aircraft centralized maintenance system (CMS), and data loading and configuration system, etc. The equipment would also be designed with provisions to support an interface with the future ATN/IPS router envisioned to be installed in the ACD. However, in this scenario, the AU will not be physically connected to any of the systems in the ACD domain. The only connectivity of the AU will be to the IP router in the AISD as shown in Figure 45.

2.10.5.2 Additional security measures beyond the AeroMACS security framework can optionally implement a security capability at IP level (e.g. IPSEC) to improve privacy and integrity of communications and optional firewall capability and to improve segregation of the ACD domain from the AISD.

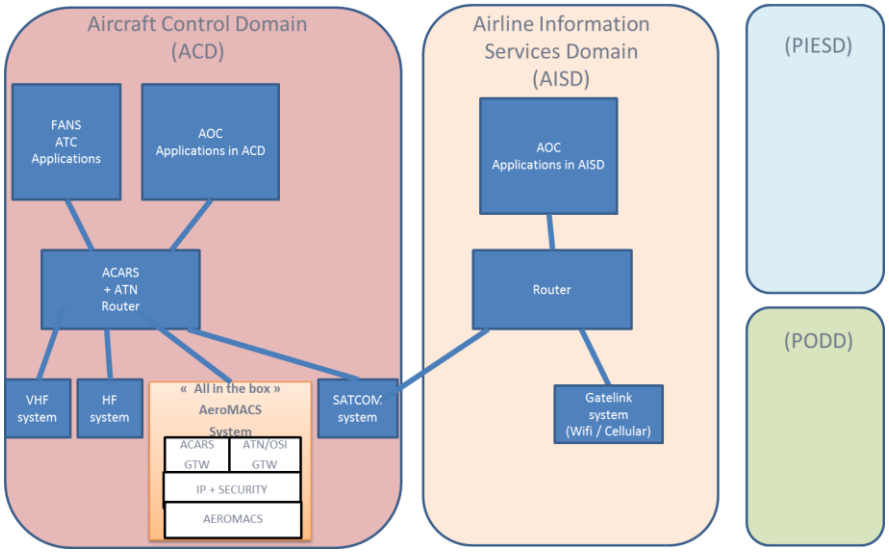


Figure 45. AeroMACS radio unit integration into aircraft - Scenario 2A

2.10.6 Scenario 2B – Installation of the AeroMACS unit (AU) in the ACD and connected to ACD and AISD

2.10.6.1 In this scenario the AeroMACS unit could simultaneously be connected to the ACD and the AISD domains, due to its capability to guarantee the needed segregation among ACD and AISD users. This approach is very similar to solutions currently envisaged for easing introduction of/transition to new IP-based satellite communication services in the ACD (Iridium and Inmarsat-SBB).

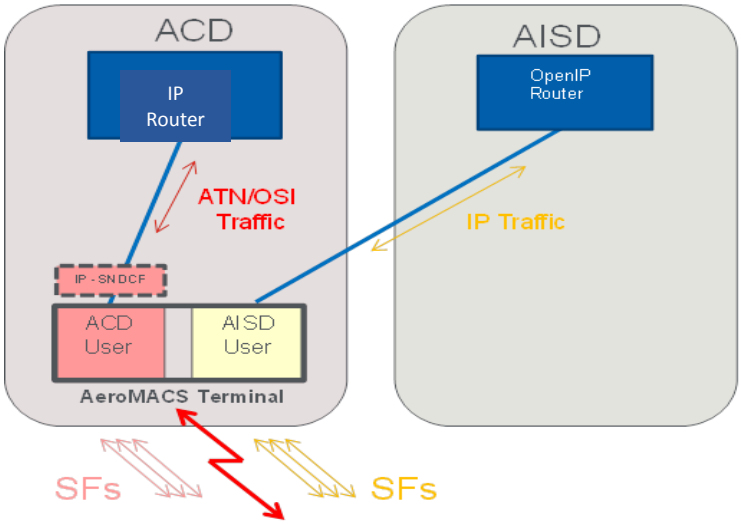


Figure 46. Scenario 2B connection between AeroMACS radio unit and ACD/AISD

2.10.7 Scenario 3A – Installation of the AeroMACS unit (AU) in the ACD with ATN/IPS router

2.10.7.1 Scenario 3A assumes that the AeroMACS unit (AU) in the ACD domain will be attached to the IPS router in the ACD over the native IP convergence sublayer (IP-CS) function.

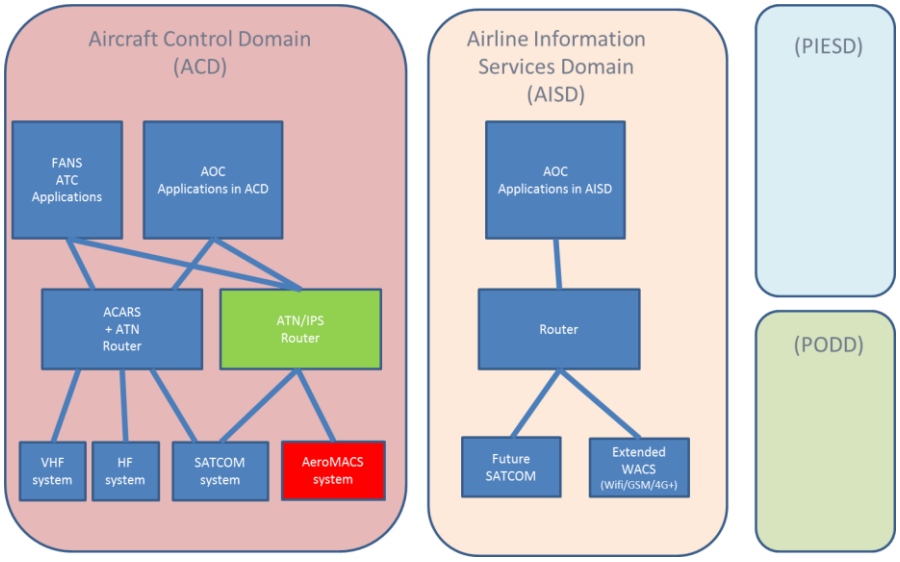


Figure 47. AeroMACS radio unit integration into aircraft - Scenario 3A

2.10.8 Scenario 3B – Installation of the AeroMACS unit (AU) in the ACD with IP connectivity to both ACD and AISD

2.10.8.1 Scenario 3B assumes that the AeroMACS unit (AU) will be installed in the ACD and attached to both the IPS router and the AISD IP router simultaneously over IP-CS. The needed segregation between ACD and AISD users will be granted by the AeroMACS Unit (AU) and by IP level security capabilities (as explained in Scenario 2B) implemented between the IPS and IP routers outside the AeroMACS unit (AU).

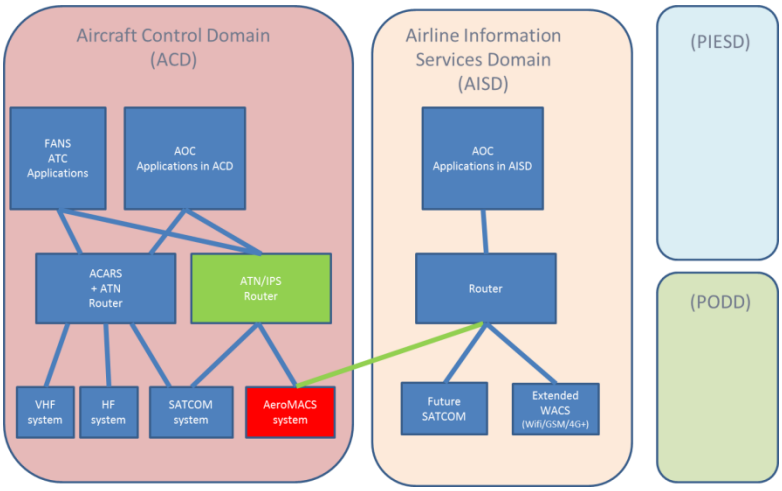


Figure 48. AeroMACS radio unit integration into aircraft - Scenario 3B

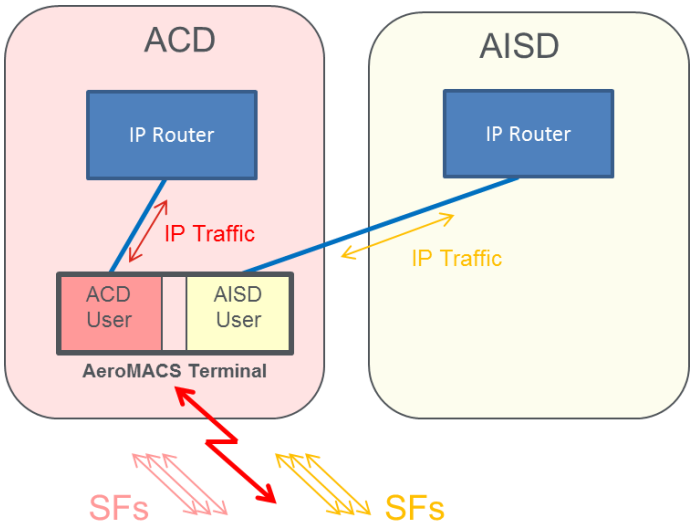


Figure 49. Scenario 3B connection between AeroMACS radio unit and ACD/AISD

2.10.8.2 The above scenarios define different strategies for implementing an AeroMACS system on aircraft, which may lead to the definition of different airborne AeroMACS system architectures.

2.10.8.3 It is worth underlying the possibility of using two separated ARU devices inside a single AeroMACS unit connected to a single antenna. This solution would grant a physical segregation between ACD and AISD, thus negating the need for an IP firewall.

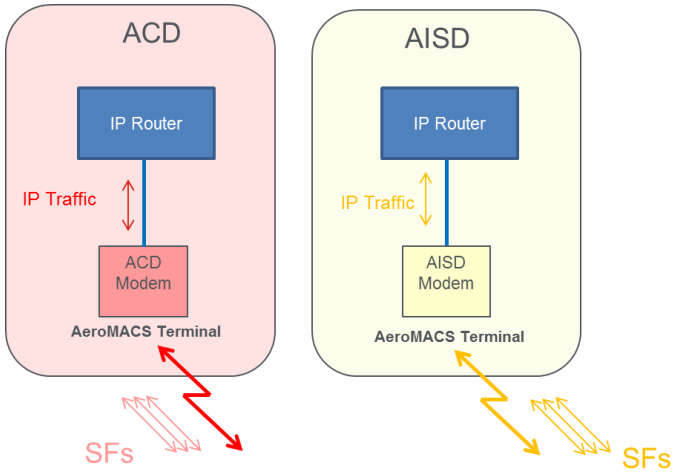


Figure 50. Physical segregation between ACD and AISD with separated AeroMACS radio units

2.11 SECURITY

2.11.1 Introduction

2.11.1.1 An AeroMACS security function is required to provide peer entity authentication of AeroMACS SS and the AAA server through the BS to permit network entry of the SS and to encrypt information exchange over the AeroMACS RF link. A security framework based on public key infrastructure (PKI) is therefore necessary to support those security functions.

2.11.1.2 It is desired that the security provisions for aeronautical communications be based on the same security framework to provide consistency across all aeronautical data links as well as to reduce the security infrastructure investments.

2.11.1.3.1 ICAO is currently working to define the overall security policy and the framework. However, this definition is incomplete. In the absence of that specification and requirements at the publication of the AeroMACS Manual, it contains the security policy, certificate profile and the framework to be implemented by AeroMACS. It is expected that a broad security policy and the framework requirements will be incorporated in another ICAO document and security provisions pertinent to AeroMACS only will remain in the AeroMACS Manual.

2.11.2 IEEE 802.16 security profile

2.11.2.1 The IEEE 802.16 security sublayer provides subscribers with authentication and data privacy. An authorization/SA module is responsible for validating the authenticity of subscriber stations and management of security associations (SA) for IEEE 802.16 connections.

2.11.2.2 SA associates encryption keys and algorithms with a traffic type so that the packets belonging to a particular traffic type can be encrypted as per its SA definitions.

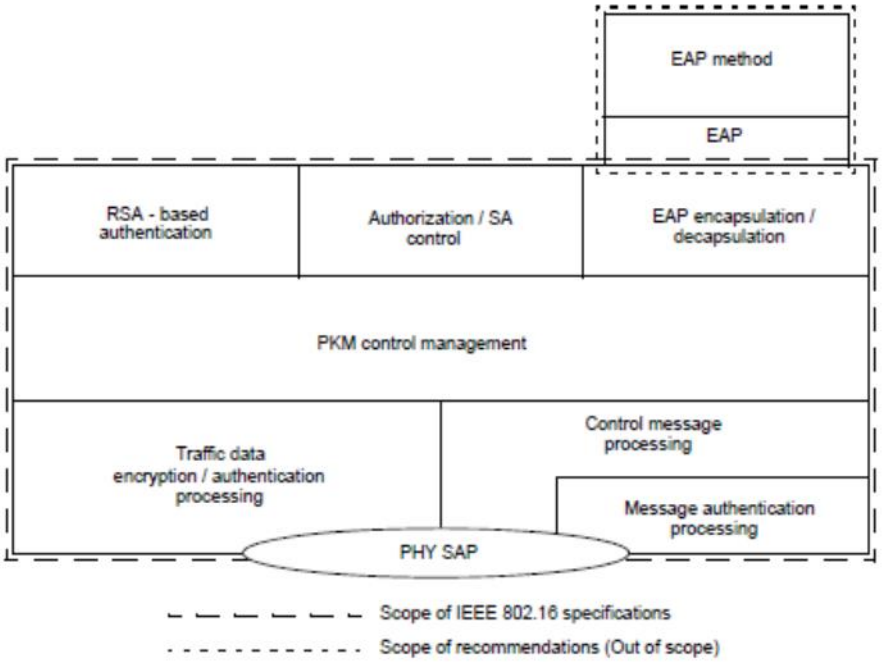


Figure 51. Scope of AeroMACS security provisions

2.11.2.3 *AeroMACS supports only EAP-based authentication*

2.11.2.3.1 The RSA authentication method is not supported by AeroMACS.

2.11.2.3.2 The EAP method offers mutual authentication in which both BS and SS authenticate each other. EAP supports multiple authentication schemes and hence provides more flexibility to the network operators in choosing subscriber authentication methods. For example, EAP-TLS is based on X.509 certificates, while EAP-SIM is based on a subscriber identity module used in mobile phones.

2.11.2.3.3 AeroMACS supports private key managementv2 (PKMv2) which supports the EAP method for mutual authentication of both SS and BS and their key management. PKMvv1 is not supported by AeroMACS.

2.11.2.3.4 In addition to PKMv2 in a typical deployment environment involving large networks, authentication and policy management for subscribers would be done at centralized locations instead of being managed locally at every BS level. In such scenarios, protocols such as RADIUS or DIAMETER may be used in conjunction with EAP methods to authenticate/authorize subscribers to use network resources.

2.11.2.3.5 The traffic encryption module supports a set of encryption algorithms to protect the message data. Depending upon the definitions in SA, this module performs encryption/decryption of the data that enter or leave the AeroMACS device.

2.11.3 **Security sublayer for AeroMACS (Layer 2)**

2.11.3.1 This section contains the definitions of the Layer 2 security sublayer down-selected from WiMAX (IEEE 802.16) profile specifications. Figure 52 provides the overall stack architecture of security layers across various network components such as SS, BS, ASN G/W and AAA servers.

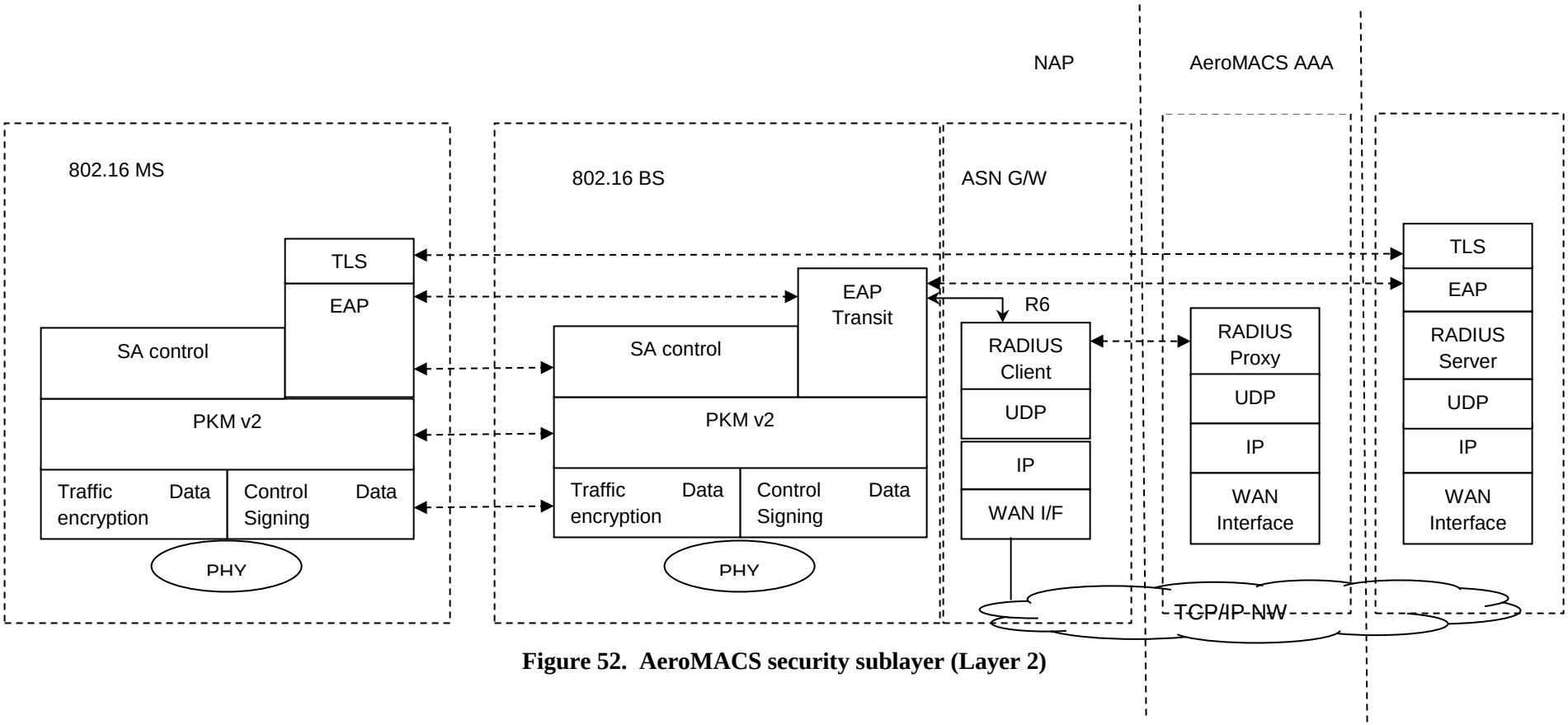


Figure 52. AeroMACS security sublayer (Layer 2)

2.11.4 **Key management**

2.11.4.1 *Authentication protocol*

The EAP protocol is required for the AeroMACS system.

2.11.4.2 *EAP authentication methods*

EAP TLS offers strong authentication based on X.509 certificates exchanged between the authenticator and the mobile station. This method is used for AeroMACS.

2.11.4.3 *Guidance on the PKI certificate policy*

2.11.4.3.1 The PKI certificate policy (CP) defines the procedural and operational requirements to which AeroMACS entities must adhere when issuing and managing digital certificates within the AeroMACS public key infrastructure (PKI). AeroMACS' certificates are controlled by the AeroMACS PKI policy authority (APPA) that determines how this CP applies to certificate authorities (CAs), registration authorities (RAs), certificate status authorities (CSAs), device sponsors, relying parties and other PKI entities that interoperate with or within the AeroMACS PKI.

2.11.4.3.2 A certificate issued in accordance with this CP conveys within the aerospace community a level of digital identity assurance associated with the subject of the certificate. Certificates created within this PKI will be medium-assurance certificates for devices with hardware cryptographic modules. In this document, the term "device" means a non-person entity, i.e. a hardware device or software application.

2.11.4.3.3 A PKI that uses this CP will provide the following security management services:

a) key generation and storage;

b) certificate generation, modification, re-key, and distribution;

c) certificate revocation list (CRL) generation and distribution;

d) directory management of certificate-related items;

e) certificate token initialization, programming, and management; and

f) system management functions to include security audit, configuration management and archive.

2.11.4.3.4 This policy establishes requirements for the secure distribution of self-signed root certificates for use as trust anchors. These constraints apply only to root CAs that choose to distribute self-signed certificates.

2.11.4.3.5 Other important documents in the AeroMACS PKI include the certification practice statements (CPS), registration authority agreements, subscriber agreements, privacy policies, and memoranda of agreement.

2.12 SUPPORT FOR BROADCAST AND MULTICAST APPLICATIONS IN AEROMACS

2.12.1 Introduction

2.12.1.1 This section provides guidance material on how AeroMACS may initially support broadcast and multicast applications as well as how it can continue to support these applications efficiently in an evolutionary way in the future when the supported traffic will be increasing.

2.12.1.2 In this section, the broadcast and multicast capability refers to functionalities that take advantage of the PMP (point to multipoint) operation of the AeroMACS link to use the radio resources efficiently by transmitting the same data payload from one BS to multiple SSs in a single multicast message (as opposed to transmitting the same information to each SS in different unicast messages).

2.12.1.3 PMP operation is independent from the operation of IP multicast and broadcast or the execution of multicast and broadcast services (MBS) at the application layer.

Note 1.— The applications requiring IP multicast and broadcast or MBS are not considered in this manual.

Note 2.— Higher layer multicast services can be transported over unicast AeroMACS data links even if the PMP operation is not supported within AeroMACS. In such a case, support for broadcast and multicast application does not optimize the radio resources.

Note 3.— It is the responsibility of the AeroMACS user to associate higher layer multicast services to corresponding AeroMACS multicast service flows through appropriate configuration of the service flow classifications. An example of service flow classification is the use of unique differentiated services code point (DSCP) values for multicast service flows. This process is needed in order to optimize the radio resources.

2.12.1.4 It should be noted that the AeroMACS PMP operation applies only to BS to SSs messages and it does not apply to the SS to a BS direction. The SS to BS transmissions are always unicast in AeroMACS as the MS transmissions are always towards the (master) BS.

2.12.2 Rationale for multicast services

2.12.2.1 The list below indicates examples of the potential MBS services envisaged to be transported over AeroMACS:

a) flight information services (D-ATIS, D-OTIS, D-RVR, D-SIG, D-SIGMET);

b) TIS-B;

c) NOTAM;

d) graphical weather information (WXGRAPH);

e) airport delay information;

f) broadcast weather information via SWIM; and

g) SURV.

2.12.2.2 In order to demonstrate the benefits of multicast over unicast, an estimation of the amount of data generated by specific services has been derived using the number of messages per dialogue and the size of these messages, together with the maximum service latency, the average data rate (in bps) can be determined to comply with the latency requirement.

2.12.2.3 Based on this analysis, the estimated peak data load generated by the ATC multicast services operated by a single aircraft ranges from 1 to 9 kbps An AOC multicast service would be expected to transmit a heavier load of data. The only available example of a computation of the expected data rate generated by an AOC multicast service has been done with WXGRAPH.

2.12.2.4 Table 25 below depicts the required bandwidth at an airport operating AeroMACS based on the operational scenarios as presented in the AeroMACS MASPS. Table 25 indicates the expected peak data rate (i.e. if all the aircraft within the BS service volume use the multicast service simultaneously) per BS. It can be observed that an AeroMACS deployment can cope well with ATC multicast services. However, when multicast AOC services are also enabled, the benefit of operating multicast connections becomes more significant.

Operations/hour per airport	**Assumption of number of simultaneous aircraft per airport**	**Assumption of number of BS (cells, i.e. sectors) deployed in airport**	**Assumption of number of MS under coverage of each BS**	**Estimated peak traffic generated per BS by ATC multicast services [kbps]**		**Estimated peak traffic generated per BS by WXGRAPH [kbps]**	
				Unicast	**Multicast**	**Unicast**	**Multicast**
20	10	3	3.33	30	9	250	75
50	25	9	2.78	25		208	
100	50	15	3.33	30		250	

Table 26. Expected peak data rates per BS

2.12.2.5 Considering the above analysis, multicast support by AeroMACS will provide the following gain to the overall AeroMACS system capacity:

Multicast gain [kbps] =

(Multicast services estimated load [kbps]) * (Number of simultaneous MS in the same BS sector - 1)

Accordingly, the multicast gain in kbps and the percentage relative to the worst case (QPSK1/2: 1.8 Mbps) and best case (64 QAM: 9.1 Mbps) capacity can be estimated from the data in Table 26 above. The results are given in Table 27.

Airport size	ATC multicast services [kbps]					AOC (WXGRAPH) multicast service [kbps]				
	Unicast	Multicast	Gain (kbps)	Gain (per cent)		Unicast	Multicast	Gain (kbps)	Gain (per cent)	
				worst	best				worst	best
20	30	9	21	1.16	0.23	250	75	175	9.72	1.92
50	25		16	1.44	0.17	208		133	7.42	1.47
100	30		21	1.16	0.23	250		175	9.72	1.92

Table 27. Multicast gain possible in AeroMACS

2.12.3 Options for multicast and broadcast services

The possible options to support multicast/broadcast according to the AeroMACS profile and MOPS are shown in Table 28 below. This table also describes the support of security features for each option. The best option depends on the type and volume of multicast/broadcast services (MBS) to be transported over the data link, and the level of security required for these services.

Multicast option	Security on multicast connections	
	Yes	No
No	N/A	Unicast
MBS	MBS with MBSGSA	MBS with either: "No authorization" policy or SA with "No encryption" cryptographic suite.
Multicast group service	Multicast traffic connection with GSA	Multicast traffic connection with either: "No authorization" policy or SA with "No encryption" cryptographic suite.

Table 28. Options for multicast and broadcast service in AeroMACS

2.12.3.1 *Unicast*

2.12.3.1.1 If this option is implemented, all multicast and broadcast services are transmitted as unicast messages on the AeroMACS data link. The CID establishment, traffic classification and QoS rules for incoming traffic are applied the same way as the rest of the service flows.

2.12.3.1.2 This option requires no support for any additional item nor any additional test case. The AeroMACS profile "multicast transport connection" item may be set to N in this case.

2.12.3.1.3 This option is acceptable if the amount of traffic generated by the network due the transmission of MBS services is small. Note that the impact on the data transmitted over the radio grows proportionally with the number of SS requiring multicast services in the service volume.

2.12.3.2 *MBS with MBS group security association*

2.12.3.2.1 MBS is an efficient method to concurrently transport DL data common to a group of SS (called multicast group). Service flows and multicast CIDs transmitting MBS flows are instantiated by a BS or group of BSs (called a BS zone) and the registered SSs belonging to the multicast group learn from them. The existence of BS zones allows for the provision of macro diversity. If a multicast CID is encrypted, it requires the establishment of a MBS group security association (MBSGSA) per multicast CID to maintain the MBS key material (MAK, MGTEK and MTK). MBSGSAs are shared between the BS in the same MBS zone.

2.12.3.2.2 This option requires the support of a large number of items such as MBS MAP IE and management of MBSGSA multicast keys. These items are currently not mandated by the AeroMACS profile.

2.12.3.3 *Multicast traffic connections*

Multicast traffic connections (MTC) are the recommended way to support broadcast and multicast in AeroMACS operations. This section distinguishes between the two types of MTC: MTC without encryption and MTC with encryption. These two options are further described in the next two subsections.

2.12.3.3.1 Multicast traffic connections without encryption

2.12.3.3.1.1 In this option, the BS establishes a transport connection separately with each SS in the multicast group by using the same CID. Use of the same CID permits the authorized SSs to listen for the same CID in the DL frame and access the multicast/broadcast data payload in the frame. From the SS point of view, the CID is treated as a unicast connection. From the BS point of view, it is also treated as a unicast connection with the exception that classification rules in the BS should be configured to transmit multicast messages over that common CID. Since each CID is associated with a service flow, it is associated with the QoS parameters of that service flow. However, HARQ is not applicable for these flows.

2.12.3.3.1.2 An authorization policy is exchanged per BS and SS pair during network entry (or re-entry). The SS informs the BS about the types of authorization policy supported during the negotiation phase (SBC-REQ/RSP message exchange). Table 29 below from the WiMAX forum profile depicts the authorization policies supported by the AeroMACS profile.

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	No Authorization	11.8.4.2	o	Y	Y	
2.	EAP-based authorization	11.8.4.2	o	Y	Y	

Table 29. PKMv2 authorization policy support - initial network entry

2.12.3.3.1.3 The "no authorization" option avoids the necessity to perform authorization and encryption for MTC, however, setting this option in the SBC-REQ/RSP exchange affects all the service flows established for that SS. Therefore, it is not acceptable for AeroMACS since it precludes unicast connections from being secured and should not be implemented.

Note.— The following encryption discussions describe secure unicast operations with unencrypted multicast traffic connections.

2.12.3.3.1.4 Cryptographic suites are combinations of mechanisms for encryption, data authentication and TEK exchange, and are specific to a security association (SA). During the authorization exchange, the BS sends the SS a list of SA descriptors informing about the cryptographic suites used by the static SAs that are active. During dynamic service addition (DSA) SAID is mapped to a given SFID. Table 30 below, from the WiMAX forum profile depicts the cryptographic suites supported by the AeroMACS profile.

2.12.3.3.1.5 IEEE Std 802.16-2009 does not preclude different SS under a BS control to have different active SA, of which some SS use key exchange, encryption and data authentication, and some SS do not. Therefore, to support unsecure multicast connections for some SS within the BS service volume, it is recommended that each BS configures a static CID well known to all SS participating in the multicast group. Upon network entry, the CID and associated SFID are established for each SS in that multicast group and a corresponding SA supporting no security is activated and associated to this CID/SFID. Note that it must be a unicast SA, meaning that it is established independently with each SS. However, since the data is sent unencrypted, all the SSs within the service volume should also be able to decode the received data.

Note.— All SSs need to have authenticated network entry. After network entry, each SS can have both secure and unsecure connections. Unsecured service flows may be used for multicast traffic and secure service flows must be used for unicast traffic. The message sequence chart in Figure 53 below illustrates this approach.

Item	Description	Reference	Status	BS Required	MS Required	Comments
1.	No data encryption, no data authentication & 3-DES, 128	11.9.14	o	Y	Y	This cryptographic suite means no encryption and no TEK exchange.
6.	CCM-Mode 128-bit AES, CCM-Mode, AES Key Wrap with 128-bit key	11.9.14	o	Y	Y	

Table 30. Supported cryptographic suites

2.12.3.3.1.6 This unsecure multicast method can be used for services that do not require security at the AeroMACS level.

2.12.3.3.1.7 To make the multicast function operate in every AeroMACS ASN, it is required that the allowed set of CID(s) is fixed globally. This option uses the support of the "multicast traffic connection" item and the support of the "no data encryption […] cryptographic suite" but is NOT supported by AeroMACS.

Note.— It is described below that the use of unencrypted multicast is permitted as long as the subscriber station is authenticated upon entry to the AeroMACS network using the appropriate cryptographic suite.

2.12.3.3.1.8 Figure 53 below depicts the message exchange during a normal network entry involving the creation of secured unicast DL/UL traffic connections and unsecured multicast DL traffic connections. Note that the unsecured multicast CID3 needs to be the same for all the SS connected to the same BS, however, the SAID is created independently per SS.

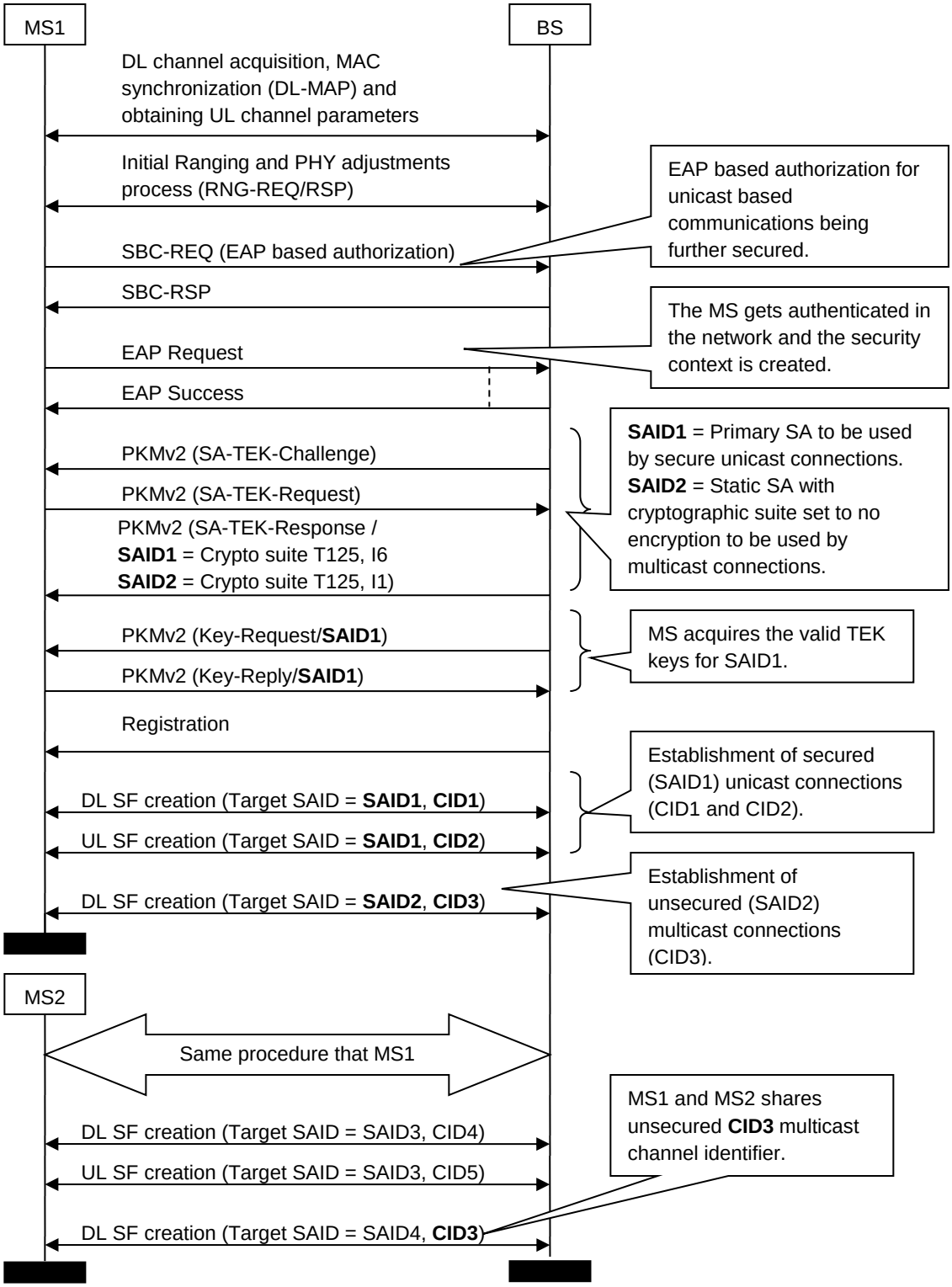


Figure 53. Establishment of encrypted unicast and unencrypted multicast connection in AeroMACS

2.12.3.3.1.9 This solution does not compromise PKMv2 authorization and authentication which is established when the SS enters the network. In addition, this solution does not preclude encryption in unicast services which are established whenever the BS and MS initiates services flows linked to security associations with encryption enabled. This approach allows secure and authenticated unicast connections as well as unsecure multicast connections.

2.12.3.3.2 Multicast traffic connections (MTC) with encryption

2.12.3.3.2.1 MTC with encryption is the evolution of the solution proposed in the previous section aiming now to also support encrypted multicast and broadcast messages.

2.12.3.3.2.2 If the DL multicast connection is encrypted, it requires the use of a group security association (GSA) to maintain group key information. During the PKMv2 handshake, the GKEK is randomly generated once and distributed to the BSs via the ASN-GW (according to Profile C), and then transmitted to each MS encrypted with each corresponding KEK. The same GTEK is thus derived for all the MSs belonging to the multicast group and encrypted with the GKEK.

2.12.3.3.2.3 This option is required if the MBS services to be transported over multicast connections need to support confidentiality. This could be the case of some flight information services such as TIS-B, or future SWIM services, but no requirement currently exists.

2.12.3.3.2.4 This option would require the support of a “multicast traffic connection” item and “group multicast service SA” item, plus the development of corresponding test cases.

2.12.3.3.2.5 Functionality will need to be provisioned in the ASN-GW to distribute the group key GKEK to the BSs and also the GTEK context during the HO procedure in order to support the HO optimization item “Skip TEK establishment phase”.

2.12.3.3.3 Encrypted unicast and unencrypted multicast coexistence

According to the message exchange above, encrypted unicast messages and unencrypted multicast messages can coexist for a given AeroMACS session. Encrypted unicast messages will be transported over CID1 and CID2, while the unencrypted multicast messages will be transported over the shared connection CID3.

2.12.3.3.4 Unencrypted and encrypted multicast services coexistence

Once encrypted multicast is supported by AeroMACS, it can also coexist with both encrypted unicast messages and unencrypted multicast messages for a given AeroMACS session. Different CIDs/SFs with different SAIDs are to be used as depicted in Figure 54 below.

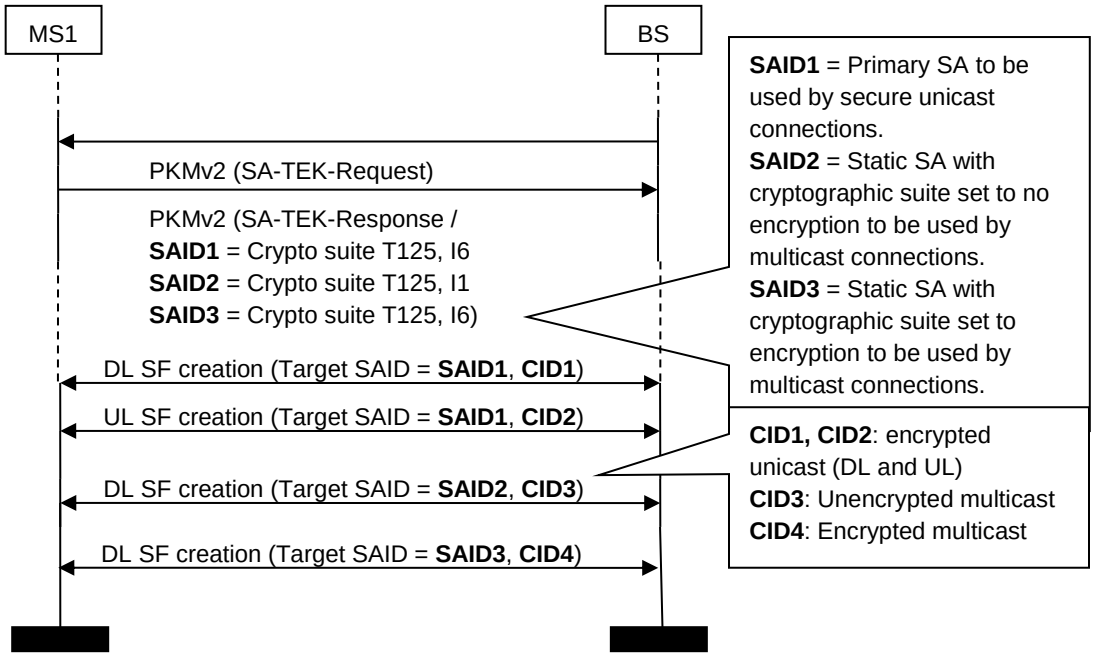


Figure 54. Encrypted multicast with other services either encrypted or unencrypted

2.13 PRIORITIZATION AND QUALITY OF SERVICE

2.13.1 Introduction

2.13.1.1 This section provides guidance material on how the AeroMACS system will support the desired quality of the service (QoS) for the various applications including prioritization of the applications.

2.13.1.2 The basic instrument in AeroMACS to support the required QoS by the applications is the use of service flows (SF) with appropriate QoS parameter configuration to comply with the application performance requirements on a per-service basis. This configuration leads to a priority and pre-emption based mechanism managed by the scheduler at the BS. This section proposes the methodology in which AeroMACS implementations will classify the upper layer application data into the MAC layer service flows (SF) in a worldwide interoperable way.

2.13.1.3 In addition, it provides guidance on how AeroMACS can support specific aeronautical requirements supporting specific ATC needs while maintaining the required QoS, and describes the proposed solution on how to map AeroMACS QoS and priority scheme to the ICAO ATN Priority Table 34.

2.13.1.4 AeroMACS supports static service flows which are created for the SS upon its entry into the AeroMACS network.

2.13.2 Quality of service (QoS) in AeroMACS

2.13.2.1 The AeroMACS QoS framework is based on the IEEE 802.16-2009 specifications. In summary, the IEEE 802.16-2009 systems are connection orientated at the MAC level and they assign the traffic that needs to be transmitted to a service flow (SF) which is mapped to a MAC connection using a connection ID (CID). The 802.16-2009 specifications support the desired QoS for the applications using the following mechanisms:

a) bandwidth allocation;

b) scheduling and classifiers (e.g. DSCP values, destination addresses, etc.); and

c) call admission control.

2.13.2.2 The bandwidth allocation scheme is performed during initialization and network entry. In this process, the BS assigns dedicated two management CIDs to each SS, named basic and primary, in order to provide the SS the ability to send and receive control messages.

2.13.2.3 In the IEEE 802.16 standard bandwidth requests are normally transmitted in two modes: a contention mode and a contention-free mode (polling). In the contention mode, the SS sends a contention based (CDMA) indication to receive an opportunity to send a bandwidth request. If the indication is received successfully by the BS, an opportunity will be given to the SS to send its request. If an opportunity is not given by the BS within the contention period, the SS resolves the contention by using an exponential back-off strategy. In the contention-free mode, the BS polls each SS, and an SS in reply sends its bandwidth request. The basic intention of unicast polling is to give the SS a contention-free opportunity to tell the BS that it needs bandwidth for one or more connections. In addition to polling individual SSs, the BS may issue a broadcast poll by allocating a request interval to the broadcast CID when there is insufficient bandwidth to poll the stations individually.

Note.— Ref. [14], paragraph 6.3.6.3.2, multicast and broadcast polling deals with the above.

2.13.2.4 The scheduler is the BS entity that manages the bandwidth allocation and transmission of queued MAC PDUs. Different scheduler classes use different bandwidth allocation schemes. Variable bandwidth assignment is possible in real-time polling service (rtPS), non-real-time polling service (nrtPS) and best effort (BE) services, whereas unsolicited grant service (UGS) service needs fixed and dedicated bandwidth assignment. The BS periodically in a fixed pattern offers bandwidth for UGS connections so UGS connections do not request bandwidth from the BS.

2.13.2.5 The scheduling algorithms provide mechanisms for bandwidth allocation and multiplexing at the packet level in IEEE 802.16-2009.

2.13.2.6 The classifiers are the entities which categorize the incoming IP packets to specific service flows by looking at desired fields of the packets and determining if the packet fits the required classification of a service flow. Each service flow will have one or more classifiers, with logical relations (AND/OR) between them. The classifiers allow the scheduler to provide QoS for service flows.

2.13.2.7 The call admission control (CAC) is the decision maker for incoming new services in the system. The admission controller implementation (and its performance) is vendor specific. When an MS sends a request to the BS with a certain QoS parameters for a new connection, the BS will check whether it

can provide the required QoS for that connection. If the request is accepted, the BS verifies whether the QoS of all the ongoing connections can be maintained. Based on this it will take a decision on whether to accept or reject the connection. The process described above is known as the CAC mechanism. The basic components in an admission controller are the performance estimator which is used to obtain the current state of the system and the resource allocator which uses this state to reallocate available radio resources.

2.13.2.8 Then the admission control decision is made to accept or reject an incoming connection. A connection is admitted if there is enough bandwidth to accommodate the new connection. The newly admitted connection will receive QoS guarantees in terms of both bandwidth and delay and the QoS of existing connections must be maintained. A more relaxed rule would be considered to limit an admission control decision (to reject) to applications with real-time hard constraints, for example, an airborne emergency call. For other requests, if there are insufficient resources, one can provide throughput less than requested by them.

2.13.2.9 A simple admission control decision can be exercised if there are enough available resources in the BS, then new connections are admitted else they will be rejected. However, a simple admission BS has to deal with both uplink and downlink traffic. Therefore, there are three different schedulers: two at the BS to schedule the packet transmission in a downlink and uplink subframe and another at the MS for uplink to apportion the assigned BW to its connections.

2.13.2.10 In order to indicate the allocation of transmission intervals in both uplink and downlink, in each frame the signalling messages UL-MAP and DL-MAP are broadcasted at the beginning of the downlink subframe. The scheduling decision for the downlink traffic is relatively simple as only the BS transmits during the downlink subframe and the queue information is located in the BS, while an uplink scheduler at the BS must synchronize its decision with all the SSs.

2.13.3 **Pre-emption in AeroMACS**

2.13.3.1 This section describes how pre-emption can be implemented in AeroMACS schedulers. Scheduler design and performance is a vendor implementation issue. AeroMACS supports pre-emption but whether pre-emption is used will depend on the operational requirement.

2.13.3.2 One example of an uplink scheduler is depicted in Figure 55 below. In this architecture, an extra queue stores a set of requests whose deadline is due to expire in the next frame.

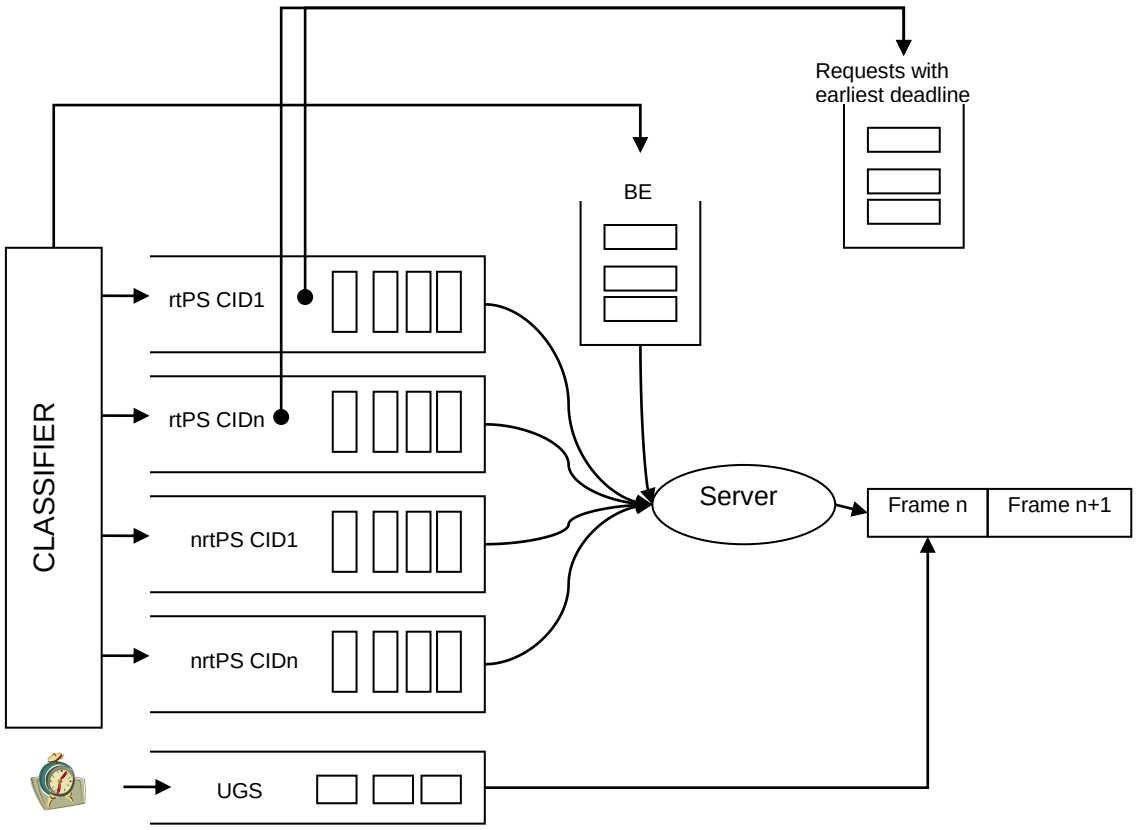


Figure 55. Uplink AeroMACS scheduler architecture example
[from "An integrated uplink scheduler in IEEE 802.16", Elmabruk 2008]

2.13.3.3 In a scheduling cycle, the scheduler will check if any request has been added to this extra queue. If so, the scheduler will then serve this queue after the UGS and polling queue. Once the extra queue becomes empty and there is available bandwidth in the UL_MAP, the scheduler will continue serving the PS list, using a round robin logic with priority for rtPS, followed by nrtPS. For BE, the remaining bandwidth will be assigned using an FIFO mechanism. A scheduler can decide to pre-empt a message to push another message with higher priority (e.g. short latency requirement) into the outbound frame.

2.13.4 Service flow management

2.13.4.1 Service flows (SFs) are the mechanism in AeroMACS to transport information. In the static service flow management approach supported in AeroMACS, they are created when MS enters the network and are destroyed when MS exits the network.

2.13.4.2 A service flow is characterized by a set of QoS parameters. A service flow is a unidirectional channel. AeroMACS data services however, require bidirectional channels as some are based on TCP (i.e. data+ack) transport protocol. Therefore, two SFs are normally needed for each exchange.

2.13.4.3 The classification rules map the higher level services to the corresponding SFs. The classification rules are loaded into the classifiers at both SS and BS when the SFs are created.

2.13.4.4 Table 32 shows the different classes of service (CoS) that are required in AeroMACS. In addition to the priority services, a DEFAULT class of data service is supported by all devices. Each of these data CoS requires different QoS parameters. The CoS are configured at the network side and provisioned to the base stations so that whenever a SS enters the network, the BS initiates the service flows with the identified CoS. For the six data services, twelve services flows (i.e. 6 CoS x 2 SFs) are required for a single aircraft. In addition up to three concurrent voice calls per aircraft need to be provisioned which results in six additional services flows being required to carry the three voice calls. The DEFAULT CoS maps to the best effort class of service. The DEFAULT service uses all remaining data capacity not utilized by other services.

Note.— The ASN GW uses the "class of service" and "device classes" to determine the service profile which is an implementation mechanism to signal the service flows from the ASN gateway to the base stations.

2.13.4.5 For each CoS in Table 30, the QoS parameters include: latency, minimum and maximum rate and priority as shown in Table 32. Some QoS parameter values, such as the maximum latency and the minimum reserved rate, are derived from the application QoS requirements.

2.13.4.6 It is highlighted that in the above context, traffic priority is only used to set priority between service flows with identical QoS parameters (like ATS1 and ATS2 in the example provided).

2.13.4.7 The maximum sustained traffic rate for high priority services can be determined by leaving a 5 per cent margin over the minimum reserved rate as a rule of thumb for peak or buffering transitions. This margin is pessimistic and can be reduced if further analysis finds that another value is more adequate.

2.13.4.8 Adequate bandwidth should be assigned to the best effort class as a whole because the majority of applications will default to this class. It is recommended to provide at least 25 per cent for best effort traffic.

2.13.4.9 The maximum sustained traffic rate for best effort services on the contrary cannot be determined from a single AeroMACS SS perspective. Calculations are required in order to determine the maximum sustained rate for the best effort services as described in the following paragraphs. The goal of this guidance is to show the methodology to determine the QoS parameter values to be configured in the service flows.

2.13.4.10 The first step is to quantify the bandwidth required by high priority services. Note that the figures in Table 31 have been extracted from the AeroMACS MASPS and figures for VoIP added. These are representative of AeroMACS performance requirements.

	Minimum reserved rate (from MASPS Table 44)		**Maximum sustained rate (5 per cent higher)**	
	DL (kbps)	**UL (kbps)**	**DL (kbps)**	**UL (kbps)**
VoIP1	64	64	N/A	N/A
VoIP2	48	48	N/A	N/A
VoIP3	32	32	N/A	N/A
NET	32	32	34	34
ATS1	32	32	34	34
ATS2	32	32	34	34
ATS3	32	32	34	34
AOC1	64	128	67	134
Total			347	414

Table 31. Bandwidth (kbps) required by high priority services

2.13.4.11 This design will support up to three simultaneous voice calls on one single AeroMACS mobile station. A "calling manager" may be required to know the current status (busy with another call or available) of each SF before placing a new call.

2.13.4.12 Then the available bandwidth per cell (i.e. the maximum sustained traffic rate QoS parameter value) can be derived from:

$$DL\ (Mbps) = 9.1 – (0.347 + 0.080) \times n$$

$$UL\ (Mbps) = 3.3 – (0.414 + 0.080) \times n$$

2.13.4.13 Where "n" is the number of concurrent AeroMACS SSs expected to be connected at the same cell sector and at the same time, that value depends on the airport size category in terms of operations/hour and the resulting cell planning.

2.13.4.14 For instance, in the case of an airport with three operations/hours, the value deemed for AOC 1 traffic on the RL according to the MASPS is 357.91 kbps for one aircraft on the ground which falls within the estimations done in this guidance: 3.3 - 0.414 = 2.916 Mbps. This value is much higher than the required data throughout 357.91 kbps.

2.13.4.15 According to these figures, another consequence is that one single cell can guarantee a sustained rate 357.91 kbps up to eight aircraft (i.e. (3.3 - 0.357)/0.414) for best effort services and at the same time meet the other QoS requirements for their high priority services.

2.13.4.16 In the case of an airport with twenty operations/hours, or higher, the number of sectors should be increased accordingly to handle the offered load. This guidance is to determine the QoS parameters per sector and is thus independent from the airport capacity requirements.

2.13.4.17 Table 32 summarizes the QoS parameters values which can be used in the service flows in order to meet AeroMACS QoS requirements for voice and data services. It should be noted that the DEFAULT best effort CoS supports routine communications for ANSPs, ATM service providers, airlines and airports.

2.13.4.18 The traffic priority is derived from the differentiated services code point (DSCP) value (and the corresponding PHB meaning, as shown in Table 35) provided by the upper layers. DSCP and per-hop behaviours (PHB) are contained in the IP header information passed through the IP convergence sublayer.

CoS	**Scheduling**	**QoS parameters values in the AeroMACS service flows**			
		Traffic priority	**Maximum sustained traffic rate (kbps)**	**Minimum reserved traffic rate (kbps)**	**Maximum latency (s)**
VoIP1	UGS	N/A	DL/UL: 64	64*	DL/UL: 0.150
VoIP2	UGS	N/A	DL/UL: 48	48	DL/UL: 0.150
VoIP3	UGS	N/A	DL/UL: 32	32	DL/UL: 0.150
NET	rtPS	N/A	DL/UL: 34	32	DL/UL: 1
ATS1	rtPS	1	DL/UL: 34	32	DL/UL: 1.5
ATS2	rtPS	2	DL/UL: 34	32	DL/UL: 1.5
ATS3	nrtPS	N/A	DL/UL: 34	32	N/A
AOC1	nrtPS	N/A	DL: 67 UL: 134	DL: 64 UL: 128	N/A
DEFAULT	BE	N/A	DL: 9 100 – 0.347 x A/C UL: 3 300 – 0.414 x A/C	N/A	N/A

*: depending on the VoIP CODECS used.

Table 32. QoS parameters values in AeroMACS (based on MASPS)

Note.— For the UGS service flow, the grant interval also needs to be specified. For VOIP, the typical value is 50msec. For the nrtPS and rtPS service flows, the Polling Interval also needs to be specified. A typical value for nrtPS is 1 sec and for rtPS it is 20 msec.

2.13.4.18 In Table 32 above, the maximum latency values refer to end-to-end application layer delay and are extracted from the draft AeroMACS MASPS. These values could become more stringent if necessary to keep the underlying requirement of one-way delay of 20 to 80 ms at MAC layer as indicated in section 7.1 in the AeroMACS MASPS. It is noted again that the traffic priority field resolves potential competition between service flows with identical QoS parameters set.

2.13.4.19 The scheme described above allows for evolution and can support new classes of service to be added to support new types of applications. In order to achieve this, new service flows (for the new CoSs) will need to be configured in the AeroMACS ASN as the AeroMACS QoS requirements may change over

time or more granularity is required in the definition of class of services. In such a case, the maximum number of active services flows supported by the SS and the ASN should be considered as an upper limit. The IEEE 802.16 Standard does not set such a limit however, this may be set by manufacturers.

2.13.4.20 As an example, the following Table 32 shows how two new (APT1 and APT2) best effort type CoSs can be added to the list of supported CoSs.

CoS	Scheduling	QoS parameters values in the AeroMACS service flows			
		Traffic priority	**Maximum sustained traffic rate (kbps)**	**Minimum reserved traffic rate (kbps)**	**Maximum latency (s)**
APT1	BE	1	DL: 1 000	N/A	N/A
APT2	BE	2	DL: (8 100 – 0.347 x A/C)/2 UL: (3 300 – 0.414 x A/C)/2	N/A	N/A
DEFAULT	BE	N/A	DL: (8 100 – 0.347 x A/C)/2 UL: (3 300 – 0.414 x A/C)/2	N/A	N/A

Table 33. QoS parameters values in AeroMACS providing APT support

2.13.4.21 For better management of the number of SFs to be activated for each SS, it is possible to define device classes that will implement only some CoSs. For example voice only devices would only use two or more SFs (DL and UL) with just the voice CoS. Similarly, video streaming only devices (such as security cameras) would only use one SF (DL).

2.13.4.22 The QoS policy provisioning between AAA and ASN is described in the WiMAX forum NWG specification and can be extended to support the device classes provisioning.

2.13.4.23 In summary, the service flow management (SFM) is a logical entity in the ASN. The SFM entity is responsible for the creation, admission, activation, modification and deletion of service flows.

2.13.4.24 Similarly, the service flow authorization (SFA) is also a logical entity in the ASN. The SFA is responsible for evaluating any service request against the user's QoS profile (i.e. device class). The AAA server holds the user's QoS profile and associated policy rules. These are transferred to the SFA at network entry as part of the authentication and authorization procedure.

2.13.4.25 SFA/SFM entities can provide the capability to provision specific SFs per device classes depending on the SFA policies. In addition, there is support for evolution of requirements and introduction of new device classes as the requirement to create new service flows in the future (for instance to transport video HD), resides in the AAA server. Therefore, legacy SSs do not need to implement anything new as they will ignore the new service flows and continue using the previous service flows.

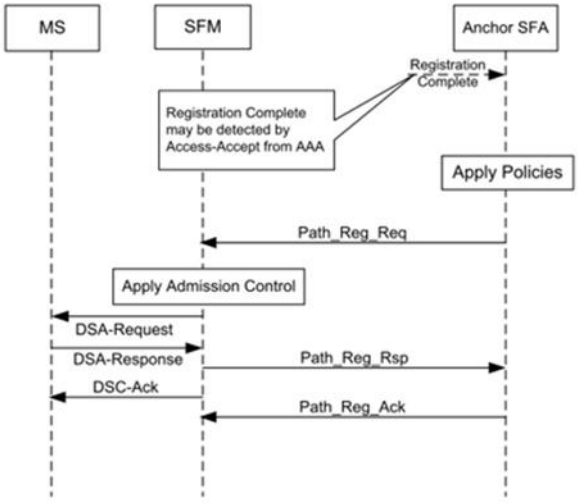


Figure 56. Service flow authorization at network entry

2.13.5 Mapping of AeroMACS priority levels to ICAO ATN priority levels

In order to support the QoS service requirements for the ATC and AOC services, a priority classification per message category is defined by ICAO and mapped to the supported ATN mobile subnetworks in Table 34 of Annex 10, Volume III. Considering the ATS and AOC classes of service as defined in the previous sections, the following Table 33 provides a mapping of the AeroMACS services to the ATN network layer priority levels.

Message categories	ATN network layer priority	Corresponding mobile subnetwork priority
		AeroMACS
Network/systems management	14	NET
Distress communications	13	ATS1
Urgent communications	12	ATS1
High priority flight safety messages	11	ATS1
Normal priority flight safety messages	10	ATS2
Meteorological communications	9	ATS3
Flight regularity communications	8	AOC1 or DEFAULT
Aeronautical information service messages	7	ATS3
Network/systems administration	6	ATS3
Aeronautical administrative messages	5	Not allowed
<unassigned>	4	<unassigned>
Urgent priority administrative and U.N. Charter communications	3	Not allowed
High priority administrative and State/government communications	2	Not allowed
Normal priority administrative communications	1	Not allowed
Low priority administrative communications and aeronautical passenger communications	0	Not allowed

Table 34. Mapping of AeroMACS priority levels to ATN priority levels

Note.— The information in the third column of this table is equivalent to the columns defined in Table 3-3 of Annex 10, Volume III, for the other mobile subnetworks.

2.13.6 Quality of service in internet protocol (IP QoS)

2.13.6.1 *Overview*

2.13.6.1.1 The aeronautical network comprises multiple autonomous networks managed by different administrative domains and interconnected to each other to form the global internet. In this scenario, the end–to-end quality of service (QoS) can only be achieved by defining a common set of rules for packet handling that could be applied uniformly across various networks.

2.13.6.1.2 IETF defines two methods of QoS handling for packets in the internet (IP QoS) namely, integrated service (IntServ) and differentiated service (DiffServ).

2.13.6.1.3 Differentiated service is based on a prioritized traffic model in which the application packets are marked for various QoS handling and the network prioritizes them as per the predefined set of rules. Diffserv model defines per hop behaviours (PHB) for various QOS categories and the routers and switches in the network implement packet handling algorithms as per the PHB definitions.

2.13.6.1.4 The DiffServ model is specified for IPS in the *Manual for the ATN using IPS Standards and Protocols* (Doc 9896), hence it is used for AeroMACS.

2.13.6.2 *DiffServ model*

2.13.6.2.1 In DiffServ specifications an 8-bit differentiated service field (DS Field) is defined in the IP header for packet marking and classification purposes. Initial 6-bits of DS field represent DSCP that defines the class of service, or in other words called PHB, required for the packet in the network. The next two bits are used for explicit congestion notification (ECN) which is outside the scope of DiffSev.

2.13.6.2.2 As the DSCP definitions are common between IPv4 and IPv6 networks, the packets are expected to receive the same kind of QOS treatment in the DiffServ network irrespective of the network layer protocol (IPv4 or IPv6).

2.13.6.2.3 DiffServ defines three categories of PHBs namely, expedited forwarding (EF), assured forwarding (AF) and default (DF) forwarding as shown in Figure-57.

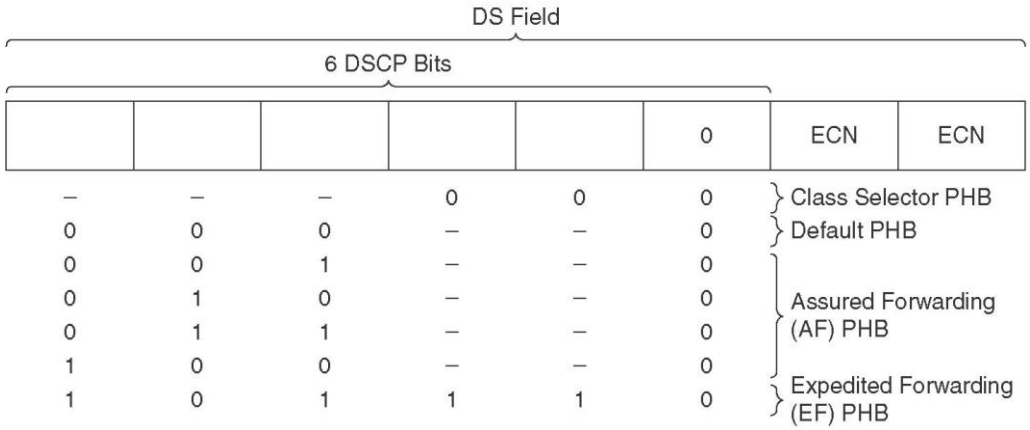


Figure 57. DS field

2.13.6.2.4 Expedited forwarding (EF) is dedicated to low loss, low delay traffic. Generally, EF is used for voice applications. EF specifications are defined in RFC 3246.

2.13.6.2.5 Assured forwarding (AF) allows the operator to provide assurance of delivery as long as the traffic does not exceed some subscribed rate. The traffic exceeding the allowed data rate is likely to be

dropped in case of congestion. Diffserv defines four AF class groups where all items in the group have the same priority. These groups are numbered sequentially, such that class group AF4x takes precedence over AF3x, which takes precedence over AF2x, which takes precedence over AF1x. Within each class group, packets are given drop precedence as high, medium or low, where higher precedence means more dropping. The combination of classes and drop precedence yields twelve separate DSCP encodings from AF11 through AF43 (see Table 35).

Assured Forwarding (AF) Behavior Group				
	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Med Drop	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
High Drop	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

Table 35. Available DCSP encoding

2.13.6.2.6 AF classes are independent of each other and benefit individual guaranteed bandwidth. This prevents one critical application to take all the available bandwidth and block other critical applications. AF is defined in RFC 2597 and updated in RFC 3260.

2.13.6.2.7 Default forwarding (DF) is a best effort class which would be used for non-mission critical, non-delay sensitive applications.

2.13.6.3 *Traffic handling in network*

2.13.6.3.1 Applications decide the DSCP settings based on their requirements and set the DSCP values in the IP header. Most TCP/IP implementations provide mechanisms (example: socket options) for setting IP header values.

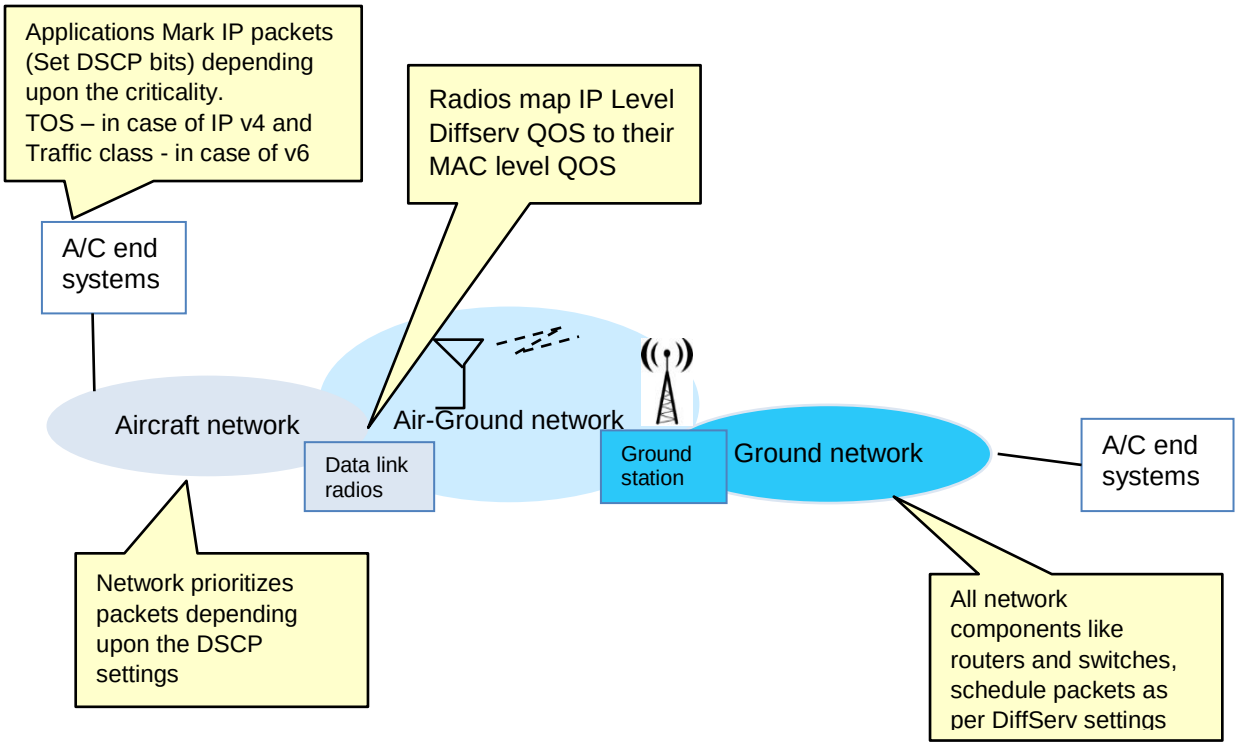


Figure 58. Traffic handling in network

2.13.6.3.2 Routers, switches or any other intermediate modules in the network handle packets as per PHB definitions. Based on the DSCP settings, the packets are classified; priority is applied and scheduled for further transmission in the network. The packets may traverse through a series of networks, but, since, at every network node, the packets are handled as per the PHBs set by the applications, end-to-end QoS is achieved in the entire network.

2.13.6.3.3 Another aspect to be considered in the overall network design is to implement the required QoS at MAC/lower layers also in line with IP QoS requirements. In most cases, Layer 2 systems have their own QoS definitions which may be different from IP QoS definitions, as Layer 2 systems handle packets from multiple network layer (Layer 3) systems. For example, the definitions of AeroMACS service types are different from IP QoS definitions. Hence, it becomes necessary to map IP QoS definitions with AeroMACS service classes to achieve end-to-end QoS performances.

2.13.6.4 *Mapping IP QoS with AeroMACS service flows*

Various applications and their classes of service are identified in the earlier sections.

CoS	Scheduling	PHB Meaning	DSCP value
VoIP1	ertPS	EF	101110
VoIP2	ertPS	EF	101110
VoIP3	ertPS	EF	101110
NET	rtPS	AF41	100010
ATS1	rtPS	AF42	100100
ATS2	rtPS	AF32	11100
ATS3	nrtPS	AF12	1100
AOC1	nrtPS	AF11	1010
DEFAULT	BE	CS0 Default	0
APT1	BE	CS0 Default	0
APT2	BE	CS0 Default	0
Emergency Video	rtPS	AF23	10110

AeroMACS supports classification rules based on DSCP

AF4X , AF21, AF22, AF12 are reserved for future traffic categories

Table 36. Class of service, scheduled and DSCP value

2.13.6.5 *Device classes*

2.13.6.5.1 Overview

2.13.6.5.1.1 The AeroMACS network is expected to support a variety of deployments at airports including mobile/fixed terminals, safety/non-safety equipment, real-time/non-real-time applications, etc. Hence, depending upon deployment requirements, device configurations of SS such as, types of services to be provisioned, number of connections and data rates would differ on a case-by-case basis. Hence, there is a need to define device classes identifying mandatory requirements for each deployment.

2.13.6.5.1.2 AeroMACS supports the following device classes:

a) aircraft - represents modems installed in aircraft. Considering both safety and non-safety applications all identified types of service flows are recommended for aircraft;

b) surface vehicle – represents devices hosted on all ground support vehicles including passenger vans/buses, dollies carrying cargo, refuel trucks, catering vehicles and Push back tugs/ tractors, etc.;

c) fixed safety equipment – represents fixed devices used to monitor/control ground equipment that are deployed for critical ATS services. Example: radars, landing systems, runway lighting controls, etc.; and

d) ground default – all other ground fixed or nomadic equipment supporting the safety and regularity of flight operations.

2.13.6.5.2 Identification of devices

2.13.6.5.2.1 During logon, as part of the authentication process, the digital certificate of a device is exchanged with the network. AeroMACS specifications, (as explained in Chapter 3) have defined certificate profiles for devices and service providers.

2.13.6.5.2.2 The device type field will be used to indicate the device class information along with its Id as shown below:

tbsCertificate.subject : <Device Type> < Device Id>

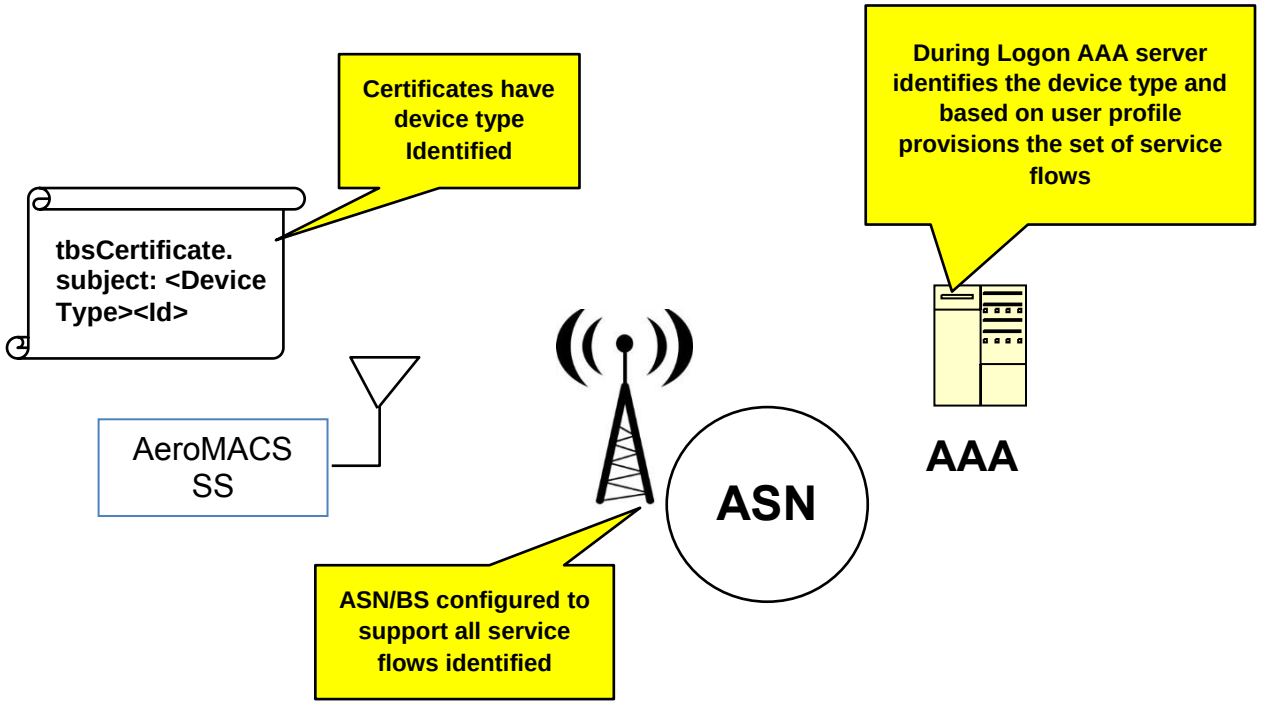


Figure 59. Device identification

a) CA creates a certificate for the device and signs it;

b) during the logon procedure, the device exchanges the certificate with the AeroMACS network;

c) the AAA server validates device certificate and identifies its device class; and

d) the AAA server transfers the device profile to the ASN gateway for service flow creation.

2.14 SUBNETWORK ENTRY AND HANDOVER

2.14.1 Overview

2.14.1.1 Subnetwork entry and handover both depend on two processes:

a) scanning; and

b) ranging.

2.14.1.2 Each of these is performed slightly differently depending on whether the AeroMACS SS is performing the initial network acquisition or a handover between BSs. These processes are described in the following paragraphs which are then followed by a detailed explanation on network entry and handover.

2.14.1.3 Scanning is the process by which the SS acquires a channel among the reachable BS upon initial network entry or handover.

2.14.1.3.1 During initial network entry, the SS listens for channels from potentially all reachable BSs and proceeds to synchronization.

2.14.1.3.2 In a different manner, scanning for the objective of performing handover occurs before the handover is triggered. While the SS is being serviced by the service BS, it periodically receives information (via MOB_NBR-ADV message) about neighbouring BSs it can potentially hand over to. When SS triggers scanning (when the scanning threshold is surpassed), it makes a request (via MOB_SCN-REQ) to avoid both uplink and downlink data transfer during scanning intervals in order to perform scanning. During this scanning phase, the SS listens selectively only to the BSs it has received information about. The service BS can thus prohibit handover to specific neighbour BSs if configured to do so.

2.14.1.4 Ranging is the process by which the SS, after having acquired a channel and information on the channel parameters (by reception of DCD/UCD), adapts its time offsets and power adjustments to be aligned with the BS.

2.14.1.4.1 In initial network entry, the SS transmits a randomly generated initial CDMA ranging code in a ranging region as announced by the UL-MAP. If the BS receives it and decodes it successfully, it responds with an RNG-RSP to correct time and power. The SS will send subsequent ranging codes until it obtains a success RNG-RSP and sets up basic CID. In the next frame, the SS will send a new RNG-REQ message in the basic CID and will continue the network entry process.

2.14.1.4.2 When a handover is triggered (when the handover threshold is surpassed), the SS already has acquired the channel information of the target BS. The SS transmits a randomly generated HO CDMA ranging code in a ranging region as announced by the UL-MAP. The rest of the procedure is similar to the initial ranging process.

2.14.1.4.3 There is the option to use fast ranging to expedite the handover ranging process where the serving BS allocating resources has previously negotiated with the target BS a non-contention allocation. In this case, the target BS announces a fast ranging allocation in the UL-MAP for the specific SS, which will transmit the RNG-REQ directly and thus does not need to transmit HO CDMA ranging codes in contention mode.

2.14.2 Subnetwork entry

2.14.2.1 This section describes the process by which AeroMACS scans and establishes a communications channel with a BS, to enter an AeroMACS network. Figure 60 defines the subnetwork entry and initialization process.

2.14.2.2 The starting point, as defined in IEEE 802.16-2009, begins when an SS starts scanning for a channel.

2.14.2.3 The end point of the subnetwork entry time is when the SS receives a DSA-ACK message, which means that a subnetwork link has been established. Following receipt of a DSA-ACK message, an SS is able to send data to a network.

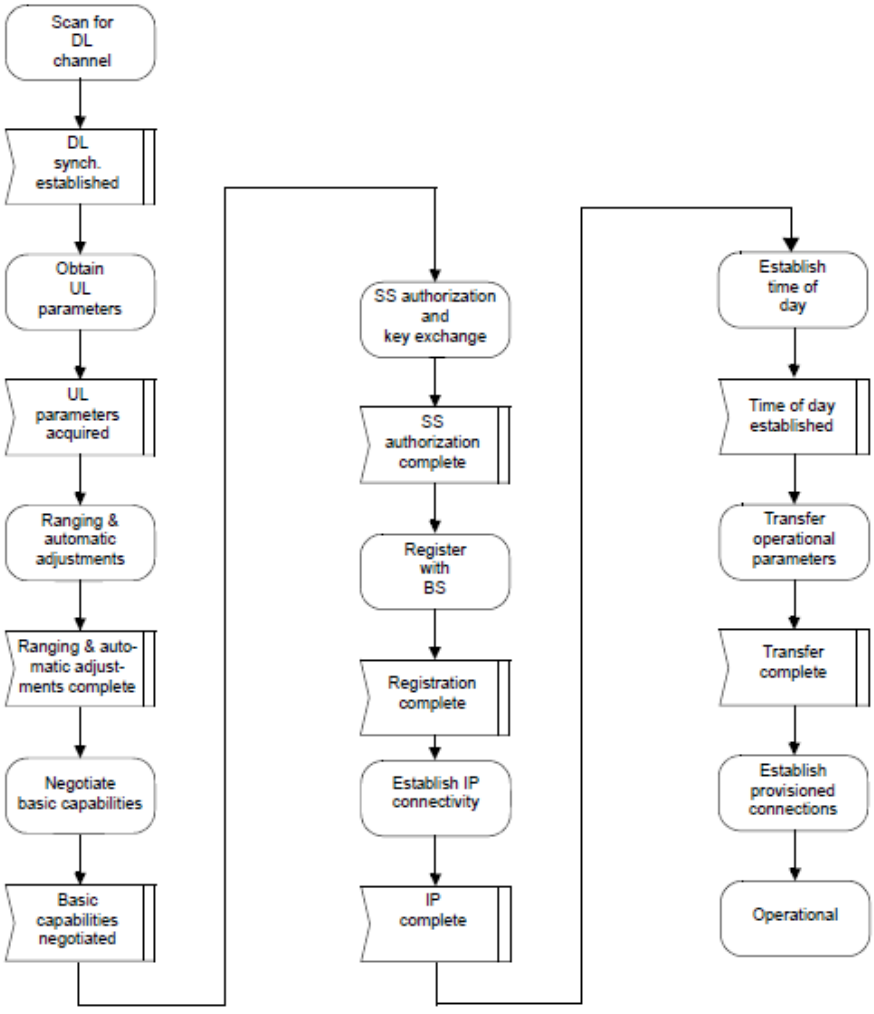


Figure 60. Initialization overview flowchart referenced by IEEE 802.16-2009

2.14.2.4 As a number of factors contribute to the time, it is useful to divide the subnetwork entry time into two components; subnetwork entry time T1 and subnetwork entry time T2.

The subnetwork entry time = subnetwork entry time T1 + subnetwork entry time T2:

a) subnetwork entry time T1 (scanning time); mainly depends on the SS implementation; and

b) subnetwork entry time T2 (ranging, authentication and registration time); mainly depends on the RF environment between the SS and BS.

1) Subnetwork entry time T1:

The subnetwork entry time T1 should be defined as following procedure.

(1) SS starts scanning the BS transmitted frequency.

Scanning frequency band should be defined. Scanning method of SS is an implementation issue.

(2) SS selects the best frequency for synchronizing

(3) SS synchronizes to BS frame

(4) SS sends initial ranging code (This initiates T2)

The starting point should be considered to be the starting point of subnetwork entry time,

This entry time depends on the condition of scanning frequency bandwidth and also depends on the SS implementation issue for scanning and selecting the best channel.

2) Subnetwork entry time T2:

For subnetwork entry time T2, the starting point and end point are defined as follows.

As is shown in Figure 62, the starting point is when the SS sends an initial ranging code. The end point is when the MS receives the DSA-ACK message.

Unlike subnetwork entry time T1, subnetwork entry time T2 does not depend on the frequency bandwidth. However, it is dependent on the RF environment. If the radio environment is noisy and an adequate S/N ratio cannot be achieved, the sequence may not proceed as shown if frames need to be resent. Given this, a sequence diagram is given showing the exchanges taking place during T2.

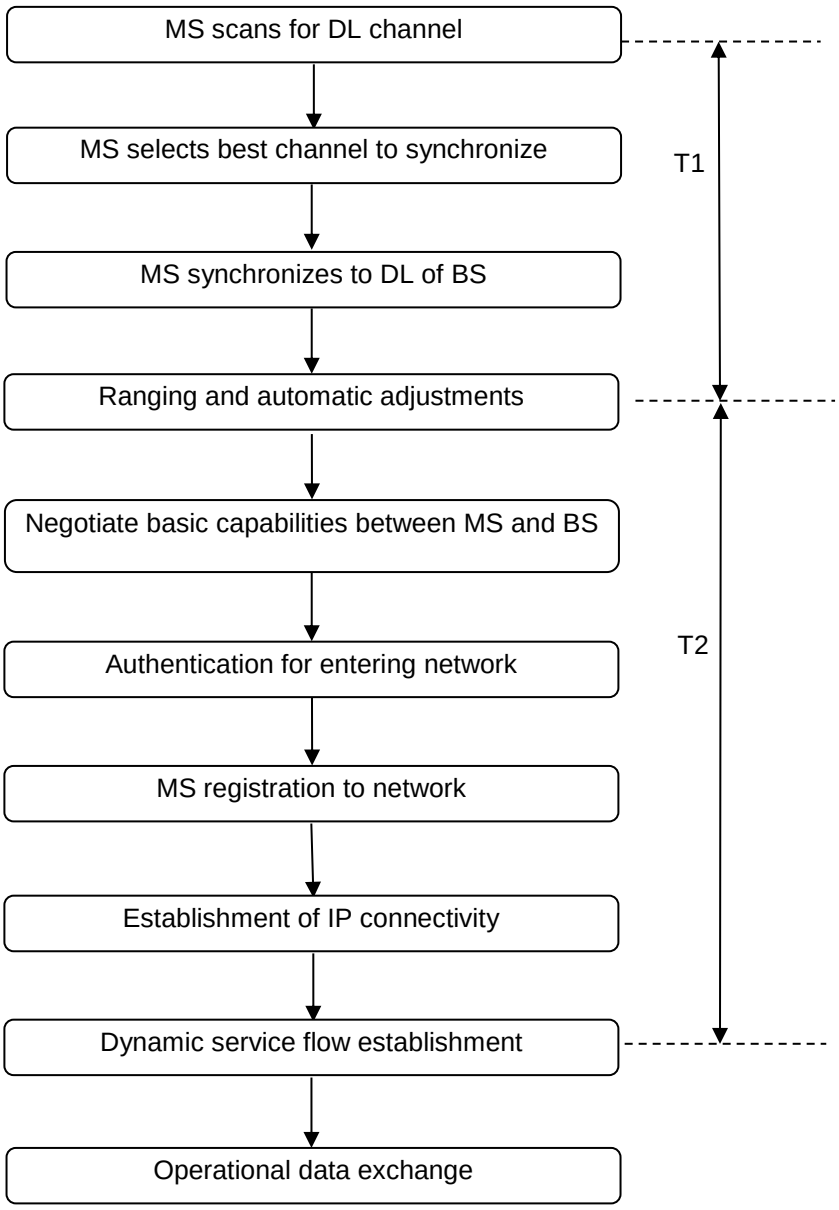


Figure 61. Sequence of T1 and T2 for total subnetwork entry time

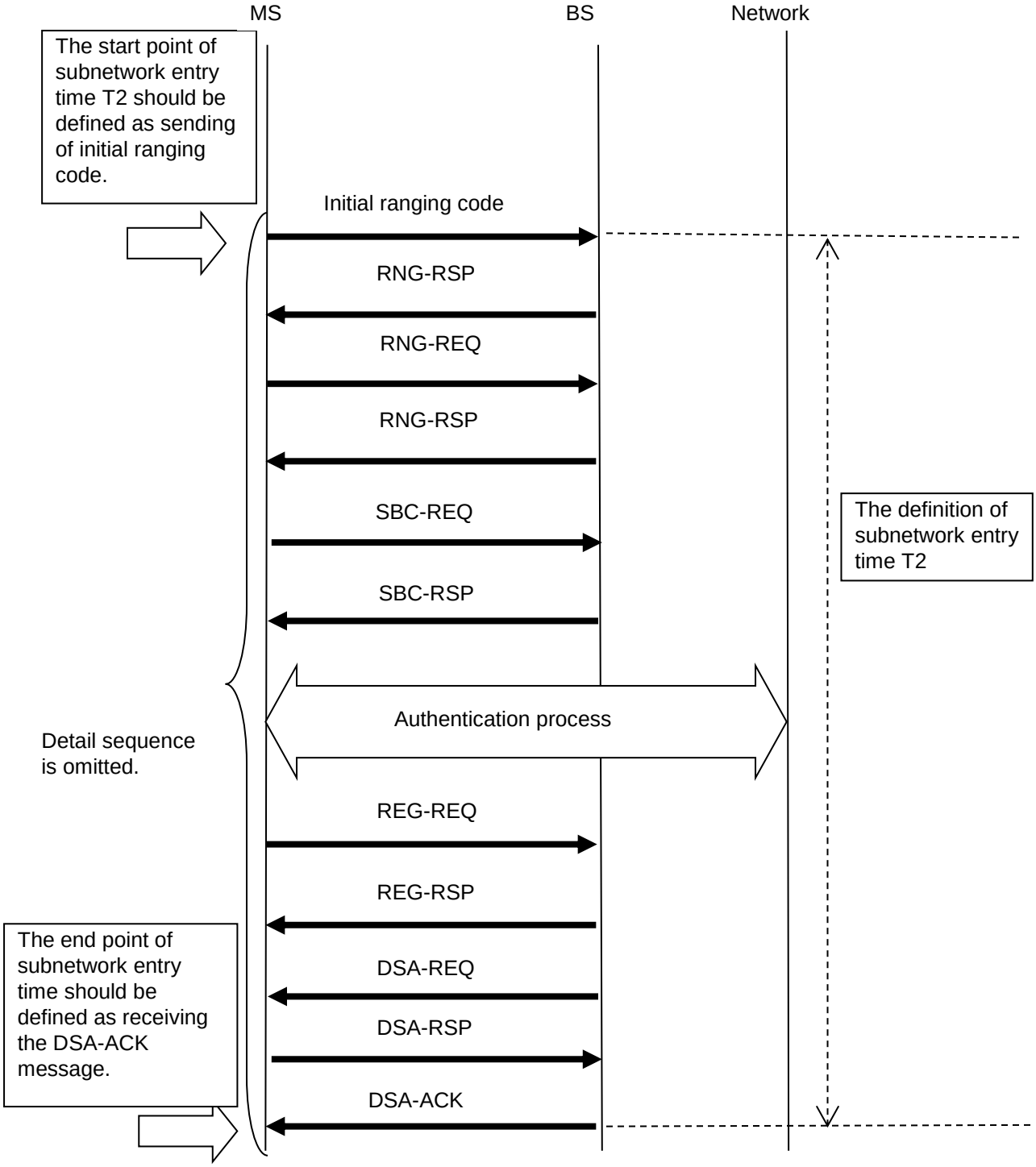


Figure 62. Detailed sequence of the subnetwork entry time T2

2.14.3 **Handover**

2.14.3.1 *Introduction*

2.14.3.1.1 This section describes the AeroMACS handover procedures and explains how the handover is done in AeroMACS systems including some practical aspects to consider in a real deployment.

2.14.3.1.2 In relation to handover, the AeroMACS Standard defines two relevant handover mechanisms:

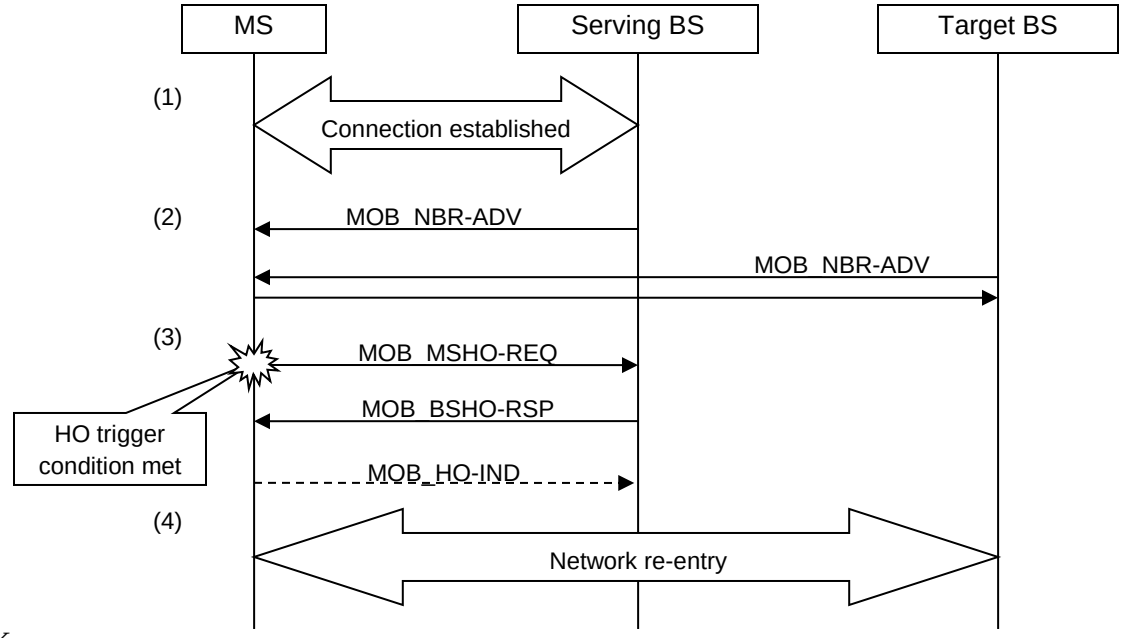
a) MS initiated handover; and

b) MS initiated handover with scanning.

2.14.3.1.3 The AeroMACS MOPS and profile require that all AeroMACS systems support MS initiated handover mechanisms and these two mechanisms are described in sections 2.14.3.2 and 2.14.3.3. In terms of which of the two mechanism to use (with or without scanning), this is a design option as explained below.

2.14.3.2 *MS initiated handover*

2.14.3.2.1 MS initiated handover is the simplest AeroMACS handover process where the MS chooses the candidate target BS based on its serving BS neighbour advertisement information and not on the actual channel conditions. The following diagram describes the MS initiated handover and exchanges that take place between the MS and the two BSs involved (serving and target).



Key:

MOB NBR-ADV: Neighbour advertisement
MOB MSHO-REQ: Mobile station handover request
MOB BSHO-RSP: Mobile station handover response
MOB HO-IND: Mobile handover indication

Figure 63. MS initiated handover

2.14.3.2.2 The different exchanges in the MS initiated handover are described below:

a) successful completion of initial network entry and service flow establishment;

b) acquiring network topology - neighbour advertisement:

1) the serving BS and the target BS send MOB_NBR-ADV. An AeroMACS BS broadcasts information about the network topology using the MOB_NBR_ADV message, which is an AeroMACS Layer 2 management message. This message provides channel information about neighbouring BSs;

c) the serving BS sends neighbour trigger TLV in MOB_NBR-ADV handover decision:

1) when the trigger conditions are met, the MS sends one or more MOB_MSHO-REQ to the serving BS;

2) the serving BS sends MOB_BSHO-RSP;

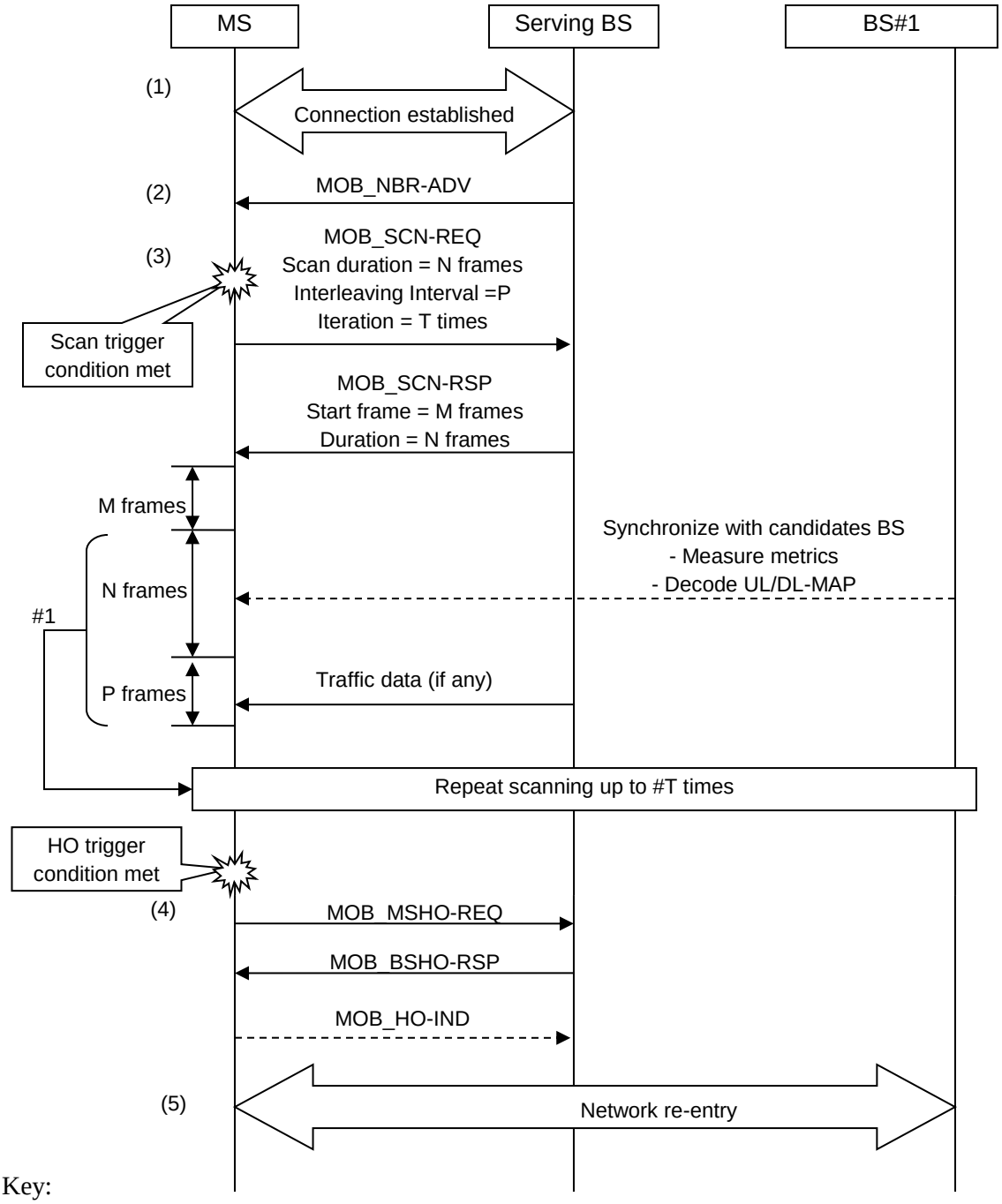
3) the MS optionally sends MOB_HO-IND to the serving BS with final indication that it is about to perform a HO; and

d) handover initiation.

Note.— TLV: type, length, value – a tag added to each transmitted parameter containing the parameter type, the length of the encoded parameter and the value.

2.14.3.3 *MS initiated handover with scanning*

2.14.3.3.1 In the MS initiated handover with scanning process, the MS uses its serving BS neighbour advertisement, not to initiate the handover itself, but to initiate the scanning for the candidate BSs thus determining the actual channel conditions before performing the handover action. This process however increases the handover latency. The following diagram describes the MS initiated handover with scanning and exchanges that take place between the MS and the BSs involved (serving BS and BS#1).



Key:
MOB NBR-ADV: Neighbour advertisement
MOB SCN-REQ: Mobile scanning request
MOB SCN-RSP: Mobile scanning response
MOB MSHO-REQ: Mobile station handover request
MOB BSHO-RSP: Mobile station handover response
MOB HO-IND: Mobile handover indication

Figure 64. MS initiated handover with scanning

2.14.3.3.2 The different exchanges in the MS initiated handover with scanning are described below:

a) successful completion of initial network entry and service flow establishment;

b) acquiring network topology - neighbour advertisement:

1) the serving BS sends MOB_NBR-ADV;

2) the serving BS sends scanning trigger. The serving BS sends UL interference and noise level estimated in BS using noise plus interference IE in DL-MAP.

c) acquiring network topology - scanning initiation:

1) when the scan trigger condition is met, the MS sends one or more MOB_SCN-REQ indicating preferred scanning parameters. This message includes the scanning values for scan duration (N), interleaving interval (P) and iterations (T);

2) the serving BS sends MOB_SCN-RSP with scanning parameters. This message includes the scanning values for start frames (M) and confirms duration (N); and

3) the MS scans neighbour BSs during scan interval as defined in MOB_SCN-RSP;

d) handover decision:

1) when the handover trigger condition is met, the MS sends MOB_MSHO-REQ indicating the Target BS;

1) the serving BS sends MOB_BSHO-RSP with action time > 0 indicating fast ranging IE is used in Target BS; and

2) the MS sends MOB_HO-IND to the serving BS effecting BS release; and

e) handover initiation.

2.14.3.3.3 The information of neighbour BSs in the MOB_NBR-ADV may include: preamble index, least significant 24 bits of BSID, frequency assignment, BS EIRP, DCD/UCD configuration change count, scheduling service supported and HO process optimization.

2.14.3.3.4 However, should the MS choose the BS candidate based on this information, the MS may not select the more suitable BS. The MS does not know at this point the actual channel conditions to the candidates BS. Based on MOB_NBR-ADV, the MS only knows that the surrounding BSs exist and how to synchronize with them, but nothing else.

2.14.3.3.5 By sending MOB_SCN-REQ, the MS uses this neighbour list, not to initiate the handover itself, but to initiate the scanning of the candidate BSs. By scanning, the MS learns the actual channel conditions and then selects the more suitable BS to perform the handover. The cost is that this scanning procedure takes some time (in terms of number of frames) thus increasing the handover total latency.

2.14.3.3.6 This additional latency due to scanning depends on the number of neighbour BSs the MS is granted to scan by the serving BS. In AeroMACS, where not many BS are expected to be deployed, this latency may not be very long (only an interval of a few frames).

2.14.3.3.7 Scanning will enable AeroMACS MSs to perform reliable handovers. Additionally, as only a few BSs will be present in AeroMACS, the latency introduced by scanning should not be high.

Note.— The duration and frequency of the alternating periods of scanning and normal operations could affect the network performance and provided QoS. A long scanning period increases the packets' jitter and the end-to-end latency because while the MS is scanning, the BS sees it as "sleeping" and will buffer its packets until the scanning is done. Contrarily, a short scanning period requires multiple iterations and increases the overall scanning duration. In general, longer scanning periods may lead to worse QoS operations (higher delay jitter) but better handover performance (solid connectivity for delay and bandwidth sensitive services). An example of the efforts of N, P and T values in latency and jitter is given in Table 37.

2.14.3.3.8 If scanning is not desired, the BS can be configured to send MOB_NBR-ADV with neighbour trigger TLV with action set to "respond on trigger with MOB_MSHO-REQ".

Parameter	**Light scanning**	**Dense scanning**
Scan duration (N)	4 frames	20 frames
Interleaving interval (P)	350 frames	140 frames
Iterations (T)	10 frames	10 frames
Performance		
Latency	48 ms	60 ms
Jitter	22 ms	33 ms

Table 37. An example of N, P and T parameter values and resulting latency and jitter performance

2.14.3.4 *HO ranging*

2.14.3.4.1 HO ranging is not an additional HO procedure but it is performed typically in the case of a HO failure and it allows a quick link recovery. In this case, instead of the MS sending a MOB-MSHO-REQ at the serving BS, the MS directly moves to the target BS and performs handover ranging to re-enter the network.

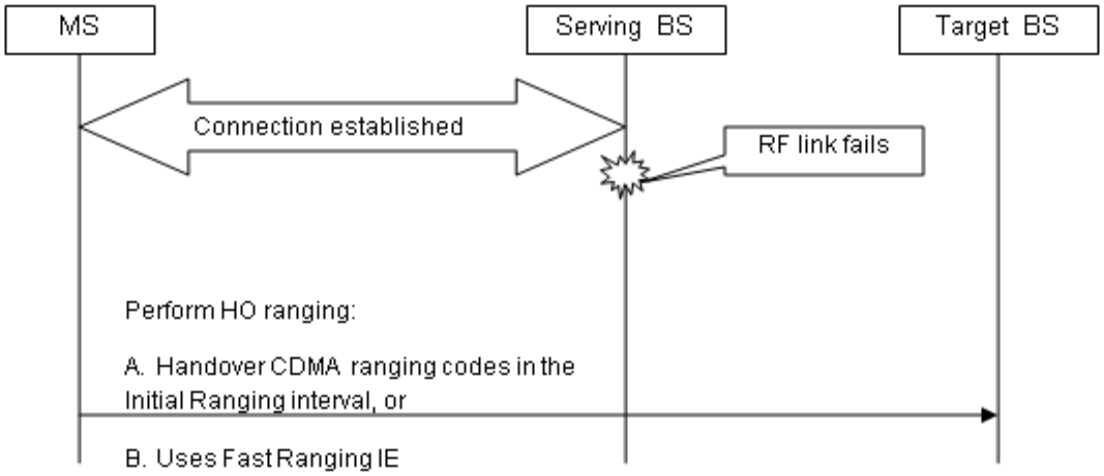


Figure 65. HO ranging

2.14.3.4.2 In this scenario the MS is aware of the BS to choose based on the information learnt from the serving BS MOB_NBR-ADV messages. This is an implementation option and as far as the delay and availability of the data path to the MS complies with the requirements, it can be up to the MS internal algorithm to pick a BS based on parameters such as channel quality, and available capacity.

2.14.3.4.3 There are two ways to perform HO ranging:

a) handover CDMA ranging codes in the initial ranging interval (described in 6.3.21.2.6 of IEEE 802.16-2009 Standard); and

b) use fast ranging IE (described in 6.2.21.2.4 of IEEE 802.16-2009 standard). MS can receive the fast_ranging_IE in the UL-MAP to allocate a non-contention-based initial ranging opportunity and can transmit an RNG-REQ code to the target BS without access collision.

2.14.3.4.4 The AeroMACS profile supports both options A and B to perform HO ranging.

2.14.3.5 *Practicalities for understanding of HO in AeroMACS*

2.14.3.5.1 The two handover procedures allowed in AeroMACS are both initiated by the MS. Overall, the use of MS initiated handover with or without scanning is a design option. MS initiated handover relies on MOB_NBR-ADV accuracy, while MS initiated handover with scanning provides a way for the MS to make sure the channel conditions are good, at the expense of introducing an additional delay.

2.14.3.5.2 For the scanning case, once the metric trigger happens, the MS initiates HO to the target BS. The point of having already received the MOB_NBR-ADV information is that the MS knows already all it needs to associate to the target BS.

2.14.3.5.3 With the scanning case, once the metric trigger happens, starting from the start frame specified by the serving BS, the MS only synchronizes to the candidate BSs (for monitoring signal quality and UL/DL-MAPs) while it remains associated to the serving BS. This happens during the scanning intervals as granted by the serving BS.

2.14.3.5.4 During the scanning interval the MS does not exchange data with the serving BS as the MS radio is busy performing the scanning. However, the serving BS is allowed to pre-set a certain buffer space to store downlink service data when an MS performs scanning.

2.14.3.5.5 The benefit of using the option with scanning is that it provides a more reliable handover procedure (i.e. lower probability of HO failure), in exchange for a higher latency, which would be in the order of a few frames (one frame being 5 ms).

2.14.3.5.6 The serving BS obtains the neighbouring BS information from the ASN-GW over the R6 interface.

2.15 UPPER LAYER INTERFACES

2.15.1 Convergence sublayer

The convergence sublayer (CS) interfaces with higher layers to accept packets from higher layers and to transfer them to the MAC common part sublayer (MAC CPS) for further processing. This layer is also responsible for categorizing the packets as per packet classification rules, mapping them to the associated service flows and scheduling them for transmission over the MAC layer based on the quality of service (QoS). CS performs packet header suppression. AeroMACS supports packet convergence sublayer (packet CS), including both ethernet specific and IP specific parts. AeroMACS does not support asynchronous transfer mode convergence sublayer (ATM CS) and generic packet convergence sublayer (GPCS). AeroMACS only supports IP-CS and optionally ethernet CS.

2.15.1.1 *Packet classification*

2.15.1.1.1 AeroMACS has a provision to specify packet classification rules so that the incoming traffic can be divided into multiple data streams. Associated with the classification rule, the type of service flow, the QoS policies and the packet header suppression policies can also be specified for each data stream. The packet classification rules are defined based on some of the packet header parameters such as, UDP port numbers, IP addresses (source or destination) or by a combination of multiple parameters. Based on the classification, individual service flows are created and the packets are scheduled accordingly as shown in Figure 66.

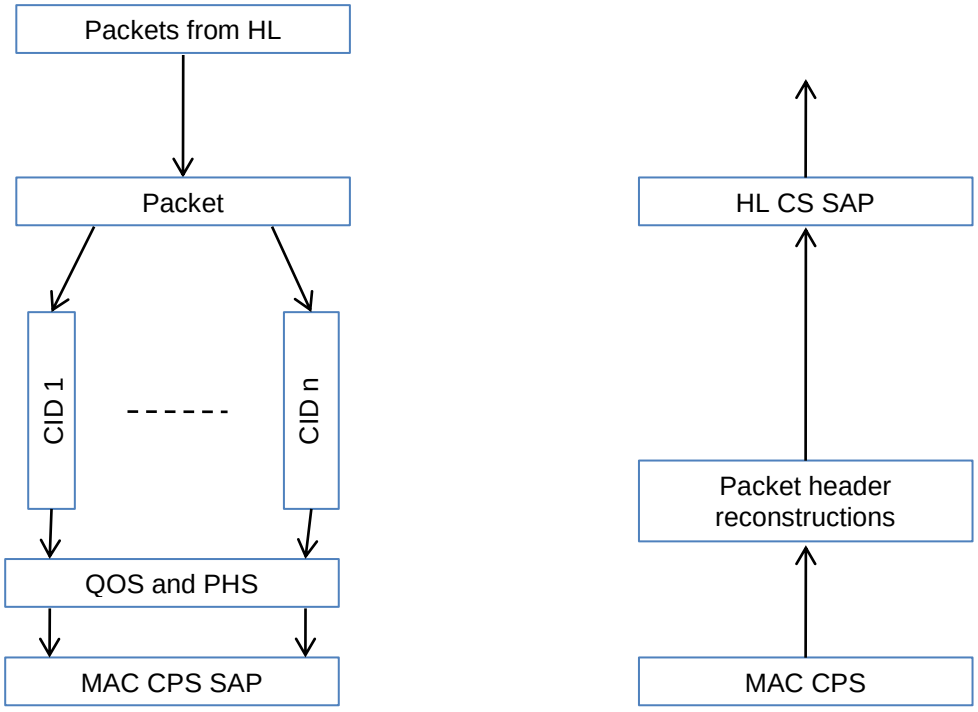


Figure 66. Convergence sublayer - packet classification

2.15.1.1.2 Many classification rules may be associated with a service flow. In such cases priority rules are set to order the packets for transmission through the connection.

2.15.1.2 *Payload header suppression*

2.15.1.2.1 Payload header suppression (PHS) function helps to remove the redundant packet header information transmitted repeatedly between base station (BS) and subscriber stations (SS) over the air interface, in order to reduce the wireless bandwidth consumption. Consider an application sending messages over an UDP connection. Every packet originating from the application will have mostly the same UDP and IP header parameters (except a few like checksums, length, etc.) added to all application payloads. Therefore, it is possible to suppress such redundant header information before packet transmissions over the air and reconstruct them back after the reception on the other end and save wireless bandwidth. AeroMACS optimizes data transmission over air interface to improve overall system performance.

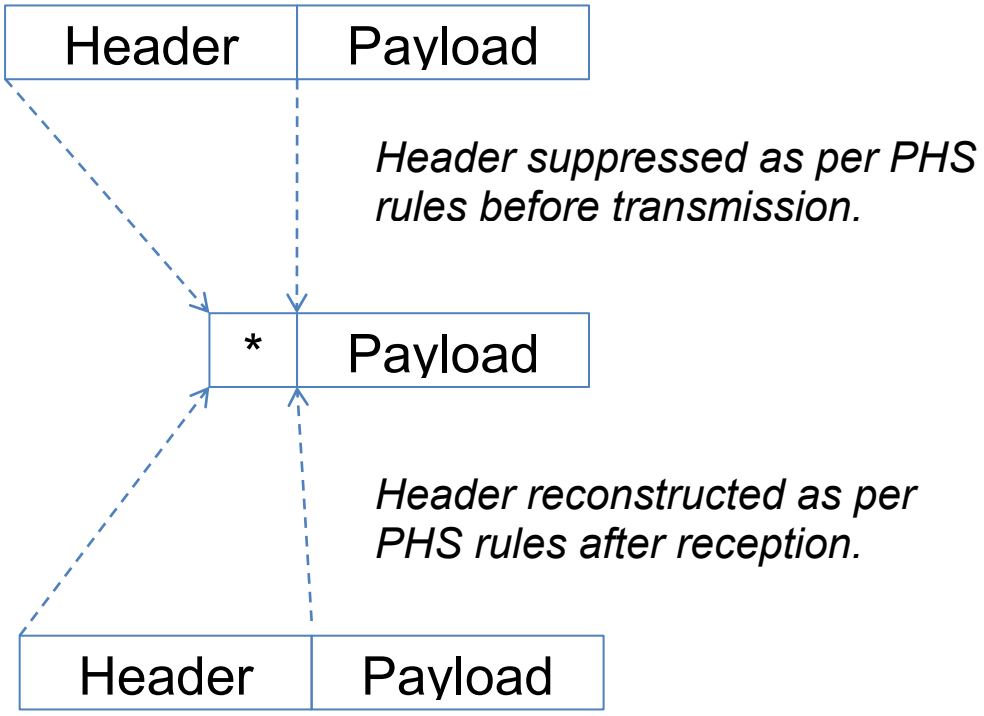


Figure 67. CS-2 payload header suppression

2.15.1.2.2 PHS happens as per a set of rules agreed in advance between SS and BS. A PHS rule is uniquely associated to a service flow identified by a classification rule. A service flow may have multiple PHS rules associated to it. In case of multiple service flows provisioned between BS and SS, it is also possible to define some service flows with PHS enabled while others with PHS disabled. AeroMACS establishes PHS rules for each service flow.

2.15.1.2.3 PHS rules are defined by a set of parameters as explained below:

PHSI

Payload header suppression index (PHSI) is used for identifying the PHS rule. This is unique per service flow. The MAC service data unit (SDU) is prefixed with PHSI when PHS is enabled. It does not exist when PHS is disabled.

PHSF

Payload header suppression field (PHSF) specifies the number of bytes in the SDU to be considered for header suppression. Based on these values the header suppression happens at the both sides. Generally, the fields in the header that do not change over the entire duration of a service flow are suppressed. The fields that change are not suppressed.

PHSM

Payload header suppression mask (PHSM) determines which parts of the PHSF need to be suppressed. A value of 1 indicates a byte to be suppressed. Otherwise, the byte is included in the transmission.

PHSS

Payload header suppression size (PHSS) indicates the size of the PHSF. Since this is just one byte, only a maximum of 255 bytes can be suppressed. During rule negotiation, if this is omitted, PHS is disabled.

PHSV

Payload header suppression valid (PHSV) indicates whether the payload header is to be verified or not before the header suppression happens. In general, enabling this field is desirable. If omitted, verification is done by default.

2.15.1.2.3 PHS operations are explained in the flow charts below.

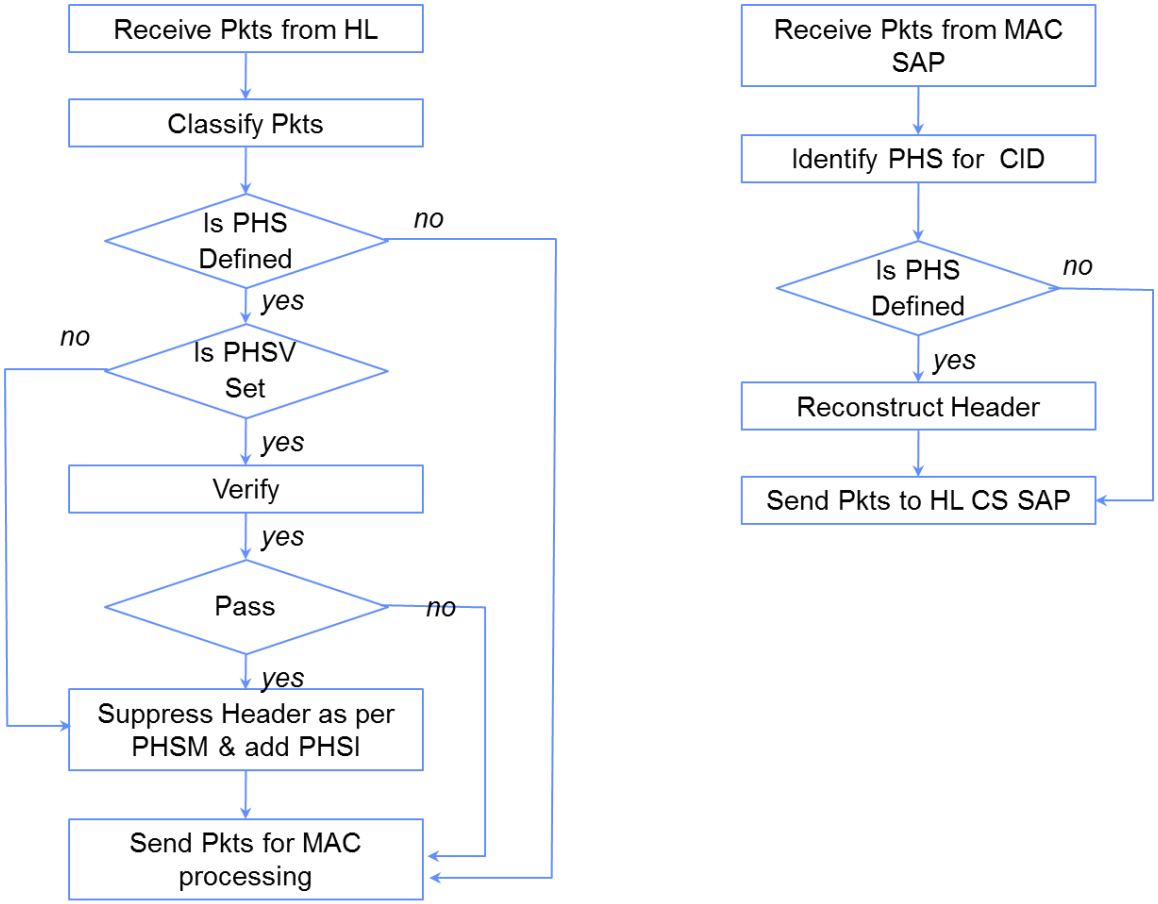


Figure 68. Convergence sublayer - PHS operations

2.15.1.2.4 On receiving packets from the higher layer, CS applies classification rules to identify the service flows for packets. If there is a PHS rule associated, then PHS definitions such as PHSI, PHSV, PHSF, PHSM and PHSS are applied to suppress the header information. If PHSV is set or not present, the bytes in the packet header are compared with the bytes in the PHSF that are to be suppressed as indicated by the PHSM. If they match, all bytes in the PHSF except the bytes masked by PHSM are suppressed. Then PHSI is prefixed to the PDU and the entire MAC SDU is presented to the MAC SAP. On reception, the CID of the packet is matched to figure out the corresponding PHS rule set. If PHS rule is identified, the packet headers are reconstructed based on PHSM and PHSF and presented to the higher layer through CS SAP.

2.15.1.2.5 The PHS rules are to be applied consistently at both SS and BS sides. Hence, this requires PHS information to be exchanged between BS and SS for the service flows.

2.15.2 IP specific part

2.15.2.1 In this configuration IP packets are directly carried over the AeroMACS link. Classification is based on IP header information. ROHC can also be used instead of PHS. Figure 69 below shows the IP CS configuration.

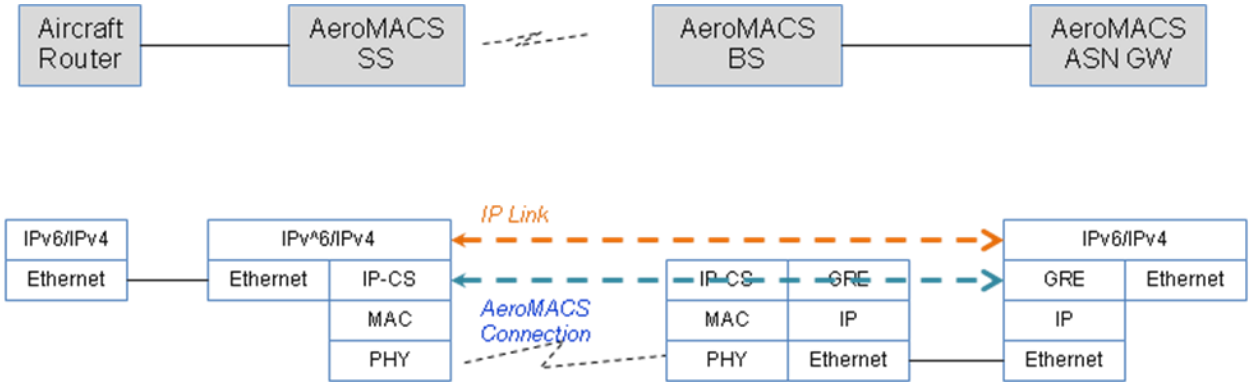


Figure 69. CS 6 IP CS

2.15.2.2 In this configuration, SS is attached to the edge IP router function. Together they establish both Layer 2 and Layer 3 connectivity with the ASN gateway.

2.15.3 Ethernet specific part

2.15.3.1 In this configuration ethernet is supported as the higher layer for AeroMACS. Ethernet packets are received at the CS SAP interface which are then classified as per the classification rules, header suppression applied if PHS rules are defined and scheduled for transmission as per the QoS policies defined for the service flow. Classification is based on ethernet header information, IP header information in case of IP over ethernet and/or VLAN header information.

2.15.3.2 Robust header compression (ROHC) is to be applied in addition to PHS to compress IP header portions in addition to ethernet header compression. ROHC operations are to be performed in accordance with RFC 3095, RFC 3759, RFC 3243, RFC 4995, RFC 3843, RFC 4996 or its successors.

The following Figure 70 shows a typical AeroMACS configuration for Layer 2 operations.

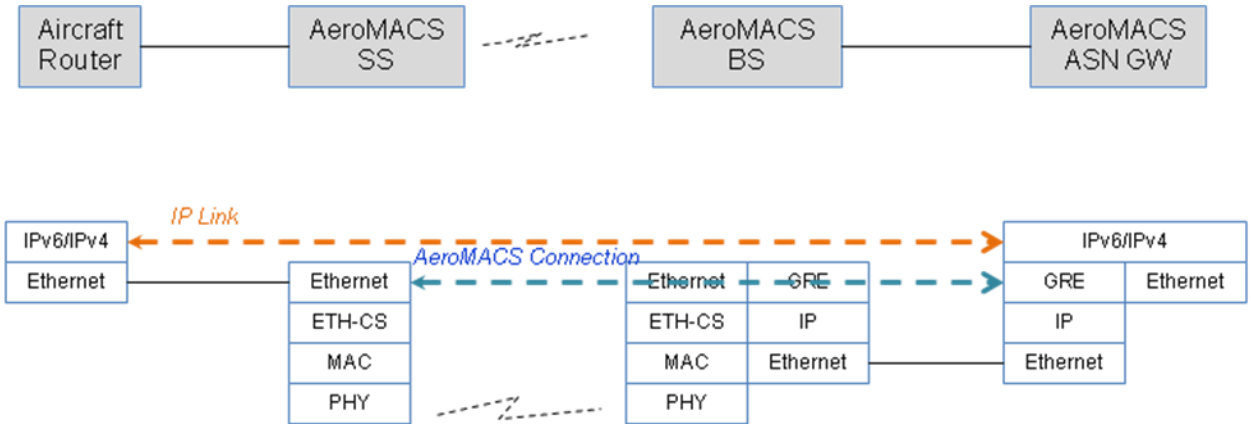


Figure 70. CS 5 ethernet CS

2.15.3.3 In this configuration BS and SS act as Layer 2 devices forwarding the ethernet packets to the other side. GRE tunnels are established between BS and the ASN gateway to extend the AeroMACS connections established between SS and BS. In this configuration SS does not perform any Layer 3 (IP) related functions such as DHCP negotiations or IP address configurations. Such functionalities are to be handled by the edge router connected to SS. Basically, the IP link is established between the SS edge router and ASN gateway.

2.16 SYSTEM MANAGEMENT

Network management services are used to establish and maintain connections between each pair of subscriber and ground systems in the AeroMACS network. These services are called NET in terms of service classification and prioritization. They include network connection and network keep-alive services and can include other performance monitoring and supervision services.

2.16.1 System supervision

System supervision capability is intended for the NAP to disseminate information concerning identified problems in the AeroMACS network to operators and ATS providers to raise awareness and facilitate problem resolution. The recommended solution is to use VLANs for network segregation, including one VLAN dedicated to management/supervision purposes (separated from user data traffic) on the BSs, and a VPN over such management VLAN used for remote access by an administrator to the BS for configuration, management and supervision purposes.

2.16.2 System management

2.16.2.1 *Overview*

2.16.2.1.1 System management features support automatic functions that are embedded in the AeroMACS protocol and administered in virtual management applications that may be running in the BS or in ancillary AeroMACS devices provided by the manufacturer such as an AAA server and a network manager console. The system management functions invoked by the protocol include:

a) security functions to authenticate and authorize the subscriber station (SS) by the BS, ASNGW and AAA server through an EAP-TLS process;

b) dynamic address allocation and management;

c) network entry and exit management of the SS;

d) handover and mobility management of the SS; and

e) service flow and QoS management.

2.16.2.1.2 These system management functions are supported by a number of system management requests/responses and notifications. As AeroMACS supports various classes of devices including aircraft, system management functions may have restrictions based on the operational requirement of the physical entity such as an aircraft it is installed on.

2.16.2.2 *System management procedures, scenarios and capabilities for the NAP*

Typical system management capability for the NAP provides an interface for use by the administrator of the network resources to configure, monitor and control AeroMACS resources. The following list contains typical system management scenarios:

a) the NAP and/or the owner of the AeroMACS system elements may need to receive notifications from the AeroMACS system elements to determine the health and activity of the AeroMACS system elements through the base station management interface. These notifications are categorized by the management application into faults, configuration, accounting, performance and security, or FCAPS;

b) if the NAP and the AeroMACS system elements belong to the same administrative domain, the NAP may need to remotely control the state of the AeroMACS system elements with basic commands to put a device in standby or normal operation and reset a device. This remote management capability from the network side is not permitted for aircraft;

c) the upper layer protocol functions, such as IPS router, may need to know the AeroMACS connectivity state in real-time to generate the appropriate routing updates and join/leave notifications. In addition, the upper layers may need to receive quality of service (such as channel utilization, transit delay, error rate, etc.) notifications in real-time for dynamic network resource management and multilink optimization; and

d) the NAP and the AeroMACS system element owner may need the capability to monitor and report intrusion attempts or other security violations.

2.16.2.3 *Event logs*

2.16.2.3.1 Each AeroMACS device maintains its own log of its own events. The logs capture event notifications from the network. Event reports include all C-aaa-IND and M-aaa-IND system management indications and trap messages from the device. Sophisticated system management applications may provide the user with a number of logs and filtering capabilities that can satisfy the typical system management needs of the NAP and the device administrator. The event log files can be automatically transferred from the system element to the central management function of its administrator periodically and/or based on specific event incidence.

2.16.2.3.2 A typical event log may capture information related to:

a) equipment changes of state, failures and recovery from failures communicated by trap messages and by notifications such as normal status;

b) results of built-in-self-tests;

c) security events such as EAP start notifications and certificate exchanges, authentication failures, detected intrusion or attack information;

d) handover events such as handover complete notifications;

e) network entry and registration events such as network attached notifications;

f) service flow events such as creation, change and deletion notifications;

g) network address assignment and address changes;

h) link connectivity state changes;

i) system configuration changes and updates; and

j) system performance information including radio frequency utilization, data throughput, one-way transit delay, bit error rate (BER), etc.

2.16.2.3.3 System management information base (MIB)

A system management information base is the repository of configuration, fault, performance, and accounting management data within the AeroMACS. Each functional component of AeroMACS, such as the BS, the SS, the ASN-GW and the AAA server will generate and maintain their own MIB. The IEEE 802.16 standard [9] specifies a set of MIB elements that are relevant for AeroMACS. However, it should be noted that all of the MIB elements defined in [9] may not be implemented by AeroMACS. Also, some of the MIB elements can be shared between AeroMACS system components, the NAP and/or the system administrator.

2.16.2.3.4 Private MIBs

In addition to the standard MIBs defined in [9], some AeroMACS implementations may use private MIB elements to provide extended management capabilities. It is difficult to specify the format and syntax of events reported by way of private MIB trap messages and that is left as a local implementation issue.

2.16.2.3.5 Network management protocol

2.16.2.3.5.1 Typically, the simple network management protocol (SNMP) is used to exchange and access the MIB elements stored in a network device. AeroMACS requires at least SNMP Version 2, while SNMP Version 3 is recommended for AeroMACS supporting safety services at higher criticality levels because SNMPv3 supports an encrypted and authenticated management information exchange.

2.16.2.3.5.2 The NAP may invoke SNMP to remotely monitor and manage AeroMACS BS, SS, ASNGW and AAA servers within its own administrative domain. ***However, due to safety concerns, remote management and monitoring of MSs installed on aircraft is not permitted.*** Similarly AeroMACS SS and network components belonging to a different administrative domain may not be accessible by the NAP, although some fault and performance management information might be shared across administrative boundaries.

2.16.3 **Performance management**

Performance monitoring consists in the collection of reliable statistics of the quality of data link communications between subscribers and ground systems within the AeroMACS network. These statistics can be collected over different timescales, including system (e.g. dropped call statistics, BS loading conditions, channel occupancy), user (e.g. terminal capabilities, mobility statistics), flow, packet, etc. The statistics are used by the AeroMACS ground system or component operator to detect data link events that cause the communication service to no longer meet the requirements for the intended function. The ground system also supports notification capability in order to enable system supervision. The monitoring capability should not impede the normal operation of the AeroMACS network.

CHAPTER 3

TECHNICAL SPECIFICATIONS

3.1 FREQUENCY ALLOCATION/CHANNELIZATION

3.1.1 RF profile for AeroMACS

3.1.1.1 AeroMACS radios must be capable of operating in the band 5 000 - 5 150 MHz.

Note 1.— The SARPs require operation from 5 030 – 5 150 per the ITU allocation however, the allocation between 5 000 and 5 030 MHz is possible through national allocations in some States, so for flexibility AeroMACS radios are to cover the entire band from 5 000 – 5 150 MHz.

Note 2.—

a) international band: 5 091 – 5 150 MHz (international table of frequency allocations);

b) national band: 5 000 – 5 030 MHz (national allocations); and

c) secondary international band: 5 030 – 5 091 MHz. This band is also allocated for use by microwave landing systems (MLS) and remotely piloted aircraft systems (RPASs).

3.1.1.2 All AeroMACS channels must use 5 MHz bandwidth and each channel must be tuneable in increments of 250 kHz.

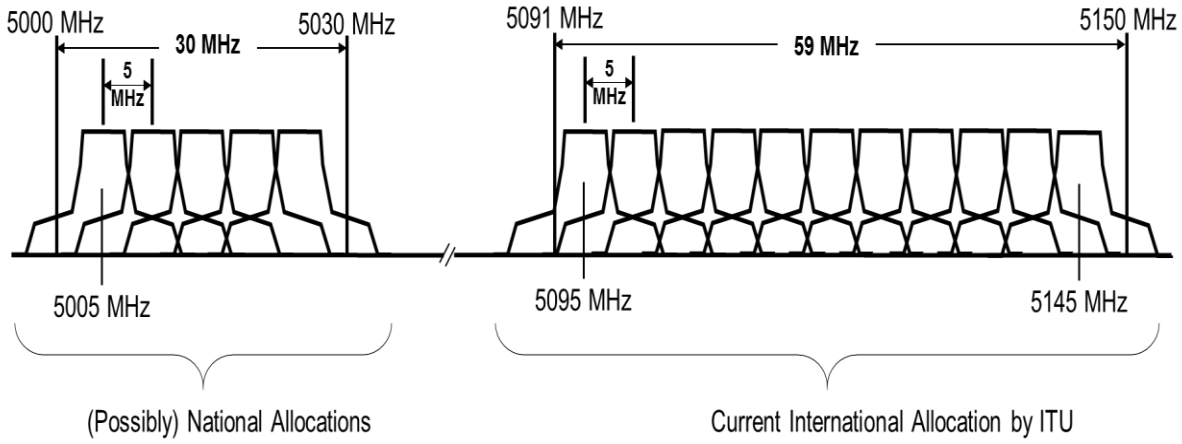


Figure 71. AeroMACS channel assignments

3.1.2 AeroMACS band class group

AeroMACS must comply with the WiMAX Forum® mobile radio specifications for mobile stations and base stations, as listed in Table 38.

Band class group	Uplink MS transmit frequency (MHz)	Downlink MS receive frequency (MHz)	Channel BW (MHz)	Duplex mode	WiMAX Forum® air interface release
10.A	5 000 – 5 150	5 000 – 5 150	5	TDD	1.0

Table 38. AeroMACS band class group and primary characteristics

3.1.3 RF profile for AeroMACS

AeroMACS must comply with the WiMAX Forum® mobile radio specifications for RF channel centre frequencies given in Table 39. RF channel centre frequencies are derived as a function of RF channel centre frequency numbers (fcN) using the following equation:

fc = 0.05 * fcN

The RF channel centre frequency (fc) is in MHz.

In Table 38, the RF channel centre frequency number set is specified using the following triple:

(fcNstart, fcNstop, step)

Where:

a) fcNstart is the starting RF channel centre frequency number assigned to the first RF channel centre frequency;

b) fcNstop is the ending RF channel centre frequency number assigned to the last RF channel centre frequency, and step is the RF channel centre frequency number step size between fcNstart and fcNstop.

Band class group	Channel BW (MHz)	Frequency range (MHz)		RF channel centre frequency number set	
		Uplink	Downlink	Uplink	Downlink
10.A	5	5 000 – 5 150	5 000 – 5 150	(100 050, 102 950, 5)	(100 050, 102 950, 5)

Table 39. AeroMACS channel set definition

Note 1.— The AeroMACS centre frequency step size is 250 KHz consistent with WiMAX Forum® Air Interface Release 1.0. Standard AeroMACS RF channels are every 250 kHz from a channel centre frequency of 5 002.5 MHz to 5 147.5 MHz.

3.1.4 Preferred channel centre frequencies for AeroMACS

AeroMACS must comply with the WiMAX Forum® mobile radio specifications for preferred channel centre frequencies as given in Table 40.

Band class group	Channel BW (MHz)	Frequency range (MHz)		RF channel centre frequency number set	
		Uplink	Downlink	Uplink	Downlink
10.A	5	5 000 – 5 150	5 000 – 5 150	(100 100, 102 900, 100)	(100 100, 102 900, 100)

Table 40. AeroMACS preferred channel set definition

Note 1.— According to Table 38, the offset between adjacent channel centre frequencies is 5MHz.

3.2 SITING

3.2.1 Antenna tower must not penetrate "imaginary surfaces" as given in Annex 14, Volume I, Chapter 4, at the airports which protect the aircraft operations from hazards.

3.2.2 (Doc 9157)The siting of all equipment and its installation in operational areas must comply with the provisions of Annex 14, Volume I, in particular Chapter 9, section 9.9.

3.2.3 The AeroMACS equipment, antenna and power supply must not be installed inside the runway safety area (RSA).

3.2.4 Antenna must be frangible in accordance with Annex 14, Volume I, provisions, in particular Chapter 5. Guidance on frangibility is available in Doc 9157, *Aerodrome Design Manual*, Part 6, *Frangibility*.

Note 1.— EIRP defined as antenna gain in a specified elevation direction plus the average AeroMACS transmitter power. While the instantaneous peak power from a given transmitter may exceed that level when all of the subcarriers randomly align in phase, when the large number of transmitters assumed in the analysis is taken into account, average power is the appropriate metric.

Note 2.— The breakpoints in the EIRP mask are consistent with the elevation pattern of a +15 dBi peak, 120 degree sector antenna as contained in ITU-R F.1336-2.

Note 3.— These values were derived using the worst-case analysis described. Other approaches involving higher powers may be acceptable, however, additional analysis must be performed to ensure the total interference allowable at the FSS satellites, consistent with ITU requirements, is not exceeded.

Note 4.— If a sector contains multiple transmit antennas (e.g. MIMO), the specified power limit is the sum of the power from each antenna.

3.3 INTERFERENCE

3.3.1 As described in sections 2.6.2.6 and 3.2, the implementation of AeroMACS needs to be planned in a way that it will minimize the risk for potential interference to FSS. In particular the channel assignments, the ground antenna patterns and antenna tilt should be considered.

3.3.2 Where antenna tilt is employed, it is highly recommended that site surveys are undertaken to ensure that extraneous reflections do not result in further interference.

3.3.3 In order to evenly spread the interference to FSS, it is recommended that the assignment of AeroMACS channels be distributed uniformly over areas containing several airports.

Note.— The above recommendation is particularly relevant for the case of airports which do not use all of the AeroMACS channels.

3.3.4 It is also recommended that the local AeroMACS implementations optimize the ground antenna gain to minimize impact to the FSS services.

3.4 SYSTEM ARCHITECTURE

3.4.1 AeroMACS ASN profile

AeroMACS must conform to WiMAX Forum® Profile C as described in [5].

3.4.2 ASN gateway

At any given time, it is required that only one ASN GW authorizes and manages service flows to an SS.

Note.— The ASN-GW implementation may include redundancy and load-balancing based on radio parameters, among several ASN-GWs.

3.4.3 AAA proxy/server

3.4.3.1 The AeroMACS AAA server of the home NSP must distribute the subscriber's profile to the NAP.

3.4.3.2 The ASN-GW must support capabilities for SS authorization and authentication through interaction with an AAA server.

3.4.4 Network architecture

3.4.4.1 Network deployment models

3.4.4.1.1 AeroMACS must be able to support multiple NSPs for the provision of ATS/AOC/airport services over the same AeroMACS link.

3.4.4.1.2 AeroMACS infrastructure must provide the capability to the SS to select the preferred CSN/NSP.

3.4.4.2 Requirements for H-NSP, V-NSP, NAP

3.4.4.2.1 The H-NSP must maintain the connectivity and reachability status of each SS for which it has an SLA.

3.4.4.2.2 The H-NSP must authenticate and authorize network entry for each SS for which it has an SLA.

3.4.4.2.3 The visited-network service provider (V-NSP) must coordinate with the H-NSP to authorize and authenticate an MS.

3.4.4.2.4 The NAP must provide the means for authentication of each SS through an NSP.

3.4.4.2.5 The NAP must provide access to AeroMACS services for each authenticated SS.

3.4.5 AeroMACS profile

3.4.5.1 An MS is required to have a list of NSPs with which it has a communication requirement.

3.4.5.2 The most significant 24 bits (MSB 24 bits) of the "base station ID" are required to be used as the operator ID, which is the NAP identifier.

Note.— NAP discovery is based on the procedures defined in the IEEE 802.16 standard and out of the scope of this specification.

3.4.5.3 In the NAP and NSP deployment case where there is only one NSP associated with the NAP and where no regulatory or deployment reasons justify separate presentation of an NSP identifier, the NAP is required to set the NSP identifier flag to a value of '0'.

Note.— In this case, when the MS detects the identifier of a NAP, the MS knows the identifier of the associated NSP.

3.4.5.4 NSP ID is required to follow the ICAO IPS object ID (OID) convention given in Doc 9896.

3.4.5.5 In the authentication process described in section 2.11, the SS is required to format the NAI (network access identifier) used as an outer identity during EAP exchanges as follows: <routing realms>< decoration><username>@<realm> where:

Note 1.— Routing realms: optionally used. The use of the routing realm is described by RFC 4282 and 7542. (RFC 4282 has been superseded by RFC 7542, however, the description given in RFC 4282 is

adequate for AeroMACS and also provides more detail, hence this is maintained as a reference for AeroMACS).

Note 2.— Decoration: decorated NAIs are optionally used to force routing of messages through a list of pre-defined realms and in that way force certain inter-realm roaming arrangements. This is described in section 2.7 of RFC 4282. NAI decoration is used by RADIUS (RFC 2486) The NAI decoration is extensible. The decoration consists of one or more attribute value pairs (avp) separated by the "|"enclosed within curly braces.

Note 3.— "{" avp1 "|" avp2 ..."}" where an avp is formatted as: name"="value with no spaces before and immediately after the "=". The character set used for name and value must be consistent with the character set specified by RFC 4282. The name must be alphanumeric with no spaces. Currently there is no specific avp defined.

3.4.5.6 When an aircraft (MS) lands and scans the AeroMACS band, it must first select a NAP and then the NSP.

Note 1.— The way/order in which the channels are scanned and the way the preferred NAP is selected are implementation-dependent. The NAP (operator) selection can rely on the following criteria:

a) preferred operator (if commercial); and

b) NSP support (especially the ability to support ATC flows and other needed flows,).

Note 2.— The procedure for NAP selection may be as follows:

a) select a NAP who is providing aircraft connectivity;

b) select a NAP who is contracted (might not be compulsory for ATC traffic only);

c) select the preferred NAP if several are possible (based on airline preferences);

d) select a NAP who can provide ATC connectivity up to H-NSP; and

e) select a NAP who can authenticate the aircraft (by relaying the AAA requests to the H-NSP).

Note 3.— The previous procedure can be satisfied either by:

a) analyzing the operator ID (that would be encoded in a specific way); or

b) pre-determining channel values/operator IDs in a local aircraft configuration file; or

c) analyzing the NSP IDs supported by the NAP and select the NAP depending on the NSP ID.

3.4.5.7 The MS may use the H-NSP realm as <routing realm> in the authentication process.

3.4.5.8 The ASN may use the H-NSP realm as <routing realm> to route to the proper NSP.

3.4.6 **Mobility**

3.4.6.1 Mobility is required to be implemented in compliance with the *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols* (Doc 9896).

3.4.6.2 A secure communication path (e.g. private network tunnel) between ASN-GW to the H-NSP is required.

3.4.6.3 To complete the support of a moving aircraft into a visited ASN, the MSs is required to support mobility.

3.4.7 **IP address configuration**

3.4.7.1 AeroMACS infrastructure is required to support network addressing as specified in Doc 9896.

3.4.7.2 AeroMACS must support IPv6.

Note 1.— AeroMACS implements IPv6 addressing architecture as specified in RFC 4291 and uses globally scoped IPv6 addresses.

Note 2.— ATN/IPS MSPs containing AeroMACS networks may obtain IPv6 address prefix assignments from their local internet registry (LIR) or regional internet registry (RIR).

3.4.7.3 AeroMACS must also support IPv4.

Note.— Support of IPv4 is required in order to be interoperable with legacy systems.

3.4.7.4 ASN routers must support dual the network layer stack, tunnelling or protocol conversion, as specified in Doc 9896, for connecting IPv6 core networks to the AeroMACS ASN network which can implement the IPv4 stack.

3.4.7.5 AeroMACS infrastructure must support network addressing for vehicles and aircraft in the home and visited networks without distinction.

3.4.7.6 Mobile IPv6 must be implemented by a mobility service provider (MSP) in compliance with ICAO 9896 standard for communication with aircraft.

3.4.7.7 AeroMACS must support both static and dynamic IP addressing mechanisms.

Note.— Details on how IPv4 addressing is to be implemented are specified in [4].

3.4.7.8 If dynamic addressing is used, then DHCP server must allocate a dynamic IP address to the SS.

Note.— ICAO is in the process of updating Doc 9896 to include IP address assignment, network discovery, routing and mobility management. This document will provide additional requirements and guidance.

3.4.7.9 AeroMACS must support multiple NSPs for the provision of ATC/AOC services over the same data link.

3.4.7.10 AeroMACS infrastructure should provide the capability to the subscriber to select the preferred CSN/NSP.

Note.— Connectivity and reachability of the preferred CSN will depend on a device authentication process at network entry.

3.4.7.11 ASN-GW is required to support GRE tunnelling on R6 interface.

3.4.7.12 The network addresses for the management/control domain of CSN must be different from the ASN data plane addresses in order to ensure network abstraction.

3.5 SECURITY FRAMEWORK

3.5.1 The AeroMACS network must support the following protocol options:

a) PKM V2 for public key management;

b) EAP for authentication; and

c) TLS method along with EAP for exchanging authentication parameters.

3.5.2 **PKI profile**

3.5.2.1 Device certificates must not include the *subjectKeyIdentifier* extension.

3.5.2.2 Device certificates must not include the *basicConstraints* extension.

3.5.2.3 The *countryName* is required to be the two-letter ISO 3166-1 country code for the country in which the device sponsor's place of business is located.

3.5.2.4 The *organizationName* must contain the device sponsor organization name (or abbreviation thereof), trademark, or other meaningful identifier.

3.5.2.5 When the *organizationalUnitName* is included, one or more OUs are required to contain additional identifying information.

3.5.2.6 The *commonName* is required to contain the device MAC Address or the aircraft 24-bit ICAO ID that will bind the certificate's public key to the device.

3.5.3 PKI management

The following section identifies the fundamental PKI specification and policy requirements of the device sponsor. A device sponsor is the entity (e.g. company or individual) that requests a certificate on behalf of a device within the AeroMACS ecosystem. The device sponsor asserts that the device will use the key and certificate in accordance with the certificate policy asserted in the certificate. The requirements in this chart are categorized into the various actions, roles and considerations throughout the certificate lifecycle.

3.5.3.1 *Certificate enrolment process and responsibilities*

Note.— The device sponsor agrees to be bound by a relevant subscriber agreement that contains representations and warranties.

3.5.3.1.1 The device sponsor must complete a certificate application by providing true and correct information.

3.5.3.1.2 The device sponsor must generate, or arrange to have generated by a trusted authority, a key pair.

3.5.3.1.3 The device sponsor must deliver the device public key, directly or through an RA, to the CA's facility.

3.5.3.1.4 The device sponsor must demonstrate possession of the private key corresponding to the public key.

3.5.3.1.5 The device sponsor must protect the private key and use the certificate and private key for authorized purposes only.

3.5.3.2 *Pre-requisites for certificate acceptance*

3.5.3.2.1 The device must be capable of downloading, installing and using the AeroMACS PKI digital certificate.

3.5.3.2.2 The device must be able to use the private key corresponding to the public key in the certificate once the device sponsor has agreed to the subscriber agreement and accepted the certificate.

3.5.3.2.3 The device sponsor must protect the device private keys from unauthorized use.

3.5.3.2.4 The device must discontinue use of the private key following expiration or revocation of the certificate.

Note.— The device sponsor should use the certificate lawfully in accordance with the subscriber agreement and the terms of the CP.

3.5.3.2.5 The device must use the certificate for functions as defined by the *keyUsage* and *extendedKeyUsage* extensions within the certificate.

3.5.3.3 *Processing certificate renewal requests*

The device must provide proof of possession of the private key in order to renew a certificate.

3.5.3.4 *Certificate re-key*

3.5.3.4.1 The device sponsor is required to identify themselves for the purpose of re-keying.

3.5.3.4.2 The device must provide proof of possession of the newly generated key pair's private key.

3.5.3.5 *Certificate revocation*

If a device sponsor is ceasing its relationship with an organization that sponsored a certificate, they must, prior to departure, surrender to the organization (through any accountability mechanism) all such hardware tokens that were issued by or on behalf of the sponsoring organization.

3.5.3.6 *Device private key compromise*

The device sponsor must report any suspected or real compromise of the device private key to their issuing CA or RA.

3.5.3.7 *Device key pair generation*

When requesting a medium-assurance software certificate, the trusted authority must generate the keys in a hardware cryptographic module rated at least FIPS 140-2, Level 2.

3.5.3.8 *Private key delivery to device sponsor*

The device sponsor must acknowledge receipt of the private key(s) for the device.

3.5.3.9 *Cryptographic module standards and controls*

3.5.3.9.1 The device with medium-assurance software certificates must use a FIPS 140-2 Level 2 or higher approved cryptographic module for their cryptographic operations.

3.5.3.9.2 Aircraft avionics devices must use hardware or software cryptographic modules that are consistent with jurisdictional regulations concerning avionics implementations supporting safety and regularity of flight services.

3.5.3.10 *Private key escrow*

Device private signatures keys must not be escrowed.

3.5.3.11 *Private key backup*

3.5.3.11.1 If required by applicable jurisdictional regulatory law to support key recovery, backed up private keys must be held under the control of the device sponsor or other authorized administrator.

3.5.3.11.2 Device private signature keys must not be backed up.

3.5.3.12 *Private key archival*

Device private signatures keys must not be archived.

3.5.3.13 *Device private keys*

3.5.3.13.1 The device must be authenticated to the cryptographic module before the activation of any private keys.

3.5.3.13.2 Entry of device activation data must be protected from disclosure (i.e. not displayed while entering).

3.5.3.14 *Certificate operational periods and key pair usage periods*

3.5.3.14.1 The device private signing keys must be valid for a maximum of five (5) years.

3.5.3.14.2 The device public verification keys and certificates must be valid for a maximum of five (5) years.

Note 1.— For aircraft, the private keys will typically have a lifetime which coincides with the aircraft maintenance cycles to ensure manual updating. The transmission of private keys over electronic media has the potential to compromise security.

Note 2.— For ground systems, the private keys will typically have a lifetime determined by a State's safety and security assessments.

3.5.3.15 *Activation data transmission*

To the extent desktop computer or network logon user name/password combination is used as activation data for a device, the passwords transferred across a network must be protected against access by unauthorized users.

3.6 PRIORITIZATION

3.6.1 AeroMACS must support expedited real-time polling service (ertPS); real-time polling service (rtPS); non real-time polling service (nrtPS) and best effort (BE) service for scheduling service flows over the physical layer.

3.6.2 AeroMACS scheduler must service the flows in priority order staring with ertPS, followed by rtPS, followed by nrtPS, followed by BE.

3.6.3 AeroMACS must pre-empt lower priority MPDUs until all higher priority MPDUs are serviced.

Note.— If a higher priority MAC protocol data unit (MPDU) arrives at an AeroMACS scheduler queue while it is servicing a low priority MPDU, the scheduler may complete processing of that MPDU and then start processing the higher priority MPDU, while pre-empting the remaining lower priority MPDUs.

3.7 SERVICE FLOW MANAGEMENT

3.7.1 Classes of service

3.7.1.1 AeroMACS must support the following classes of service:

a) VoIP1;

b) VoIP2;

c) VoIP3;

d) NET;

e) ATS1;

f) ATS2;

g) ATS3;

h) AOC1; and

i) DEFAULT.

Note 1.— Service flows are unidirectional. So, two service flows are created for each di-directional information exchange.

Note 2.— CoS 1 through 8 above are priority services that are supported by reserving specific throughput (data rate) for transmission over the AeroMACS network.

Note 3.— DEFAULT CoS is a best effort and is common for all devices. Any residual bandwidth after the priority classes are allocated to DEFAULT, which is then shared among all devices on a best effort basis.

3.7.1.2 AeroMACS BS must create the required service flows for each SS upon its entry into the AeroMACS network.

3.7.1.3 AeroMACS must allocate minimum and maximum sustained data rates to each of the priority CoS as shown in Table 41.

Note.— For each CoS in Table 40, the QoS parameters include: latency, minimum and maximum rate, and priority. Some QoS parameter values, such as the maximum latency and the minimum reserved rate, are directly imposed by the application QoS requirements.

	Minimum reserved rate		**Maximum sustained rate (5 per cent higher)**	
	DL (kbps)	**UL (kbps)**	**DL (kbps)**	**UL (kbps)**
VoIP1	64	64	N/A	N/A
VoIP2	48	48	N/A	N/A
VoIP3	32	32	N/A	N/A
NET	32	32	34	34
ATS1	32	32	34	34
ATS2	32	32	34	34
ATS3	32	32	34	34
AOC1	64	128	67	134
Total			267	334

Table 41. Bandwidth (kbps) required by high priority services

3.7.2 Traffic handling in the network

3.7.2.1 AeroMACS must receive user data priority and CoS indication from the internet protocol layer through the IP-CS interface.

3.7.2.1.1 The DSCP value in the ToS field of IPv4 header or the DSCP value in the traffic class field of the IPv6 header must be used to signal the application's priority and CoS requirement.

3.7.2.2 In case of congestion, AeroMACS must queue IP packets according to the different priorities and CoS (RFC 4594 gives a recommendation on service categorization).

3.7.2.3 Packets entering DiffServ networks must be classified and scheduled as per the DSCP markings.

3.7.3 Mapping of IP QoS with AeroMACS service flows

3.7.3.1 AeroMACS must map DSCP and PHB values signalling IP priority and precedence to the AeroMACS service flows as defined in Table 42 below.

	Generic Layer 3			Generic Layer 2	ATN Mapping	AeroMACS Mapping	
DSCP value	**PHB meaning**	**Drop probability**	**Equivalent IP precedence value**	**Precedence value**		**CoS**	**Scheduling**
0	CS0 Default	N/A	000 - Routine	Routine	BE	DEFAULT, APT1, APT2	BE
1000	CS1			Priority			
1010	AF11	Low	001 - Priority		AIDC	AOC1	nrtPS
1100	AF12	Medium	001 - Priority			ATS3	nrtPS
1110	AF13	High	001 - Priority				
10000	CS2			Immediate	CM		
10010	AF21	Low	010 - Immediate		ATSMHS		
10100	AF22	Medium	010 - Immediate				
10110	AF23	High	010 - Immediate			Emergency video	rtPS
11000	CS3			Flash			
11010	AF31	Low	011 - Flash		Voice recording		
11100	AF32	Medium	011 - Flash			ATS2	rtPS
11110	AF33	High	011 - Flash				
100000	CS4			Flash override	CPDLC ADS-C		
100010	AF41	Low	100 - Flash override		Voice signalling	NET	rtPS
100100	AF42	Medium	100 - Flash override			ATS1	rtPS
100110	AF43	High	100 - Flash override				
101000	CS5			Critical			
101110	EF	N/A	101 Critical		Voice	VoIP1, VoIP2, VoIP3	ertPS
110000	CS6			Internetworking control			
111000	CS7			Network control			

Table 42. Mapping of IP QoS with AeroMACS service flows

Note 1.— Values of DSCP not shown in this table are assumed to be assigned to the default (CS0) CoS. Local implementations may assign DSCP values not shown in this table for local use on a per-hop behaviour and, therefore, not affecting all routers in the possible path of the message. Those DSCP values will map to default.

Note 2.— ATN mapping for CPDLC and ADS-C are assigned to DSCP CS4, which is a generic Layer 2 assignment. Therefore, CPDLC and ADS-C are to be transferred over AeroMACS using ATS1, which uses the generic Layer 2 flash override assignment and therefore maintains the same Layer 2 level.

Note 3.— ertPS service is allocated for voice services and is mapped to expedited forwarding (EF) in IP QoS.

Note 4.— NET traffic corresponds to network control and management packets. It is mapped to AF31 PHB at IP level and allocated to rtPS scheduling for AeroMACS.

Note 5.— ATS1 and ATS2 services are identified as rtPS, while lesser critical ATS3 service is identified as nrtPS for scheduling.

Note 6.— An emergency video service is introduced with a PHB value of AF23 mapping to rtPS scheduling for AeroMACS.

Note 7.— AOC1 service having nrtPS scheduling is mapped to the PHB value of AF13.

Note 8.— All other services namely AOC2, APT1 and APT2 are mapped to BE (default PHB).

3.7.4 **Device classes**

AeroMACS must support aircraft, surface vehicle, video sensor, ground critical and ground default device classes.

3.7.4.1 AeroMACS must at least support the mandatory service provisions for each device class as shown in Table 43 below.

CoS	Scheduling	AeroMACS Traffic Priority	IP QoS PHB	Aircraft	Surface Vehicle	Video Sensor	Ground Critical	Ground Default
Voice	ertPS	N/A	EF	X	X			
NET	rtpS	N/A	AF31	X	X	X	X	X
ATS1	rtPS	1	AF32	X	X		X	
ATS2	rtPS	2	AF33	X				
ATS3	nrtPS	N/A	AF12	X				
AOC1	nrtPS	N/A	AF13	X				
Video (E)	rtPS	N/A	AF23			X		
Default	BE	N/A	DF	**Default supported by all devices**				
APT1	BE	N/A						
APT2	BE	N/A						

Table 43. Mandatory service provision for each device class

3.7.4.2 Network control/management (NET) and default (DF) CoS must be provisioned for all device classes.

3.7.4.3 Aircraft devices must be provisioned with at least additional five CoS, i.e. VOIP1, ATS1, ATS2, ATS3 and AOC1.

Note 1.— Surface vehicle device class should support at least additional voice and ATS1 CoS.

Note 2.— Ground critical device class is intended to be used by safety critical sensors at the airports. Therefore, additional ATS1 CoS is recommended for these devices.

Note 3.— Video sensor device class is intended for sending uni-directional videos during emergency situations. Hence, only one additional emergency video CoS is recommended for this device class.

Note 4.— The identified services flows are proposed as mandatory for the device classes, but this may not restrict an AeroMACS service provider to offer more provisions for a device depending upon the availability of its network resources.

3.7.4.4 *Identification of classes*

3.7.4.4.1 The AeroMACS PKI device certificate profile must include a field called "tbsCertificate.subject" that is used to provide the identity of the associated device.

3.7.4.4.2 While requesting a PKI digital certificate for a device, device credentials along with its device type must be provided to certificate authority (CA).

3.7.4.4.3 The AeroMACS AAA server must contain the device profiles with mandatory CoS requirements as defined in section 3.8.4.1 above.

3.7.4.4.4 During the network entry of an SS, the AAA server must determine the required CoSs for the SS based on its device class from the certificate and the device profile stored in the AAA server's configuration database.

3.7.4.4.5 During network entry of an SS, the AAA server must inform the ASNGW about the required static service flows that must be provisioned for that SS.

3.7.4.4.6 The ASNGW, in conjunction with the BS, must establish the required service flows for the SS.

3.8 HANDOVER

3.8.1 AeroMACS must support the handover process in which a subscriber station (SS) migrates from the air-interface provided by one base station (BS) to the air-interface provided by another BS. AeroMACS must implement the HO process as defined in IEEE 802.16-20096.3.21.2.9.

3.8.2 The SS typically initiates the handover process when channel quality deteriorates by:

a) identifying other possible base stations to handover to;

b) requesting a handover to the desired base station through an exchange of messages with the target BS;

c) initiating a handover time; and

d) handing over communications to the target base station in an orderly manner that maintains continuous and uninterrupted communications to and from the SS.

3.8.3 The SS must restart the handover process automatically if the handover timer expires before handover to the target BS is completed.

3.8.4 The SS may stop the handover process if channel conditions change and become more favourable and handover becomes unnecessary during the handover timer period.

3.8.5 The target BS must deny the SS handover request if the target BS is fully subscribed and the service flows from the SS have insufficient priority to pre-empt existing service flows associated with the target BS. In this event, the SS initiates a new handover process to another available BS.

Note.— Macro-diversity handover (MDHO) and fast-base station switching handover (FBSS) features are not required to be supported by AeroMACS.

3.9 ROUTING AND DISCOVERY

AeroMACS must support static and dynamic addressing in order to support the routing and discovery mechanisms to be used for the ATN/IPS.

Note.— The ATN/IPS routing and discovery mechanisms are defined in Doc 9896, Part 1, paragraphs 2.3.2 and 2.3.14 to 18.

3.10 UPPER LAYER INTERFACES

3.10.1 AeroMACS must support the IP-CS convergence sublayer supporting the internet protocol.

3.10.2 The recommendation is made that, as an option, AeroMACS can support the ETH-CS convergence sublayer.

3.11 SYSTEM MANAGEMENT

3.11.1 General

3.11.1.1 AeroMACS must support fault, performance, configuration and security management functions necessary for safety and regularity of flight.

3.11.1.2 AeroMACS must support simple network management protocol (SNMP) Version 2 or higher, to exchange system management information between AeroMACS subsystems using a centralized network management function and local system management function as applicable.

3.11.1.3 AeroMACS system components must store system management elements (events, alerts and configuration items) in a management information base (MIB).

3.11.1.4 AeroMACS system management elements to be shared or accessed via SNMP must conform to the MIB specifications defined in IEEE 802.16 Standard.

3.11.1.5 AeroMACS MS installed on an aircraft must exchange MIB elements only with the local system management function and upper layer protocol functions that are also installed on the aircraft.

3.11.1.6 AeroMACS MS installed on an aircraft must reject any MIB element access or update requests received through the air/ground network interface.

3.11.1.7 AeroMACS BS, ASNGW, AAA server and SS installed on the ground must exchange MIB elements with network operator and network management function if they belong to the same administrative domain.

3.11.1.8 It is recommended that the AeroMACS SSs, installed on ground, BSs, ASNGW and the AAA Server share basic fault and performance management MIB elements with the network operator in a different administrative domain to facilitate troubleshooting, network resource management, information routing and operation of the network.

3.11.2 Fault management

3.11.2.1 Each AeroMACS subsystem must execute periodic, non-destructive self-tests to detect faults.

3.11.2.2 Each AeroMACS subsystem must generate meaningful alerts if any fault is detected which transitions the subsystem to subnormal or failure state as applicable.

3.11.2.3 Each AeroMACS subsystem must generate alert-clear notifications when the fault condition is cleared, which returns the subsystem to normal operating state.

3.11.3 Performance management

3.11.3.1 AeroMACS BS and SS MUST collect pertinent link and physical layer performance data which may include one-way link transit delay, average available bandwidth on the physical channel for information exchange, average bit error rate experienced on the AeroMACS channel and average packets dropped per service flow.

3.11.3.2 AeroMACS BS and SS must report the collected performance data to the local system management function and the upper layer protocol (IPS) for QoS computation and for routing decisions.

3.11.3.3 AeroMACS BS and MS installed on an aircraft MUST monitor link state (disconnected, connected, connection available).

3.11.3.4 AeroMACS BS and MS installed on an aircraft MUST generate alerts to local system management and the upper layer protocol (IPS) every time the link connectivity state changes.

3.11.3.5 It is recommended that each AeroMACS subsystem generates alerts if a configurable threshold exceeds on some performance parameters being monitored.

3.11.4 Configuration management

3.11.4.1 Each AeroMACS subsystem MUST only permit system configuration updates and changes from a TRUSTED system management function belonging to the same administrative domain as the subsystem itself.

3.11.4.2 AeroMACS MS installed on an aircraft must reject system configuration changes or updates originating from any system outside that aircraft's control or information services domain (ACD or AISD).

3.11.4.3 AeroMACS subsystems must log every configuration change in the MIB event log.

3.11.5 Security management

3.11.5.1 Each AeroMACS subsystem must store its digital certificate and the certificate chain up to its root of trust in a local storage.

3.11.5.2 Each AeroMACS subsystem must ensure that its private key is stored securely in local storage and is accessed only through a secure mechanism.

3.11.5.3 An AeroMACS certificate must be permanently and digitally bound to the device it is installed on.

3.11.5.4 Disassociation of an AeroMACS certificate from the device it is installed on must revoke that certificate.

APPENDIX

TEST PROCEDURE FOR SPECTRAL MASK AND EMISSIONS

A.1 INTRODUCTION

The purpose of this test is to verify compliance of the spectral mask and emissions requirements as required by the SARPs Standard. This procedure provides the minimum procedures necessary to ensure compliance with section 7.4.5 of the AeroMACS SARPs and section 2.5 of this manual.

The above requirements exist to ensure that the BS/MS do not transmit signals with unwanted emissions in the frequency range immediately outside the necessary bandwidth to avoid interference to other frequency bands or systems.

A.2 GENERAL INFORMATION

A.2.1 **References**

[1] ITU-R SM.329-12 (2012-09)

A.2.2 **Abbreviations**

BS: Base station
BSE: Base station emulator
MS: Mobile station
RBW: Resolution bandwidth
SARPs: Standards and Recommended Practices (SARPs)
UUT: Unit under test
WiMAX: Worldwide interoperability for microwave access

A.3 DEFINITION OF THE SPECTRAL EMISSION MASK AND THE ZERO dB REFERENCE

A.3.1 The power spectral density of the emissions when all active sub carriers are transmitted in the channel should be attenuated below the maximum power spectral density as follows:

a) on any frequency removed from the assigned frequency between 50 – 55 per cent of the authorized bandwidth: 26 + 145 log (per cent of BW/50) dB;

b) on any frequency removed from the assigned frequency between 55 – 100 per cent of the authorized bandwidth: 32 + 31 log (per cent of (BW)/55) dB;

c) on any frequency removed from the assigned frequency between 100 – 150 per cent of the authorized bandwidth: 40 +57 log (per cent of (BW)/100) dB; and

d) on any frequency removed from the assigned frequency beyond 150 per cent of the authorized bandwidth: 50 dB.

Note.— The power spectral density at a given frequency is the power within a bandwidth equal to a 100 kHz centred at this frequency, divided by this measurement bandwidth. Further, the measurement of the power spectral density should encompass the energy over at least one frame period.

A.3.2 The zero dB reference of the spectral mask should be the peak power spectral density in the assigned channel bandwidth of 5 MHz.

A.4 TEST SETUP

A.4.1 The test setup below is considered for the spectral mask test. Figures 72 and 73 show examples of a BS/MS testing setup.

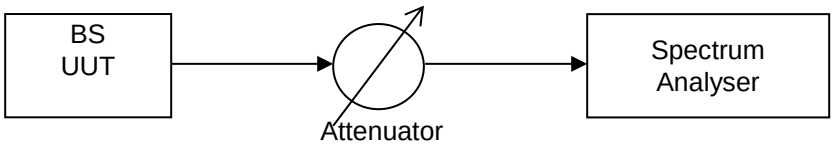


Figure 72. BS test setup

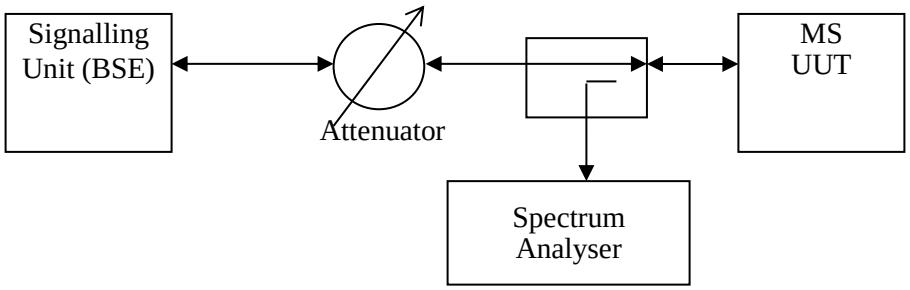


Figure 72. SS test setup

A.4.2 **Test procedure**

A.4.2.1 *Initialization*

a) Set up the test environment for the UUT; and

b) configure the spectrum analyser in accordance with Table 44.

Note.— Although the resolution bandwidth (RBW) is set to 100 kHz, the RBW can be set to 10 kHz or a value smaller than 100 kHz to improve measurement accuracy for a narrow region where the variation of the power is large, such as a) range defined in paragraph A3.

Items	RBW=100kHz	RBW=10kHz
Centre frequency	Centre frequency of UUT.	Centre frequency of UUT.
Span	25 MHz	25 MHz
Resolution bandwidth	100 kHz	10 kHz
Video bandwidth	100 kHz	10 kHz
Sweep time	All the measurement of the power spectral density should encompass the energy over at least one frame period.	All the measurement of the power spectral density should encompass the energy over at least one frame period.
Detector	Positive Peak	Positive Peak

Table 44. Conditions for spectrum analyzer

c) turn UUT power on; and

d) set a frequency to UUT.

A.4.2.2 *Test procedure*

Step P-1. Transmit signal using all active subcarriers at maximum power.

Step P-2. Start to sweep the transmit power on the spectrum analyzer.

Step P-3. Save the sweeping data as the test result.

Step P-4. Take the peak value of the test result as 0 dB reference.

Step P-5. Align the top of the spectral mask to 0 dB reference and compare the spectral mask and the test result.

Step P-6. Repeat Step P-1 through P-5 at least for low, mid and high frequencies supported by the UUT.

Step P-7. End of test.

A.4.2.3 *Compliance requirements*

A.4.2.3.1 Pass verdict:

At all frequencies, test result read in P-5 is not higher than the spectral mask.

A.4.2.3.2 Fail verdict:

At any frequencies, test result read in P-5 is higher the spectral mask.

A.4.3 **Supplemental information**

In ITU-R [1] the procedures is described the following:

Annex 2: Methods of measurement of spurious domain emissions, 1.1.2 Resolution bandwidths.

A.4.3.1 As a general guideline, the resolution bandwidths (measured at the -3 dB points of the final IF filter) of the measuring receiver should be equal to the reference bandwidths as given in recommendations in 3.1. To improve measurement accuracy, sensitivity and efficiency, the resolution bandwidth can be different from the reference bandwidth. For instance, narrower resolution bandwidth is sometimes necessary for emissions close to the centre frequency. When the resolution bandwidth is smaller than the reference bandwidth, the result should be integrated over the reference bandwidth (the integration should be made on the basis of a power sum unless the spurious signal is known to be additive in voltage or with intermediate law).

A.4.3.2 RBW is the equivalent bandwidth to that of the IF filter the spectrum analyzer is equipped with. Due to the characteristics of the IF filter, the signal (power) outside the band may be detected and displayed as a spectrum. In order to reduce this undesired detection, it is necessary to narrow the RBW and thus increase the frequency resolution. However, too narrow a RBW will lead to an excessively long sweep time, so it is necessary to pay sufficient attention to this.

A.4.3.3 When measuring signals with steep spectral curves such as OFDM, failure to use sufficient frequency resolution will incur considerable stretching to the spectrum contour.

A.4.3.4 More specifically, even when the RBW is configured to 100 kHz, the power beyond 100 kHz can pass through depending on filter characteristics, as a result the power beyond 100 kHz is also undesirably integrated and reflected in the test result. (Figure 73).

A.4.3.5 In order to mitigate the impact from filter characteristics and improve the measurement accuracy in those areas with steep spectrum, it is preferable to set the RBW narrower, according to the stipulations of the ITU-R.

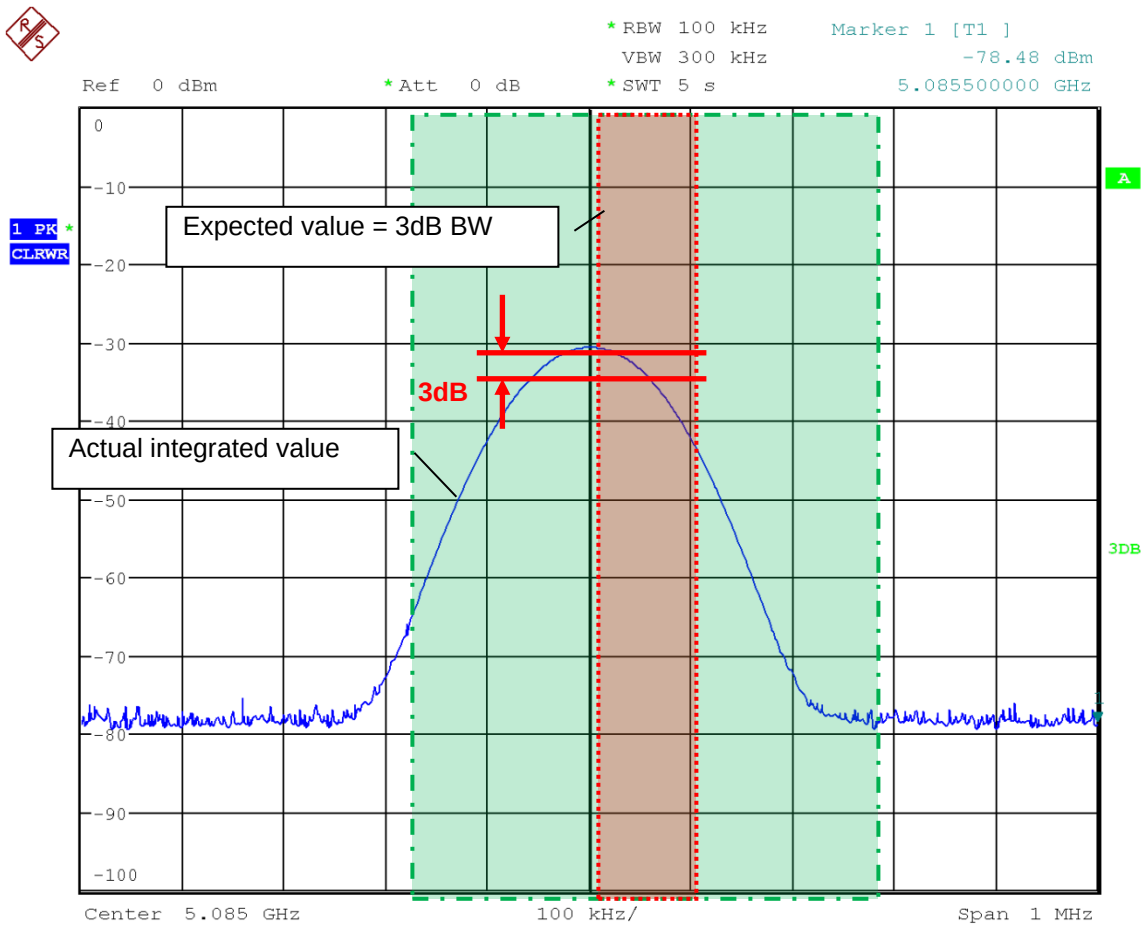


Figure 73. Filter frequency response

A.4.3.6 Moreover, since the subcarrier interval for AeroMACS is defined as 10.94 kHz, a RBW of 10 kHz can make the measurement accurate enough in terms of frequency domain; however, after the RBW is reduced, captured data needs to be integrated over 100 kHz. It is also necessary to properly increase the measuring period to avoid loss of opportunities for detecting peaks due to the reduction of the RBW.

— END —