ARINC

INTERNETWORKING SPECIFICATION

ARINC SPECIFICATION 637

PUBLISHED: SEPTEMBER 6, 1993

AN ARINC DOCUMENT

Prepared by
AIRLINES ELECTRONIC ENGINEERING COMMITTEE
Published by
AERONAUTICAL RADIO, INC.
2551 RIVA ROAD, ANNAPOLIS, MARYLAND 21401

ARINC SPECIFICATION 637©

INTERNETWORKING SPECIFICATION

Published: September 6, 1993

Prepared by the Airlines Electronic Engineering Committee

Specification 637 Adopted by the Airlines Electronic Engineering Committee: June 4, 1993

Specification 637 Adopted by the Industry: July 20, 1993

FOREWORD

Activities of AERONAUTICAL RADIO, INC. (ARINC)

and the

Purpose of ARINC Reports and Specifications

Aeronautical Radio, Inc. is a corporation in which the United States scheduled airlines are the principal stockholders. Other stockholders include a variety of other air transport companies, aircraft manufacturers and foreign flag airlines.

Activities of ARINC include the operation of an extensive system of domestic and overseas aeronautical land radio stations, the fulfillment of systems requirements to accomplish ground and airborne compatibility, the allocation and assignment of frequencies to meet those needs, the coordination incident to standard airborne communications and electronics systems and the exchange of technical information. ARINC sponsors the Airlines Electronic Engineering Committee (AEEC), composed of airline technical personnel. The AEEC formulates standards for electronic equipment and systems for airlines. The establishment of Equipment Characteristics is a principal function of this Committee.

It is desirable to reference certain general ARINC Specifications or Reports which are applicable to more than one type of equipment. These general Specifications or Reports may be considered as supplementary to the Equipment Characteristics in which they are referenced. They are intended to set forth the desires of the airlines pertaining to components or equipment is concerned.

An ARINC Report (Specification or Characteristic) has a twofold purpose which is:

(1) To indicate to the prospective manufacturers of airline electronic equipment the considered opinion of the airline technical people coordinated on an industry basis concerning requisites of new equipment, and

(2) To channel new equipment designed in a direction which can result in the maximum possible standardization of those physical and electrical characteristics which influence interchangeability of equipment without seriously hampering engineering initiative.

ARINC SPECIFICATION 637
TABLE OF CONTENTS

ARINC SPECIFICATION 637
TABLE OF CONTENTS

ARINC SPECIFICATION 637
TABLE OF CONTENTS

ARINC SPECIFICATION 637
TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose

The intent of this document is to provide general and specific design guidance for the development and installation of the Network layer protocols and services needed to route and relay bit-oriented air-ground data link messages in an Open Systems Interconnection (OSI) environment. The protocols and services defined herein are consistent with those used in the Aeronautical Telecommunication Network (ATN).

COMMENTARY

CAUTION! This document was presented for adoption with the intention of providing a basis for initial airborne router prototype iplementations. The material contained herein is not considered complete because it may not be adequate to ensure interoperability of production systems. Further change and expansion is envisioned as tests of actual systems go forward.

1.2 Scope

This document is primarily concerned with those protocols and services that define the Network Layer. This document describes the communication functions that should be performed by the aircraft avionics to successfully transfer messages using standard OSI protocols. Messages processed by avionics will be transferred:

- from avionics to ground systems
- from ground systems to avionics
- within the aircraft.

1.3 Background

Communications across the air-ground link have traditionally been performed by using the Aircraft Communication Addressing and Reporting System (ACARS). The ACARS air-ground system description was initially included in ARINC Characteristic 597. It was later transferred to ARINC Specification 618.

The air-ground data communication functions described herein are compatible with the OSI Model. They were developed as the first step toward a fully OSI compliant protocol "suite". These protocols may be installed in an Aircraft Communications Addressing and Reporting System (ACARS) Management Unit (MU), in a Communications Management Unit (CMU) onboard the aircraft, or in any End System or Intermediate System (IS) onboard the aircraft.

The capability to accept and transfer code and byte independent messages is provided in lieu of, rather than in addition to, the processing of original ACARS messages in character-oriented format.

COMMENTARY

Passing the traditional full ACARS protocol/data formats over an OSI communications system is not a desired end. There are numerous benefits to be gained from data communications using the OSI model. The discussion and evaluation of those benefits is beyond the scope of this document.

A significant inventory of equipment, both in the airplane and on the ground, will continue to operate using ACARS. These equipments, and the related processes administered by ground service providers and airline host computers needed to enable them to operate, should continue to be supported for the foreseeable future. A migration path should be constructed between current data communication methods (ACARS) and the desired goal of communicating in an ATN environment. By providing an OSI-compatible data communications system, current data formats can continue to be supported by the same communication system that supports OSI-compatible applications. The level of OSI (bit-oriented) and non-OSI (character-oriented) message activity will then be determined by the marketplace.

1.4 Network Layer Model Overview

This section provides a general discussion on aspects of the Network layer.

Layer three of the OSI model is the Network Layer. The Network Layer provides a uniform service interface for the transfer of Network User data among End Systems (ES) and Intermediate Systems (IS) conforming to the ISO OSI Network layer architecture. The OSI Network layer provides routing and relaying services via available subnetworks and data links. The Network layer operates ES to IS and IS to IS. The Network layer isolates the way in which underlying resources (e.g., data link services) are utilized from the Network service user, which is typically the transport layer.

An ES consists of at least the Transport Layer plus lower layers and one or more application processes (i.e., users of the OSI services). An ES is addressed by an NSAP. An ES is the lowest level of granularity identified by an NSAP. An Application Process is the ultimate originator and/or destination of an OSI message.

An IS consists of the Network layer and below, where the Network layer includes the Subnetwork Independent Convergence Protocol (SNICP) sublayer of the Network layer. An IS performs routing and relaying functions.

The Network layer is often internally organized into three sublayers as depicted in ISO 8648:

- Subnetwork Access Protocol (SNAcP) Sublayer
- Subnetwork Dependent Convergence Protocol (SNDCP) sublayer
- Subnetwork Independent Convergence Protocol (SNICP) sublayer (which includes the routing information exchange functions and the Internetworking or routing and relaying functions).

Each of these sublayers have a service and protocol definition. Figure 1-3 of Attachment 1 depicts the general Network layer organization.

1.0 INTRODUCTION (cont'd)

1.4.1 Subnetwork Access

The subnetwork environment consists of the Physical Layer, Data Link Layer and Subnetwork Access sublayer protocols. Different subnetworks can implement different Subnetwork Access protocols and convergence functions to fit each environment.

The Subnetwork Access sublayer is an optional part of the Network layer which defines the access to the subnetwork between routers or End Systems. For example, there is a Subnetwork Access sublayer for ISO 8208 subnetworks in the Network layer. The Subnetwork Access sublayer provides services to the SNDCF sublayer and utilizes the services of the data link layer. At times there is no Subnetwork Access sublayer, because the Internetwork sublayer operates directly over an SNDCF for the data link layer (e.g., Internetwork sublayer operating over an IEEE 802 Local Area Network).

Routers accessing air-ground subnetworks, such as SATCOM, Mode-S, and AVPAC, require a Subnetwork Access sublayer. Current air-ground Subnetwork Access sublayers are specified based on the ISO 8348/ISO 8208 connection oriented network. ISO 8348 specifies the connection oriented Network service, which defines:

- Connection establishment and termination
- Each connection's quality of service
- Data transfer subject to flow control
- Expedited data transfer subject to different flow control
- Reset capability
- Acknowledgement

ISO 8208 "X.25 Packet Level Protocol for Data Terminal Equipment" specifies a connection oriented Network layer protocol. The services specified by ISO 8348 are provided by the ISO 8208 protocol. In order to use ISO 8208 as a Subnetwork Access protocol, ISO 8208 options are selected based on the properties of the subnetwork.

Air/ground subnetworks provide an interface between two or more BISs on the aircraft and between a BIS on the aircraft and routers on the ground. The Subnetwork Dependant Convergent Function (SNDCF) sublayers for avionics subnetworks are defined in Section 6.4. See Figure 1-1 of Attachment 1.

This specification is limited to the Connectionless Network Service, Routing Information Exchange Protocols and the necessary convergence functions and protocols to access real subnetworks. The Subnetwork Convergence Sublayer uses the protocol identification value to deliver NPDUs to the protocols in the Internetwork sublayer.

COMMENTARY

This document does not contain specifications for the SNAcP sublayer.

1.4.2 Subnetwork Dependent Convergent Function (SNDCF)

The SNDCF sublayer converges the Internetworking protocol into the Subnetwork Access protocol. SNDCF provides the interface between incompatible Internetworking and Subnetwork Access protocols. For example, ISO 8473 specifies a SNDCF for converging between an ISO 8473 Internetwork sublayer and a ISO 8208 subnetwork. It should be noted that the SNDCF sublayer may not be utilized for some subnetworks (e.g., a Subnetwork Access sublayer is not required). The SNDCF sublayer provides services to the Internetwork sublayer and utilizes the services of the Subnetwork Access sublayer. ARINC Specification 637 specifies the SNDCF sublayer for each subnetwork within the avionics. See Figure 1-2 of Attachment 1.

1.4.3 Subnetwork Independent Convergence Protocol (SNICP) Sublayer

The SNICP sublayer is responsible for performing data transfer, relaying, and routing functions across subnetworks connected to avionic ISs and ESs. The internetwork sublayer is independent of the underlying subnetworks. ISO 8473 defines the main component of the internetwork sublayer (with support from routing information exchange protocols appropriate for the system component). See Figure 1-2 of Attachment 1.

The Internetwork sublayer performs the Router functions. It uses routing information exchange services to obtain necessary information from adjacent Routers or ESs in order to build dynamic routing information databases. The routing information databases are used to perform the Routing function and the Network Protocol Data Unit (NPDU) build functions. ES-IS routing information exchange is utilized when routing information is being exchanged between the end-system and the Router. IS-IS Router information exchange is utilized when routing information is being exchanged between adjacent Routers.

A router performs routing and relaying functions. At the Internetwork sublayer, the router directs a message via the appropriate subnetwork according to the message's Network Service Access Point (NSAP) address when routing to an end-system external or internal to the router unit. Routing to external ESs is performed either directly over a subnetwork to a destination ES or over a subnetwork to another router which has direct or indirect access to the destination ES.

This document specifies the Internetwork sublayer for the ATN domain. The Internetwork sublayer provides services to the Transport layer and utilizes the services of the: SNDCF sublayer, Subnetwork Access sublayer, or Data Link Layer (depending on the underlying service).

1.5 Document Overview

An overview/preview of this document, ARINC Specification 637, "Internetworking Specification" is provided in this section. Chapter 2 describes the addressing structure to be used by End Systems and Intermediate Systems within the ATN. The ATN Network layer model defines several subfunctions. Based on these logical subfunctions, Chapters 3-6 describe provisions applicable to avionics systems operating within the ATN environment. Each of these chapters are further organized into subsections to define the services and

1.0 INTRODUCTION (cont'd)

protocols of these subfunctions. Specifically, the logical subfunctions of the Internetworking Specification include:

- The ATN NSAP Definition and Addressing Plan
- The Internetworking Services and Protocol (ISO 8473)
- The ES_IS Protocol Specification (ISO 9542)
- The Inter-Domain Routing Protocol (ISO 10747, IDRP)
- SNDC Requirements
- Internal Router Initialization Functions

Guidance concerning the necessary Network Layer Management Information Base (MIB) is provided in Appendix A.

The protocol used in the subnetwork environment across an air-ground "subnetwork" or any other subnetwork in the ATN domain is referred to formally as a Subnetwork Access Protocol (SNAcP). This will be referred to within this document as the "Subnetwork Protocol". The SNAcP specification for a particular subnetwork is in the corresponding ARINC standard, such as ARINC Characteristic 741 for SATCOM.

The Network layer also contains a common Internetwork protocol or, formally, a Subnetwork Independent Convergence Protocol (SNICP). This Internetwork protocol allows Network layer service to be provided across potentially many subnetworks and allows these subnetworks to support an infrastructure to provide a common Internetwork service to the Network service user or Transport Layer. When distinguishing between more generic Internetwork Protocols (IP) this may also be referred to as the ATN ConnectionLess Network Protocol (CLNP). The SNDCF is a mapping function which is required to map between the Subnetwork protocol and the ATN IP. The subnetwork protocol is outside the scope of this specification.

ISs should support two routing information exchange protocols, as well as the two Subnetwork Convergence services (SNDCF and SNDCP). An ES in the subnetwork, that does not support the full internetworking router function, only requires the CLNP and ES-IS Protocol within its Internetwork sublayer. An ES should also be capable of supporting the appropriate convergence function for mapping primitives to the SNAcP.

Subnetwork user data is passed from the Internetwork sublayer to the SNDCF. Subnetwork Convergence user data is passed from the SNDCF to the internetwork sublayer.

The protocol data unit (PDU) which is produced by the SNICP for dissemination across the ATN Internetwork is referred to as the NPDU.

The following subsections provide an overview of the corresponding sections within ARINC Specification 637 on indicated Network layer subfunctions as well as the NSAP Addressing Plan.

1.5.1 NSAP Addressing Plan

Chapter 2 of this specification describes the NSAP addressing plan for the ATN domain as it applies to airborne systems. An ATN NSAP identifies an ATN End System (ES). An ATN End System may have more than one NSAP address. Normally, each ATN NSAP uniquely identifies a physical unit, such as the left Flight Management Computer (FMC), on a particular airplane.

NSAP addresses are physical in nature. For specialized needs, such as redundant systems, mechanisms can be used to address an End System function without identifying its physical location. Application Entity Titles and upper layer selectors aid this process. See ARINC Specification 638.

An IS should be capable of routing messages according to the NSAP address. The IS passes messages on through the appropriate subnetwork according to the NSAP, when the NSAP addressed end-system resides external to the router. ISs route messages destined for avionics ESs via the appropriate avionics subnetwork or LAN. ISs route messages destined for ground host ESs via the appropriate air-ground subnetwork. In addition, when the NSAP addressed end-system resides internal to the router, the router passes the message on to the appropriate Network layer user (e.g., Transport Layer) through that NSAP.

1.5.2 Internetworking

The CLNP and service definition are specified in Chapter 3 of this document. The CLNP conforms with the ISO Connectionless Internetwork Protocol (ISO IP) as specified by ISO 8473. It is a basic protocol which can be utilized over all subnetworks to provide a common Network layer service to all End Systems and Intermediate Systems throughout the ATN domain.

The Internetworking service definition is intended to conform to the Network Service Definition (ISO 8348), Addendum 1: Connectionless Mode Transmission (ISO 8348 AD 1), and Addendum 2: Network Layer Addressing (ISO 8348 AD 2). If there are any differences between this specification and the cited documents, then this document shall have precedence.

ISO 8473 is a standard with many optional features. It is the intention of chapter 3 to fully specify the ISO 8473 protocol options to conform with other documents which specify the ATN interworking and functions. Chapter 3 is intended to summarize the optional functions, QOS parameters and the negotiation of optional functions required for the use of ISO 8473 for the air-ground context. ISO 8473 exists in both ESs and ISs. The optional and mandatory functions within ISO 8473, selected for the air-ground context, are intended to simplify the protocol state machine in general.

ISO 8348/Addendum 1 specifies the connection-less Network service. The parameters in the basic service primitive include source and destination NSAP address, quality of service (transit delay, protection, cost determinants, priority, source routing, and residual error probability), and user data. These parameters are supported by ISO 8473 protocol.

The Internetwork sublayer uses routing information exchange between peers to obtain the necessary

1.0 INTRODUCTION (cont'd)

1.5.2 Internetworking (cont'd)

information to build CLNP packets and to appropriately route CLNP packets. If convergence to a Subnetwork Access sublayer is required, then the Internetwork sublayer operates over a SNDCF.

1.5.3 Routing Information Exchange

One of the functions of the Network layer is to provide Routing Information Exchange. Routing protocols allow this dynamic exchange and maintain local data bases which contain the routing information. These data bases are accessible by the CLNP while performing the routing and relaying function. In this way, the onward relay of NPDUs can be accomplished based on current information.

ISO 9542 is the protocol used to provide ES-IS routing information exchange. ISO 9542 also updates the local Forwarding Information Base. This information is then passed to the IS-IS routing protocol. The ES-IS routing information exchange function is specified in Chapter 4.

The inter-domain protocol ISO 10747 (IDRP) is utilized to provide the IS-IS routing information exchange function. The Link State Database and the Forwarding Database are maintained to support the routing function. These routing protocols allow the dynamic exchange of routing information at the Network layer. Routing protocols maintain local data bases which contain the dynamic routing information.

COMMENTARY

Routing and relaying is provided in order to allow ESs and ISs to find an appropriate path between two or more ESs for a given instance of communications. Relaying is concerned primarily with the actual transformation and manipulation of NPDUs as they transit ISs. Routing is primarily concerned with the maintenance and selection of paths through multiple subnetworks and ISs which allow NPDUs to flow smoothly between communicating ESs.

The IDRP routing information exchange function is specified in Chapter 5.0.

COMMENTARY

ISO 9542 is defined for use in exchange of routing configuration information and is used in conjunction with both the inter-domain routing protocol IDRP (ISO 10747) and the Internetworking protocol, ISO 8473.

Routing databases are utilized to perform the routing functions. There are two classes of routing databases identified:

- Dynamic Routing Information Database
- Policy Database.

The Dynamic Routing Information Databases dynamically maintain relevant information obtained by using ISO 9542 and IDRP routing information exchange services. The information collected in these databases include relevant information about adjacent Boundary Intermediate Systems (BIS) and ESs. These databases include the link state and local forwarding databases discussed earlier.

The Policy database indicates routing preferences for particular messages based on either quality of service (QOS) requirements such as cost and throughput (i.e., to indicate preference based on customer policy for a particular subnetwork) or policy preferences. For example, preference of the Mode-S subnetwork for FAA related messages could be indicated as part of this policy data base.

1.5.4 Network Layer Management Information Base (MIB)

Introductory guidance material concerning the Network Layer MIB can be found in Appendix A.

1.5.5 Avionics and Air-Ground SNDCF

The SNDCF sublayer needs to be defined for each identified subnetwork type. This includes the SATCOM, AVPAC, Mode-S, and avionics end-system subnetworks. The air-ground SNDCFs converge the Internetworking protocol (i.e., ISO 8473) into the Subnetwork Access protocol (i.e., ISO 8208) as appropriate for each particular air-ground subnetwork. The SNDCF sublayer is identical for each of the currently defined air-ground subnetworks.

In order to accommodate Internetworking services in a low overhead manner, two functions are required for implementation between the CLNP and the Subnetwork Access Protocol. The SNDCP is responsible for compression and decompression of the CLNP header to achieve improved efficiency over the air-ground subnetworks. A SNDCF is also responsible for the mapping of service primitives between the CLNP protocol and on-board aircraft subnetworks.

The air-ground and avionics SNDCF sublayers are specified in the protocol specification associated with each sublayer medium. The conventions used for the service definitions at the top and bottom of the SNDCF are drawn from ISO 8348, ISO 8348/AD1 and ISO 8473. The Network layer service definition in Chapter 3 acts as the guideline for notation and requirements of the SNDCF.

1.6 Relationship of this Document to Other Standards

1.6.1 Relationship of this Document to ARINC Characteristics and Specifications

The provision defined in this Specification may be incorporated in any appropriate avionics equipment by reference. ARINC Characteristics that describe the physical hardware which are candidates to incorporate the ATN router function defined herein include Characteristics 724, 724B and 748.

ARINC Characteristic 748 describes the Communications Management Unit (CMU), which has prime responsibility for routing bit-oriented air-ground data messages within the ATN. It may do so for messages which cross a variety of media from the aircraft to the ground.

1.0 INTRODUCTION (cont'd)

COMMENTARY

New aircraft will be equipped with communications architectures designed to operate within the ATN. The CMU described in ARINC Characteristic 748 will house the protocols described in Chapters 2 through 6 of this Specification. The CMU may also support gateway functionality for interfacing with non-OSI peripherals.

Upper layer protocols (Transport, Session, Presentation and Application Layer) and their definitions for use in avionics are described in ARINC Specification 638. This ARINC specification can support the ISO 8073 Connection Oriented Transport Protocol or ISO 8602 Connectionless Mode Transport Protocol in accordance with AEEC Specification 638, when the Network Service User is the Transport Service. Any other users of the Network Service should use the primitives and parameters of ISO 8473.

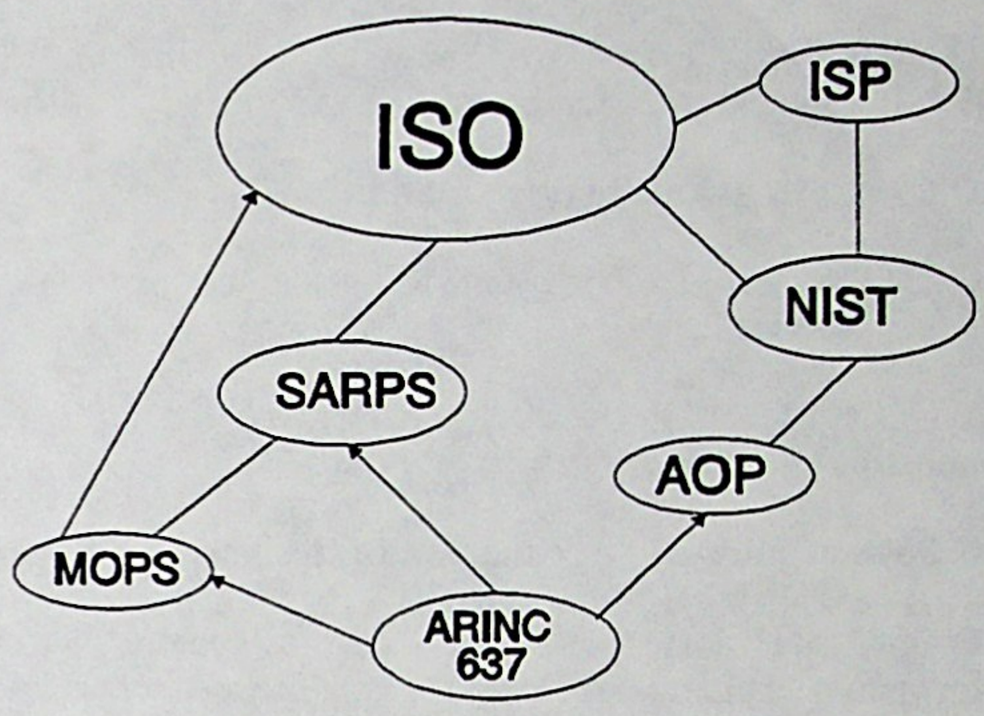


Figure 1.6.2-1
Relationship of Standards

1.6.2 Relationship to Other Standards

This specification is designed to be used in conjunction with other industry standards to ensure uniform implementation such that interoperability of systems and networks is achieved.

This specification defines the protocols and functions of the ATN Network Layer from an avionics point of view. Because of the requirement for conformance and interoperability with the remainder of the ATN, the avionics specifications should be subservient to the higher-level specifications for the overall ATN.
These higher-level specifications are the pertinent ICAO Standards and Recommended Practices (SARPS), the RTCA Mimimum Operational Performance Standards (MOPS), and the ATA/IATA Aeronautical OSI Profiles (AOP), in descending order of priority.

Therefore, this specification defines only those items which are unique to the avionics and provides a general description of the remainder of the ATN requirements to give an overall understanding of the context of the avionics-unique requirements. Where differences or inconsistencies between this specification and the above named high-level specifications occur which would cause interoperability problems, the high-level specifications will prevail. Some of the documents and their respective originating agencies are illustrated in the figure below.

This document is based on: ISO 8473, ISO 8348 AD 2, ISO 9542, ISO 10747 and other ISO standards referenced in Section 1.8. This specification delineates the implementation of these international standard protocols as interpreted to best serve the air transport industry. There is no intent to violate any provision of these standards, however, some provisions may be unused while other permitted variations may be defined herein.

The (AOP) is a standards document that defines the protocol architecture for conducting ground-ground data communications within the ATN. The AOP also specifies the profiles within these ISO standards.

1.7 Regulatory Approval

The equipment should meet all applicable FAA and FC C regulatory requirements. This document does not and cannot set forth the specific requirements that an equipment should meet to be assured of approval. Such information should be obtained from the regulatory agencies themselves.

1.8 Documents Referenced

This specification references the following documents:

AEEC Specification 631, "Avionics VHF Packet Communications (AVPAC)"

AEEC ARINC Specification 638, "Upper Layer Specification (End System Communications Specifications)"

AEEC ARINC Characteristic 750, "VHF Data Radio"

ARINC Characteristic 748, "Communications Management Unit (CMU)"

ARINC Characteristic 724, "Mark 2 Aircraft Communications Addressing System"

ARINC Characteristic 724B, "Aircraft Communications Addressing System (ACARS)"

ARINC Characteristic 741, "Aviation Satellite Communications System"

ATA/IATA Aeronautical OSI Profile (AOP), Version 1.1.2

Government Open Systems Interconnection Profile (GOSIP), Version 2, October, 1990

ISO 8208, "X.25 Packet Level Protocol for Data Terminal Equipment"

1.0 INTRODUCTION (cont'd)

1.8 Documents Referenced (cont'd)

ISO 8072, "Transport Service Definition"ISO 8073,"Connection Oriented Transport Protocol Specification"
ISO 8348, "Network Service Definition"

ISO 8473, "Protocol for providing the connectionless network service"

ISO 8602, "Protocol for providing the connectionless-mode transport service"

ISO 8648, "Internal Organization of the Network Layer"

ISO 9542, "End system to Intermediate system routing information exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service"

ISO/IEC TR 9575, "Information Technology - Telecommunications and Information Exchange Between systems - OSI Routing Framework"

ISO IEC 10747, "Information Processing Systems - Telecommunications and Information Exchange between Systems - Protocol for Exchange of Inter-domain Routing Information among Intermediate systems to support Forwarding of ISO 8473 PDUs."

IEEE 802, "Local Area Networks"

CCITT X.25, "Interface Between Data Terminal Equipment (DTE) and Data Circuit Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuits"

RTCA DO-205, "Design Guidelines and Recommended Standards to Support Open Systems Interconnection for Aeronautical Mobile Digital Communications"

NIST/OIW "Stable Implementors Agreements", Version 4

2.0 INTERNETWORK ADDRESSING

2.1 Network Service Access Points and Network Entity Titles

Network Service Access Points (NSAP) and Network Entity Titles (NET) are described in ISO 8348 AD 2.

2.2 ATN Network Addressing Information

NSAP addresses are constructed so that they uniquely identify end to end correspondence between communicating systems using the Network Service. The definition and formatting of NSAP addresses for use in the ATN is summarized below and contained in Attachment 2. ATN NETs comprise the portion of the ATN NSAP up to but not including the Selector Value (SEL) field. An ATN NET uniquely addresses a Network Entity and does not address anything above the Network layer. In contrast, an ATN NSAP uniquely addresses a Network Service user which is by definition above the Network layer.

2.2.1 ATN NSAP Addressing

ISO 8348 AD 2 defines the abstract syntax and semantics of the Network address. It does not specify the way in which the semantics are encoded in Network layer protocols. This document provides detailed information for the implementation of an NSAP addressing plan.

This document is intended to be in agreement with other aeronautical standards and authoritative documents including the ATN Proposed Standards and Recommended Practices (SARPS) and the ATA/IATA Aeronautical OSI Profile (AOP). This document is intended to be implemented with the upper layer address resolution details defined in AEEC Project Paper 638. The Network Layer address syntax and semantics as specified in both this document and AEEC Project Paper 638, shall be utilized by end-users and service providers participating in the world-wide aeronautical OSI data networking environment.

COMMENTARY

The plan defined herein is not intended to preclude connectivity to ground end systems using NSAP values not encoded as specified below.

The NSAP addressing space defined below works in conjunction with the TSAP/upper-layer selector (as defined in AEEC project Paper 638) in order to fulfill the following addressing functions:

- The NSAP addresses provide unambiguous identification of end-systems (ESs).
- The NSAP address syntax and semantics support efficient network layer routing.
- The NSAP address and TSAP/upper-layer selector syntax and semantics ensure the efficient delegation of address/selector administration.
- The NSAP addresses are structured and administered to ensure support for the ISO Routing Framework (ISO TR 9575) and the AOP.

This document defines an NSAP address space containing an International Code Designator (ICD) format Domain Specific Part (DSP) using binary DSP syntaxes as well as a hierarchical, name-based Network layer address format. The structure of the NSAP is given in Figure 2-1 of Attachment 2.

The Routing Domain Identifier (RDI) portion of the ATN NSAP address is jointly administered by ICAO and IATA. Alignment between the assignments made by IATA and ICAO is maintained to preserve the integrity of ATN internetworking. ATN NSAP semantics (i.e. field content and interpretation) are defined and administered by IATA and ICAO. Re-delegation of this authority may be made by their respective sub-authorities.

This document describes network address semantics as specified in the sections below.

2.2.1.1 Initial Domain Part (IDP)

The Initial Domain Part (IDP) is the initial field of any NSAP which contains the Authority and Format Identifier (AFI) and Initial Domain Indicator (IDI) as specified in ISO 8348 AD 2. Specific AFI and IDI values for the ATN NSAP are listed below.

2.2.1.1.1 Authority and Format Identifier (AFI)

This field specifies the authority responsible for allocating values for the IDI field, and the abstract syntax representation (binary or decimal, etc.) used for the Domain Specific Part of the NSAP as a whole.

The AFI value for an ATN NSAP shall be "47" encoded as a two digit Binary Coded Decimal (BCD) value as defined in ISO 8348 AD 2 to imply: (1) that the IDI consists of a 4 digit ICD allocated according to ISO 6523, and (2) that the DSP syntax is binary.

2.2.1.1.2 Initial Domain Indicator (IDI)

This field specifies the abstract syntax and semantics of the DSP portion of the ATN NSAP address. This field contains the value "0027" for all ATN NSAP addresses.

2.2.1.2 Domain Specific Part (DSP)

The Domain Specific Part (DSP) of NSAP addresses specified by this document consist of the following seven fields.

2.2.1.2.1 Version (VER)

The version (VER) field has a binary value of "01" to define the field and format definition of the ATN NSAP format. Future versions of ATN NSAP may use other version values.

2.2.1.2.2 Administrative Identifier (ADM)

The administrative identifier field specifies the organizational authority responsible for administration of an "ATN area". It is an IA-5 encoded ADM value.

COMMENTARY

Differentiation between ICAO and IATA domains is accomplished solely based on the value of the ADM

2.0 INTERNETWORK ADDRESSING (cont'd)

2.2.1.2.2 Administrative Identifier (ADM) (cont'd)

field. The ADM allotment will be divided among IATA members and ICAO states in the following manner:

IATA Domains:

IATA may assign any IATA member a three-character ADM value that begins with the upper-case alphabetic character "A" through "Z" inclusive, or that begins with the numeric character "0" through "9" inclusive; e.g. an IA-5 encoded field. The latter two characters of the three character ADM value are unconstrained. The intent of this format is to allow the encapsulation of the three-character IATA organization identifiers within the ADM abstract syntax in a manner that does not interfere with the ICAO syntax proposed below and which allows some degree of growth.

Avionics designed for air-transport airplanes will use the three-letter IATA Airline Designator as specified in the IATA Airline Coding Directory.

ICAO Domains:

ICAO may assign any ICAO state a three-character ADM value that begins with the IA-5 character "@", or that begins with any other IA-5 character whose octet encoded value is between the unsigned hexadecimal integer "60" and the unsigned hexadecimal integer "7f", inclusive. The intent of this clause is to allow encapsulation of two-character ISO 3166 alphabetic country codes within the ADM abstract syntax in a manner that does not interfere with the IATA syntax proposed above, and which allows some degree of growth. This also allows ICAO use of the three character ISO 3166 country codes, represented in abstract syntax as lower-case alphabetic characters, if desired.

All other values of the first octet of the ADM field are reserved for future growth, and are administered by ICAO.

2.2.1.2.3 Routing Domain Format (RDF)

The Routing Domain Format (RDF) identifies groups of routing domains. The RDF field contains a two digit hexadecimal value. For aircraft systems the 1 octet hexadecimal value is "81". For non-aircraft systems the hexadecimal value is "01".

2.2.1.2.4 Area Routing Selector (ARS)

The Area Routing Selector (ARS) field is provided to allow the further partitioning of the address space administered by a single ATN administrative domain authority into more than one subdomain. The ARS field shall contain a 3-octet binary code for an ATN domain partition. The ARS field contains a 24-bit ICAO aircraft identifier for aircraft.

For non-aircraft systems, the 3 octet ARS field contains a routing domain identification number assigned by the airline or ICAO State administration responsible for the system operation. If not specified by the organization denoted in the ADM field, this field will carry the hexadecimal value "000001".

2.2.1.2.5 Location Identifier (LOC)

The Location Identifier (LOC) field in the ATN NSAP address structure represents a routing subdomain referred to as an Area. An Area subdomain maintains detailed routing information about it's own composition and also maintains information which allows it to reach other areas within the routing domain.

For onboard avionics networks the LOC field can be used to decompose the Routing Domain (identified by the RDI) into multiple Areas. The decomposition of the routing domain into Areas may be used to simplify intra-domain routing within the airplane.

COMMENTARY

IATA Location Identifiers can be encoded as Base 37 alphanumeric values in the LOC field at the discretion of the Administrative Domain Authority specified by the ADM field. See Table 2.4 of Attachment 2.

2.2.1.2.6 System Identifier (SYS)

The System Identifier (SYS) portion of the NSAP address is a 6 octet field which uniquely and unambiguously identifies the avionics end-system (within the Area sub-routing domain) which contains the network entity identified by the NSAP address. It is the responsibility of the authority designated in the ADM field of the NSAP address to administer this field so as to meet this requirement. This specification does not otherwise constrain the format and content of this field. However, guidance on how this field might be administered is provided in Appendix TBD.

2.2.1.3 Selector Value (SEL)

The Selector Value (SEL) field identifies the ES Network Service User Process responsible for originating or receiving Network Service Data Units (NSDUs). This field contains a two digit hexadecimal representation of a Transport Layer entity protocol selector. While this field is intended to identify a specific Transport Layer protocol and some of the values are defined by GOSIP, this field can be used to describe any Network Service User using a value assigned by the ADM authority.

Current ISO SEL values which are assigned are:

"00"	Reserved Code
"01"	ISO 8073 Connection Oriented Transport Protocol
"02"	ISO 8602 Connectionless Transport Protocol
"03-ff"	Reserved Codes

3.0 INTERNETWORKING SERVICE AND PROTOCOL

3.1 Introduction

ISO 8473 is the protocol specification for providing the ConnectionLess-mode Network service Protocol (CLNP). The term Internetworking Protocol (IP) may also be used where the mode (connection-oriented/connectionless) is well known. This section describes the CLNP configuration for the avionics and the air-ground link.

3.1.1 Model

As outlined in Section 1.4, the network layer may be subdivided into three sublayers. The 8473 IP is a Subnetwork Independent Convergence Protocol (SNICP) that provides the network users with independence from the underlying real networks used for message transmission. The CLNP is responsible for routing and relaying functions both within any subnetwork and throughout the entire ATN. This is diagrammed in Figure 1-1 in Attachment 1.

3.1.2 General Operation

The CLNP is a connectionless network layer specification. Only the data transmission operation is required, therefore each Protocol Data Unit (PDU) is routed independently of all other PDUs. The CLNP provides a common network layer service to all End Systems within the ATN.

This section is intended to summarize the implementation dependent functions, QOS parameters and the negotiation of optional functions required for the use of ISO 8473. All ISs and ESs should use CLNP that conform with ATN as specified in this document. The optional and mandatory functions selected for the air-ground context of ISO 8473 are intended to simplify the protocol state machine.

The remainder of this section concentrates on CLNP services and the CLNP protocol specification. The services and protocol differ in that the services are concerned with the CLNP interfaces, while the protocol specification is concerned about the internal operation of the CLNP entity.

3.2 Services

This section specifies the services required and offered by the CLNP. The service definitions are described in an abstract way and do not imply any particular implementation. Within the context of this section the network service user is an entity at the transport layer which makes use of the services provided by the CLNP. These services are provided through the use of service primitives. A service primitive is an abstract, implementation-independent description of an interaction between service user and service provider; It is an input to a protocol state machine. A service primitive may contain parameters which describe information that is mandatory (M) or optional (O). The definition of any implementation of these primitives is outside the scope of this document. In any particular interface, not all parameters need be explicitly stated. Some may be implicitly associated with the NSAP at which the primitive is issued.

The subsections which follow describe in detail the primitives and parameters associated with the identified services.

3.2.1 Services Provided by the Internetwork Protocol

The CLNP provides only the connectionless-mode network service described in ISO 8348/AD1. This service requires only two primitives as described below.

The Network Service (N_SERVICE) primitives defined in the following subsections are exchanged between the SNICP user (transport) and the SNICP service provider sublayer. The N_service primitives are only exchanged in ESs and not ISs, though a particular node could serve as both an ES and an IS.

3.2.1.1 Network UNITDATA Request

The N_UNITDATA.Request primitive is the service request primitive for the data transfer service. It is generated by the network user, generally the transport layer, and transferred to the network provider to request that the attached parameters be passed to a remote network user. QOS parameters, if present, can include transit delay, expense, residual error probability, and protection from unauthorized access and priority values.

Parameters:	NS-Source-Address	(M)
	NS-Destination-Address	(M)
	NS-Quality-of-Service	(O)
	NS-User-Data	(M)

3.2.1.2 Network UNITDATA Indication

The N_UNITDATA.Indication primitive is the service indication primitive for the data transfer service. It is generated by the network provider, the CLNP, and passed to the network user, generally the transport layer. QOS parameters, if present, can include transit delay, expense, residual error probability, protection from unauthorized access and priority values.

Parameters:	NS-Source-Address	(M)
	NS-Destination-Address	(M)
	NS-Quality-of-Service	(O)
	NS-User-Data	(M)

3.2.1.3 Network Echo Request

The N_ECHO.Request primitive is the service request primitive for the Echo function. It is generated by the network user and transferred to the network provider to request that the network provider send an echo packet to another network provider. QOS parameters, if present, can include transit delay, expense, residual error probability, and protection from unauthorized access and priority values.

Parameters:	NS-Source-Address	(M)
	NS-Destination-Address	(M)
	NS-Quality-of-Service	(O)

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

3.2.1.4 Network Echo Indication

The N_ECHO.Indication primitive is the service indication primitive for the echo function. It is defined in ISO 8473.

3.2.2 Underlying Service Assumed by the Internetwork Protocol

The CLNP assumes that a real subnetwork provides the connectionless-mode underlying network service required for operation. The underlying service provides only two primitives as described below. If all required services are not provided, an SNDCP or SNDCF will be required to supplement the real subnetwork interface.

The Subnetwork service (SN_SERVICE) primitives defined in the following subsections are exchanged between the SNICP sublayer and the underlying service provider. The underlying service provider is most likely the SNDCP sublayer, unless a SNDCP sublayer is not needed. Thus, the SN-service primitives are exchanged in both ESs and ISs.

3.2.2.1 Subnetwork UNITDATA Request

The SN_UNITDATA.Request primitive is the service request primitive for the data transfer service. It is generated by the CLNP and passed to the real subnetwork to request that the attached parameters be passed to a remote CLNP entity. QOS parameters, if present, can include transit delay, expense, residual error probability, and protection from unauthorized access and priority values.

Parameters:		
	SN-Source-Address	(M)
	SN-Destination-Address	(M)
	SN-Quality-of-Service	(O)
	SN-User-Data	(M)

3.2.2.2 Subnetwork UNITDATA Indication

The SN_UNITDATA.Indication is the service indication primitive for the data transfer service. It is generated by the real subnetwork and passed to the CLNP. QOS parameters, if present, can include transit delay, expense, residual error probability, protection from unauthorized access and priority values.

Parameters:		
	SN-Source-Address	(M)
	SN-Destination-Address	(M)
	SN-Quality-of-Service	(O)
	SN-User-Data	(M)

3.2.2.3 Subnetwork Facility Request

The SN_FACILITY request is issued by the NS_providerSNS_user to request information about the characteristics of the service which may be expected to be available for an SN_UNITDATA request to a given SN_Destination address.

Parameters: None

3.2.2.4 Subnetwork Facility Indication

The SN_FACILITY indication conveys characteristics of the service to the SNS-user which may be expected to be available for SN_UNITDATA requests given a particular SN_Destination address. The primitive is issued by the SNDCF in response to an SNS-user initiated SN_FACILITY request or may be issued by the SNDCF independent of any request by the SNS_user.

Parameters: None

3.2.2.5 Subnetwork Report Indication

The SN-REPORT indication conveys information about a failure to provide the requested QOS characteristics to the SNS-user relating to a failure to satisfy the constraints imposed upon an SN-UNITDATA request given a particular SN-Destination address. The SNDCF will only issue an SN-REPORT indication when an LQA value cannot be satisfied.

Parameters: None

3.2.3 Services Assumed from the Local Environment

The CLNP assumes that a timer service is provided by the local environment. The timer service should be provided to allow the CLNP to schedule events. Descriptions of the three timer primitives follow.

The S_TIMER primitives defined in the following subsections are exchanged between the local environment and the CLNP. The S_TIMER primitives are exchanged in both ESs and ISs.

3.2.3.1 S-TIMER Request

The S_TIMER.Request primitive indicates to the local environment that it should initiate a timer of the specified name and subscript and maintain it for the duration specified by the time parameter.

Parameters:		
	S-Name	(M)
	S-Subscript	(M)
	S-Time	(M)

3.2.3.2 S-TIMER Response

The S_TIMER.Response primitive is initiated by the local environment to indicate that the delay indicated by the corresponding S_TIMER.Request primitive has elapsed.

Parameters:		
	S-Name	(M)
	S-Subscript	(M)

3.2.3.3 S-TIMER Cancel

The S_TIMER.Cancel primitive is an indication to the local environment that the specified timer(s) should be canceled. If the subscript parameter is not specified, then all timers with the specified name are canceled; otherwise, the timer of the given name and subscript is canceled.

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

Parameters: S-Name (M)
S-Subscript (M)

3.3 Specification of the Internetwork Protocol

This section specifies the particular aspects of ISO 8473 that will be used in the ATN. The section specifically addresses the protocol functions and the network protocol data unit (NPDU) formats supported.

3.3.1 Protocol Functions

A subset of the protocol functions outlined in ISO 8473 will be supported for the ATN. Table 3-1 of Attachment 3 defines the provisions of functions for conformance.

3.3.1.1 NPDU Composition Function

This function consists primarily of determining the header or Protocol Control Information (PCI) required to deliver the N_UNITDATA.Request to its destination and attaching the appropriate fields. The PCI required is determined from the N_UNITDATA.Request primitive parameters as well as from current state and local information.

An originating End System does not have to specify priority. A source network entity which does not want to use the priority option includes the priority field, and sets the priority value to zero, which is the lowest priority value.

An originating End System will specify the QOS Maintenance option using the Global Unique QOS format.

3.3.1.2 NPDU Decomposition Function

This function is responsible for removing the PCI from a received PDU and generating N_UNITDATA.Indication primitive parameters. No PDU should be discarded by the destination ES solely because options other than security have been selected. Use of the NPDU priority values for local queue management in the destination ES is optional.

3.3.1.3 Header Format Analysis Function

This function first determines whether a Protocol Identifier reflects a standard version of the protocol and then whether the received PDU has reached its destination, using the destination address (DA) in the PDU editor. If the DA does not identify a network layer user served by this network entity, the corresponding NPDU is forwarded to the Route PDU Function (see Section 3.3.1.5).

3.3.1.4 NPDU Lifetime Control Function

This function is used to enforce the maximum lifetime of a NPDU. It determines whether a NPDU received may be forwarded or whether its assigned lifetime has expired (value zero), in which case it is discarded.

The operation of this function uses the Lifetime Field in the NPDU header. The Lifetime Field is binary encoded, and represents the remaining lifetime of the NPDU in units of 500 milliseconds. The network entity of the originating End System determines the lifetime of the Initial NPDU and places it in the Lifetime Field in the NPDU header. The network entity of every Intermediate System which then processes the NPDU should decrement the value in the Lifetime Field by at least one.
The NPDU Lifetime Field is decremented by a value determined by computing or estimating the sum of the transit delay in the underlying service from which the NPDU was received, and the delay within the system processing the NPDU. The Lifetime Field is then decremented by a value of one for each 500ms of delay. In the case when an estimation of the sum is made, an overestimate will be used.

The guideline for the NPDU Lifetime field decrement value for the air-ground BIS-BIS hop is 3000 ms. Within the avionics subnetwork, the guideline for the NPDU Lifetime field decrement value is 500 ms.

The lifetime parameter should have an initial value of at least 3 times the network span or 3 times the maximum transit delay (in units of 500 milliseconds) whichever is greater.

If the Lifetime Field of the NPDU header reaches a value of zero before it is delivered to the destination End System, the NPDU will be discarded which results in the generation of an Error Report PDU. Specifically, if an Error Report flag is set by the originating network-entity, and if the Lifetime field in the PDU header reaches a value of zero before the PDU is delivered to the destination, then an Error Report PDU should be sent. Other rules for Error Reporting are defined in Section 3.3.1.10.

Destination End Systems do not perform the Lifetime Control Function. Intermediate Systems should always perform the Lifetime Control Function.

3.3.1.5 Route NPDU Function

This function determines the network entity to which a PDU should be forwarded and the underlying service that should be used to reach that network entity. The results of the Route PDU function are passed to the Forward PDU function along with the PDU for further processing.

Selection of the underlying service used to reach the next network entity will be influenced by Quality of Service (QOS) and other parameters such as policy, if present.

For the purposes of routing and relaying, a protocol entity need not verify the correctness of ISO 8348/Addendum 2 semantics carried in the NSAP of received PDUs.

3.3.1.6 Forward NPDU Function

This function issues the SN_UNITDATA.Request primitive to one of the SNDCFs, SNDCPs, or subnetworks with the specified primitive parameters. This function should be implemented in all network entities.

These parameters include the NPDU as user data as well as address information needed by the SNDCF, SNDCP,

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

3.3.1.6 Forward NPDU Function (cont'd)

or subnetwork to identify the next-hop within the network addressing domain. QOS information is also passed on this primitive. These parameters are defined in Section 3.2.2.1, SN_UNITDATA.Request.

3.3.1.7 Segmentation Function

The segmentation function is invoked when the size of the NPDU is greater than the maximum SN-User-Data supported by the underlying subnetwork. This function creates two or more "derived PDUs" from the received PDU. Note that, depending on the size of the NS-User-Data, an N_UNITDATA.Request may never create an "initial PDU", but may result in the generation of multiple derived PDUs. The data unit identifier of all derived PDUs should be the same as the initial PDU. The same data unit identifier should not be re-assigned for the lifetime of the initial PDU. Refer to Section 3.3.2.4.1 and the following figure for more information on the data unit identifier of derived PDUs.

Segmentation Part

Data Unit Identifier	n, n + 1
Segment Offset	n + 2, n + 3
Total Length	n + 4, n + 5

The Segmentation Function is required to be implemented within all Network entities.

The non-segmenting subset will not be used. Implementations will not generate data PDUs without a segmentation part. However, implementations will receive and correctly process PDUs which do not contain the segmentation part.

If the PDU is larger than the maximum SDU size allowed by the subnetwork and if the Segmentation Permitted flag is not set, then the Network Entity should discard the PDU. An Error Report PDU should also be sent if the Error Report flag is set in the originating PDU. See Figures 3.1A, 3.1B and 3.1C of Attachment 3 for an example of segmentation/reassembly.

3.3.1.8 Reassembly Function

The Reassembly function reconstructs the original PDU from the Derived PDUs generated by the operation of the Segmentation function. Reassembly is performed at End Systems and is not implemented in Intermediate Systems.

Segments of the original PDU will be held at a reassembly point for a limited time period before being discarded. This time bound allows reassembly resources to be released when it is no longer expected that any outstanding segments of the original PDU will arrive at the reassembly point.

Upon receipt of the first Derived PDU, a Reassembly Timer is initiated with a value which indicates the amount of time which elapses before any outstanding segments from the original PDU should be assumed to be lost. If this timer expires, all segments of the original PDU held at the reassembly point are discarded and the resources allocated for those segments are freed. The reassembly timer value should be less than the initial Lifetime value since reassembly can not take place after the Lifetime of the PDU has expired. This timer value parameter requires further study during implementation.

COMMENTARY

It is difficult to specify a specific Reassembly timer value for just air-ground and avionics because one can not be certain where the segmentation occurred within the ATN.

3.3.1.9 Discard PDU Function

Whenever a NPDU is discarded the Error Report function is invoked. This function should be implemented in all network entities.

3.3.1.10 Error Reporting Function

The invocation of this function causes the evaluation necessary to determine if an Error Report PDU (ER PDU) is to be sent to the source network entity of a NPDU which was discarded. An Error Report PDU is only sent when the Error Report flag is set to one in the discarded NPDU. This flag is set by the originating end system. The setting of the Error flag is dependent upon one or more of the following conditions being met:

- If the Priority Option or the QOS Maintenance Option is selected in the original Data PDU, and the system generating the Error Report PDU supports the option, then the Error Report PDU specify the same option, using the value that was specified in the original Data PDU.

- If the Security Option is selected in the Data PDU and the system generating the Error Report supports this option, then the Error Report PDU should specify the option using the value that was specified in the original Data PDU. If the system does not support the Security Option, an Error Report is not generated for a Data PDU that selected the Security Option.

- If the Complete Source Route Option is selected in the original Data PDU, and the system generating the Error Report PDU supports this option, then the Error Report should specify the Complete Source Route option. The Source Route parameter value is obtained by extracting from the original Data PDU that portion of the complete source route that has already been traversed, and reversing the order of network-entity titles which comprise the list. If the system does not support the Complete Source Route Option, an Error Report is not generated for a Data PDU that selects the Complete Source Route option.

Non-receipt of an ER PDU does not imply delivery. An ER PDU is not generated to report the discard of an ER PDU.

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

An ER PDU identifies the discarded NPDU and specifies the type of error detected. The entity generating the report (ES or IS) should insert in the destination address field of the ER PDU the contents of the source address field of the PDU that generated the error. Reasons for Error Reports and PDU discards are specified in Section 3.3.2.8.1, Reason for Discard.

This function should be implemented in all network entities.

3.3.1.11 PDU Header Error Detection Function

The use/non-use of checksums should be capable of being configured. The default setting should be non-use. This function is intended to evaluate the header checksum value if a non-zero value is present and discard the PDU if the checksum fails.

COMMENTARY

Network Header Checksum will not be supported across the air-ground subnetwork because the checksum will be lost if header compression is used. Network Header Checksum may be used onboard the aircraft.

3.3.1.12 Padding Function

The Padding Function is supported by ATN Network entities when received, i.e., PDUs received with padding will be processed. Sending entities should not generate padding.

3.3.1.13 Security Function

The security function is an optional function which can be used to provide various protection services including data origin authentication, data confidentiality and data integrity services.

No specific ATN security methods are identified at this time. If an implementation does not support this function, and the function is selected in a PDU, then the PDU is discarded. An Error PDU is not generated.

3.3.1.14 Source Routing Function

The Source Routing Function is not supported. If the function is selected in a NPDU, then the NPDU is discarded. An Error PDU is not generated.

3.3.1.15 Record Route Function

The Record Route function records the path taken by an NPDU as it traverses a series of ATN Routers. A recorded route consists of a list of Network entity titles held in a parameter within the options part of the NPDU header.

It is required that all ATN ISs support the Partial Record Route Function. The Partial Record Route Function is optional but not recommended. The Complete Record Route function is not supported. If the Complete Record Route parameter code is encoded in a NPDU, that NPDU should be discarded. An Error Report should be generated and forwarded to the originating network entity if the Error Report flag is set.

3.3.1.16 QOS Maintenance Function

The QOS Maintenance Function allows originating network entities to provide information to network entities in ATN ISs which will be used to make routing decisions. This function is mandatory for both ISs and ESs.

A QOS Maintenance parameter, encoded according to the globally unique format specified in ISO 8473, should be included in each PDU originated by an ES. In the absence of a function that maps Network Service User QOS requirements to the QOS M parameter, a configurable QOS M will be generated by a Network entity in the ES.

Intermediate Systems should support QOS Maintenance and take into account the QOS Maintenance parameter (if it exists in the NPDU) when making a routing decision.

3.3.1.17 Priority Function

All ISs should support the optional Priority function. The following implementation agreements should apply:

A. The forwarding of NPDUs should be scheduled based on the Priority function. The scheduling algorithm for achieving this priority function is left as a local matter, however, it is necessary that the following constraints be met:

   1) An NPDU of lower priority should not overtake an NPDU of higher priority (i.e. exit the IS ahead of a higher priority PDU arriving before it) in an intermediate system when both NPDUs are being forwarded to the same subnetwork.

   2) A minimum flow should be provided for lower priority PDUs.

B. NPDUs in which the priority parameter is absent should be processed as if the priority value were "zero", which is the lowest priority value according to the encoding rules of ISO 8473.

All ESs should support the optional priority function. The following implementation should be used:

A. The full range of 15 priority levels provided by ISO 8473 should be used. The mapping of QOS priority information provided by the NS User and used by the network entity to set these priority values shall be:

B. An ES does not have to use the priority function for all NPDUs it originates. If no priority QOS parameter is provided by the NS User upon an invocation of the service, the network entity should not include the optional priority field in the NPDU.

C. Use of priority for local queue management in the receiving (destination) ES is optional.

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

3.3.1.17 Priority Function (cont'd)

A list of priority coding is included in Table 3.7 of Attachment 3.

3.3.1.18 Congestion Notification Function

ISs may inform the destination network entity of congestion by setting the Congestion Experienced (CE) flag in the QOS maintenance parameter. This flag is initially set to zero. This function is mandatory for an IS.

The definition for congestion and the algorithms used for determining congestion should be uniform within the ATN.

An IS should set the CE flag in all NSDUs forwarded on a Queue which has an average queue length greater than one;

The queue length averaging algorithm computes the average queue length over two cycles, where the two cycles are:

a) the "previous cycle", which is the interval from when the IS becomes busy, until it becomes idle and the idle ends (indicated by the instant the first packet arrives to the idle IS);

b) the "current cycle", which is the interval from the end of the idle interval to the current time instant when the average queue length is computed;

An embodiment of the averaging algorithm is shown in Table 3.6 of Attachment 3.

3.3.1.19 Echo Function

The function of the echo-request entity is to accept an incoming echo-request PDU, perform some processing, and generate an echo-reply PDU. The echo-request entity may be thought of as an entity that co-exists with the network layer.

The term "ping" will be used to mean the act of transmitting an echo-request PDU to a remote system (with the expectation that an echo-reply PDU will be sent back to the transmitter).

When a system decides to ping a remote system, an echo-request is built. All fields of the PDU header are assigned normal values. The address of the system to be pinged is inserted as the destination NSAP address. The rules of segmentation defined for a DT PDU also apply to the echo-request PDU.

The echo-request is switched through the network toward its destination. Upon reaching the destination system, the PDU is processed according to normal processing rules. At the end of the input processing, the echo-request PDU is delivered to the echo- request entity.

The echo-reply entity will build and dispatch the echo-reply PDU. Except as noted below, this second PDU is built using the normal construction procedures. The destination address of the echo-reply PDU is taken from the source address of the echo-request PDU.

3.3.2 NPDU Structure and Format

This section describes the ATN NPDU structure and format consistent with ISO 8473. All CLNP NPDUs are one of two possible types. User information is transferred between entities using the Data (DT) PDU. Error information is transferred using the Error Report (ER) PDU.

3.3.2.1 General NPDU Structure

All NPDUs will contain an integral number of octets. The NPDU header is followed by the Data Part. Protocol Data Units are composed of some or all of the following parts in order:

NPDU Header

a) the fixed part
b) the address part
c) the segmentation part
d) the options part (if present)

Data

e) the data part (if present).

3.3.2.2 NPDU Header Fixed Part

The fixed portion of the CLNP NPDU is nine octets in length, and contains parameters common to all NPDU types, all of which are specified with fixed length fields.

The fixed part fields include:

- Network Layer Protocol Identifier
- Header Length Indicator
- Version/Protocol Identifier Extension
- NPDU Lifetime
- Segmentation Permitted Flag
- More Segments Flag
- Error Report Flag
- Type Code
- NPDU Segment Length
- NPDU Header Checksum.

The fifth octet in the fixed part contains the Segmentation Permitted flag, the More Segments flag, and the Error Report flag, followed by a five bit Type field.

3.3.2.2.1 Network Layer Protocol Identifier

This field is the initial octet of the NPDU and should be set to the value H '81'. Any other value, including 0 (H '00') for the Inactive Network Layer protocol subset, is not supported by the Internetworking Protocol and will cause the NPDU to be discarded.

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

Implementations will not transmit PDUs encoded using the inactive subset.

COMMENTARY

This section refers only to ISO 8473 protocol identifiers. Protocol identifier values corresponding to routing protocol data units are supported and are not the subject of this chapter.

3.3.2.2.2 Header Length Indicator

This single octet parameter is a binary number which indicates the length in octets of the header. This value will stay the same for all segments (Derived NPDUs) of the Initial NPDU. The maximum value allowed for this parameter is 254 (H 'FE').

COMMENTARY

The "Initial NPDU" is created from a single N_UNITDATA.Request and corresponds to a single Data Unit ID (DUID) field value. Multiple segments or derived NPDUs can be created from an Initial NPDU in order to pass across subnetworks with a limited maximum unit data size. This may even be done in the originating end-system, causing derived NPDUs to be sent from it.

3.3.2.2.3 Version/Protocol Identifier Extension

The value of this one octet parameter should be 1 (H '01') indicating the first version of ISO 8473.

3.3.2.2.4 NPDU Lifetime

The NPDU lifetime parameter is a one octet field and is encoded as a positive binary number representing the remaining lifetime of the NPDU, in increments (units) of 500 milliseconds.

The NPDU lifetime parameter should have an initial value of at least three times the network span or three times the maximum transit delay (in units of 500 milliseconds), whichever is greater.

3.3.2.2.5 Segmentation Permitted Flag

The value (1 - permitted, 0 - not permitted) of the Segmentation Permitted flag is determined by the originator and cannot be changed by any ISs. When the value 0 is selected, this indicates that: segmentation is not permitted; that the segmentation part of the NPDU header is not present; and that the segment length field is the same as the NPDU total length field.

To remain conformant with this specification, segmentation will be performed at a given node when the size of the NPDU is greater than the maximum Subnetwork PDU (SNPDU) size supported by the underlying subnetwork service used for transmission of the PDU.

In this case, the Segmentation Permitted flag will be set to "one" by the source network entity to indicate that segmentation is allowed at the intermediate nodes.

COMMENTARY

The case where segmentation is not permitted, but a PDU is larger than what a subnetwork can support is not expected to occur on avionics or air-ground subnetworks, however it is possible that packets will be discarded if this occurs.

3.3.2.2.6 More Segments Flag

The More Segments flag is used to indicate whether or not the NPDU containing the flag is the last one in the sequence. If the More Segments flag is set to "zero" the NPDU is the last (or only) segment produced from a single N_UNITDATA.Request. If the More Segments flag is set to "one", segmentation has occurred and the NPDU containing the flag is not the last one in the sequence.

3.3.2.2.7 Error Report Flag

When the Error Report flag is set to zero, discard of the Data NPDU will not cause the generation of an Error Report PDU (ER PDU). If the Error Report flag is set to one, an ER PDU is sent by the discarding CLNP entity to the NPDU source if the appropriate conditions are met. The default condition is to set the flag to one. Specific Error Report options are listed in Section 3.3.1.10.

3.3.2.2.8 Type Code

This five bit code indicates the NPDU type as encoded below.

PDU	BITS
Type Code	5 4 3 2 1
DT PDU	1 1 1 0 0
ER PDU	0 0 0 0 1
ERQ PDU	1 1 1 1 0
ERP PDU	1 1 1 1 1

3.3.2.2.9 NPDU Segment Length

This two octet field contains the entire length in octets of the NPDU, including both header and data (if present). If the PDU is not segmented, this field will contain the same value as the Total Length field in the Segmentation Part of the header.

3.3.2.2.10 NPDU Header Checksum

The Header Checksum is a two octet field which is computed on the entire header. A value of zero is reserved to indicate that this checksum was not computed by the originator and is to be ignored.

3.3.2.3 NPDU Header Address Part

The address part immediately follows the fixed part of the NPDU header. It contains destination and source addresses in that order. Each of these addresses is preceded by a one octet address length indicator. This length indicator is binary encoded positive integer which indicates the length of the following address in octets. The address field length is 20 octets. The addresses conveyed in the fields are Network Service Access Point

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

3.3.2.3 NPDU Header Address Part (cont'd)

addresses. Refer to Chapter 2 for format and encoding information on ATN NSAP addresses.

3.3.2.4 NPDU Header Segmentation Part

The segmentation header part will only be present if the Segmentation Permitted flag is set to one. The segmentation header part contains parameters required for the successful segmentation and reassembly of NPDUs.

Segmentation is performed when the size of the network protocol data unit is greater than the maximum service data unit size supported by the underlying subnetwork service used for transmission of the PDU.

Segmentation consists of composing two or more Derived PDUs from the SDU received from the layer above. The user data encapsulated within the original PDU are divided into the smallest number of Derived PDUs which it will take to satisfy the size requirements of the Userdata parameter field of the UNITDATA.Request primitive.

The segmentation header part contains the Data Unit Identifier, the Segment Offset and the NPDU Length, which are required for the successful segmentation and reassembly of NPDUs. An example of segmentation is shown in the Segmentation Figures in 3.1A, 3.1B and 3.1C of Attachment 3.

3.3.2.4.1 Data Unit Identifier

The Data Unit Identifier (DUID) is unique for all segments associated with a single N_UNITDATA.Request, for at least the lifetime of the associated NPDUs. The DUID identifies the original PDU and all of its Derived PDUs after Segmenting, so that a segmented data unit may be correctly reassembled. The DUID is assigned by the source End System.

3.3.2.4.2 Segment Offset

The Segment Offset field specifies the relative position (in octets) of the segment contained in the data field of the derived NPDU with respect to the start of the data field contained in the NS-User-Data field of the N_UNITDATA.Request which generated the NPDU. The first segment and an unsegmented PDU have segment offset values of zero, otherwise this value should be a multiple of eight.

3.3.2.4.3 NPDU Total Length

The value contained in the NPDU Total Length field is the total length in octets of the Initial NPDU including header and data. This field is not changed during the lifetime of the NPDU and is applicable to Initial and Derived NPDUs.

3.3.2.5 NPDU Header Options Part

The NPDU Header Options Part portion of the NPDU header, if present, may contain one or more parameters. The length of the Header options part is the header length minus the lengths of the Fixed Part, Address Part and Segmentation Part, in octets. All parameters contained in the options part of the NPDU header are preceded by a one octet Parameter Code and a one octet Parameter Length.

Field Length	Field Name
1	Parameter Code
1	Parameter Length (m)
m	Parameter Value

Duplication of options is not allowed and will produce a protocol error.

Option values are provided by the ATN End System Network entity which originates internetwork protocol data packets. As a part of the CLNP header, options are carried transparently over ATN subnetworks, and are evaluated in turn by each receiving ATN router. While certain data compression and protocol conversion techniques may be applied to minimize the quantity of Network layer protocol overhead carried on air-ground data links, it should be noted that the information content of the CLNP packet header should be delivered unchanged to each successive ATN entity.

Of the ISO CLNP options permitted by ISO 8473, four are regarded as essential for operation of the ATN. The essential options are Partial Route Recording, Priority, Quality of Service Maintenance and Congestion Notification.

Complete Source Routing and Complete Record Route options are not supported by ATN Network Entities. Network entities are not compelled to act based on the presence of Padding or Partial Source Routing options.

The following subsections contain a detailed description of each option.

3.3.2.5.1 Padding

In general, ESs and ISs should not generate padding. PDUs received with padding will be recognized and processed.

3.3.2.5.2 Security

The Security is not currently defined for ATN Network entities. If an implementation does not support this function, and the option is selected in a PDU, then the PDU is discarded. An Error PDU is not generated.

3.3.2.5.3 Source Routing

There are two Source Routing options: Complete and Partial. ATN does not support the use of either option. If the Complete Source Routing option is selected in a PDU, then the PDU is discarded. An Error PDU is not generated. If a Partial Source Routing option is selected in a PDU, then the parameter is ignored.

3.3.2.5.4 Record Route

The Record Route records the path taken by an NPDU as it traverses a series of ATN Routers. A recorded route

3.0 INTERNETWORKING SERVICE AND PROTOCOL (cont'd)

consists of a list of Network entity titles held in a parameter within the options part of the NPDU header. The length of this parameter is determined by the originating Network entity, and does not change as the NPDU traverses the Network. The list is constructed as the NPDU is forwarded along a path towards its destination. Only the titles of ATN Router Network entities are included in the recorded route; the Network entity title of the NPDU originator is not recorded in the list.

All ATN Network entities should support the Partial Record Route Function. The Complete Record Route Function is not supported by ATN Network entities. If the Complete Record Route parameter code is encoded in a NPDU, that NPDU should be discarded. An Error Report should be generated and forwarded to the originating network entity if the Error Report flag is set.

COMMENTARY

The Record Route function is intended to be used in the diagnosis of subnetwork and/or routing problems.

3.3.2.5.5 Quality of Service Maintenance Option

The Quality of Service Maintenance provides information to Network entities in ATN Routers which may be used to make routing decisions where such decisions affect the overall QOS provided to NS users.

All ATN ISs should support the Quality of Service Maintenance option, using the globally unique encoding.

3.3.2.5.6 Priority

Priority allows an NPDU with a numerically higher priority value to be processed preferentially with respect to other NPDUs with numerically lower priority values.

Avionics ISs should process NPDUs based on the Priority Option.

3.3.2.6 NPDU Data Part

The Data Part of the NPDU consists of an ordered sequence of octets which should be identical to or part of the NS-User-Data field passed down to the CLNP in the N_UNITDATA.Request (for the Data NPDU) or the header of the discarded PDU (for the Error Report PDU), or the contents of the ERQ PDU (for the Echo Reply PDU).

3.3.2.7 Data NPDU

The data part of the Data NPDU (DT PDU) is the SDU in the NS-User-Data field of the N_UNITDATA.Request. All fields of the Data PDU header are as specified above. Table 3.3 of Attachment 3 depicts the structure of the DT PDU.

3.3.2.8 Error Report NPDU

Table 3.4 of Attachment 3 depicts the structure of the Error Report NPDU (ER PDU).

The ER PDU header has the following constraints:

- The Error Report Flag, Segmentation Permitted Flag, and More Segments Flag of the ER PDU are always set to zero.
- ER PDUs do not contain a Segmentation Part.
- The destination address field of the Error Report PDU will be the contents of the source address field of the PDU that generated the error.
- The Source Address is the Network Entity Title of the end or intermediate system discarding the DT PDU.

3.3.2.8.1 Reason For Discard

The Reason for Discard parameter Code is "1100 0001". the Parameter Length is two octets and the type of error is encoded in binary. The first octet of the value is an error type code. If the error in the discarded Data PDU can be localized to a particular field, the number of the first octet of that field is stored in the second octet of the Reason for Discard parameter field. If the error cannot be localized to a particular field, then the value of zero is stored in the second octet of the Reason for Discard parameter field.

3.3.2.8.2 Error Report Data Part

The data part of the Error PDU (ER PDU) is the entire CLNP header of the discarded Data PDU.

3.3.2.9 Echo Request NPDU

The data part of the Echo Request NPDU (ERQ PDU) is as defined in ISO/IEC 8473/PDAM6.

3.3.2.10 Echo Reply NPDU

The data part of the Echo Reply NPDU (ERP PDU) is as defined in ISO/IEC 8473/PDAM6.

4.0 ES-IS PROTOCOL SPECIFICATION

4.1 Introduction

The End System (ES) to Intermediate System (IS) Protocol (ES-IS) permits the exchange of configuration and routing information to facilitate the routing and relaying functions of the Network Layer. This Network Layer protocol assumes that routing to a specified Subnetwork Point of Attachment (SNPA) on the same subnetwork is carried out satisfactorily by the subnetwork itself. The subnetwork though is not capable of routing on a global basis using the NSAP address alone to achieve communication with a requested destination. The avionics implementation of this protocol is as defined in ISO 9542 and herein.

Included in this chapter are the following descriptions and definitions:

- The Role of ISO 9542
- The ISO 9542 Service Definition
- ISO 9542 Protocol Functions and Protocol Data Units (PDU) Structure
- Air-Ground Router PDU Requirements
- Avionics Host & Router PDU Requirements
- Summary of PDU Types and Options

4.2 Role of ISO 9542

The ES-IS protocol as defined in ISO 9542 will perform the roles of:

- an ES to IS routing protocol for avionics Host/Router routing exchange.

- an IS to IS connectivity discovery function.

The routers will operate the ISO 9542 to establish connectivity and exchange configuration information. Intra-domain and inter-domain routing protocols may then be used to exchange dynamic routing information.

ISO 9542 is designed to support either point-to-point, broadcast, or general topologies. The ATN air-ground link is defined as a point-to-point subnetwork topology as specified in the ICAO SARPS. Therefore, many of the routing information and protocol function capabilities supported by ISO 9542 and/or used in the ES-IS scenario are not applicable to the ATN air-ground subnetworks. The primary, if not only, function of ISO 9542 utilized over the air-ground subnetwork is to send IS Hello (ISH) PDUs between the airplane router(s) and adjacent ground router(s). When an air-ground router receives an ISH, it should respond promptly.

4.3 ISO 9542 Service Definition

ISO 9542 does not provide specific services to a Network Layer user and, therefore, does not define service primitives. ISO 9542 is used in conjunction with ISO 8473 in support of the routing functions. It is only used to exchange configuration information between systems attached to the same subnetwork. ISO 9542 is initiated by systems management action. Systems management will initiate the ISO 9542 entity when subnetwork connections are established, or when a system is initialized.

4.3.1 Initiating ISO 9542 over Air/Ground Subnetworks

ATN air-ground subnetworks are defined as point-to-point subnetworks. ISO 8208 is used as the subnetwork protocol. As aircraft air-ground routers establish ISO 8208 connections with ground based air-ground routers, systems management will be notified of the connection. Systems management will then initiate the ISO 9542 entity. Systems management need only initiate the ISO 9542 entity once, when the first subnetwork connection is established to a specific air-ground router. See Appendix C of this specification for information concerning the termination of connection.

4.3.2 Initiating ISO 9542 over Avionics Subnetworks

Each time that a system attached to an avionics subnetwork is initialized, systems management will initiate the ISO 9542 entity.

4.4 ISO 9542 Protocol Functions and PDU Structure

The Protocol Functions that are applicable to the ATN air-ground and avionic subnetwork are defined in this section along with the PDU Structure.

4.4.1 Protocol Functions

Most of the ISO 9542 functions are timer based and are executed upon expiration of a timer (rather than upon receipt of a PDU or invocation of a service primitive). The two types of ISO 9542 timers are a (local mode) Configuration Timer (CT) and a Holding Timer (HT).

The ISO 9542 functions that are applicable to the End Systems and Intermediate Systems include the:

- Report Configuration Function
- Record Configuration Function
- Flush Old Configuration Function
- Configuration Notification Function
- PDU Header Error Detection
- Protocol Error Processing Function
- Request Redirect Function
- Record Redirect Function.

For avionics LANs, implementations should support both Configuration Information (CI) and Route Redirection Information (RI); all mandatory protocol functions of both CI and RI are necessary. No subset is supported. The redirection functions are not applicable for use over the ATN air-ground subnetworks.

A complete list of ISO 9542 provisions and their Mandatory/Optional status for ATN is contained in Table 4.1 of Attachment 4.

For air-ground subnetworks, the Holding time should be set to the maximum value in both aircraft routers and ground routers, to preclude their expiration.

COMMENTARY

The intention is that the Holding timer exceeds the value of other events. Thus a IS Hello will never be initiated as a result of the expiration of the Holding timer.

4.0 ES-IS PROTOCOL SPECIFICATION (cont'd)

4.4.2 PDU Structure

There are three PDUs defined in the ISO 9542. These include the:

- ESH PDU
- ISH PDU
- RD PDU.

All PDUs contain an integral number of octets, with numbering and significance as specified in ISO 9542. Optional parameters are also encoded as defined in ISO 9542. The air-ground routers and the avionics hosts and routers have different PDU requirements. In this section the following fields are defined for each PDU.

- PDU Fixed Header
- PDU Parameters and Options.

4.4.2.1 Fixed Header

All ISO PDUs contain a fixed header with an integral number of octets, with numbering and significance as specified in Section 7.2 of ISO 9542, with the following clarifications.

The three high order bits of the type code field (Sp, M, and E/R) are not used and shall be set to a value of zero. For air-ground subnetworks, the Holding Time should be set to the maximum value in both aircraft routers and ground routers.

4.4.2.2 ESH PDU Parameters and Options

Sections 7.5 and 7.3.3 of ISO 9542 defines format, size, and options of the ESH PDU which must be generated by ESs on the aircraft.

4.4.2.3 ISH PDU Parameters and Options

Sections 7.6 and 7.3.4 of ISO 9542 defines format, size, and options of the ISH PDU which must be generated by ISs.

COMMENTARY

It is recommended that ISs include the optional "Suggest ES Configuration Timer" (ESCT) field in their ISH PDUs. It is recommended that ESs process the optional ESCT field according to ISO 9542 and use the suggested value as its "active" ES Configuration timer.

4.4.2.4 RD PDU Parameters and Options

Section 7.7 of ISO 9542 defines format, size, and options of the RD PDU which may be generated by ISs on the aircraft.

4.5 Air-ground Subnetwork PDU Requirements

a. Applicable PDUs

Only the ISH PDU is applicable to air-ground subnetworks. None of the ISH PDU options are required for the air-ground link.

b. Applicable Options

No options are required.

4.6 Avionics Subnetwork PDU Requirements

a. Applicable PDUs

All three PDUs (ESH, ISH, RD) are applicable to avionics subnetworks.

b. Applicable Options

The following options are supported: Security, Quality of Service Maintenance, Priority, Address Mask, and SNPA Mask. The values for the Priority, QOS, and Priority options when encoded in the RD PDU shall be directly mapped from the Data PDU that is being routed.

4.7 Summary of PDU Types and Options

Figure 4.7 below contains a list of PDU options.

PDU TYPE/ OPTIONS	AIR/ GROUND	AVIONICS
ESH	N/A	YES
Security	N/A	YES
Priority	N/A	YES
ISH	YES	YES
Security	NO	OPTIONAL
Priority	NO	OPTIONAL
RD	N/A	YES
Security	N/A	OPTIONAL
Priority	N/A	OPTIONAL
QOSM	N/A	OPTIONAL
Address Mask	N/A	OPTIONAL
SNPA Mask	N/A	OPTIONAL

Figure 4.7
PDU Options

4.8 Recommended Implementation Provisions

The following implementation provisions pertaining to ISO 9542 (ES-IS) protocol are recommended. These recommendations are based largely on Version 4, Part 3, Section 8.1, of the NIST/OIW Stable Implementors Agreements.

4.0 ES-IS PROTOCOL SPECIFICATION (cont'd)

4.8 Recommended Implementation Provisions (cont'd)

1. For the air-ground and Gatelink subnetworks, implementations should support Configuration Information for ISs only. All mandatory functions of Configuration Information for ISs are necessary; no subsets are permitted.

2. Implementations should support any valid NSAP address format and length. For the purposes of the protocol, NSAP addresses are treated simply as octet strings.

3. All timer values should be configurable by the System Management Entity.

4. The use of checksums is discouraged. Even so, implementations should be capable of checksum generation. The use or non-use of checksums should be configurable.

5. The QOS, Security and Priority parameters should not be used for routing purposes. For conformance, ISs should transmit these parameters in RD PDUs if they are present in the data PDU which generated the redirect. However, ESs should ignore them in RD PDUs.

6. Configuration Notification functions should be supported in ESs and in ISs.

   a. ISs should invoke the function upon receipt of either an ESH or an ISH.

   b. ISs should invoke the function even if the ESH received has an incorrect RDI or Area field.

   c. ESs should invoke the functions only upon receipt of an ISH.

7. For avionics LANs, the ES-IS protocol employs the same LSAP value as is used for other OSI Network layer protocols (i.e. Hex"FE").

8. With respect to Redirection information:

   a. The encoding of the BSNPA (Better Subnetwork Point of Attachment) address follows the syntax rules for the data link being used.

9. Unless otherwise specified, implementations should use the standard IEEE-registered values for the multi-cast addresses corresponding to ALL_IS_SNPA and ALL_ES_SNPA.

10. With respect to the Query Configuration function:

    a. The Error Report flag should be set to zero (0) for NPDUs sent as a result of invoking the Query Configuration function.

    b. ISO 8473 PDUs sent as a result of invoking the Query Configuration function should use the Network Layer Protocol ID (NLPID) assigned to ISO 8473.

    c. An ISO 8473 PDU received as a result of another ES having performed the Query Configuration function should be processed as follows:

       i. If the ISO 8473 PDU is addressed to one of the NSAPs present in the ES, the ES should process the PDU according to the applicable clauses of ISO 8473 and invoke the Configuration Response function.

       ii. If the ISO 8473 PDU is not addressed to one of the NSAPs present in the IS (or ES), the system should discard the PDU without generating an ISO 8473 Error Report.

5.0 INTER-DOMAIN ROUTING PROTOCOL

5.1 Introduction

This section describes the routeing protocol used between the aircraft and the ground systems. This protocol will be ISO 10747, the Protocol for Exchange of Inter-domain Routing Information, as profiled by the following paragraphs.

ISO 10747 is a distance vector routeing protocol that allows the exchange of routeing information between the aircraft Boundary Intermediate System (BIS) and a ground BIS based on policy considerations.

In the ATN environment, each aircraft constitutes its own unique routeing domain. IDRP makes a distinction between End Routeing Domains (ERDs) and Transit Routeing Domains (TRDs). The airborne routeing domain acts as an ERD while the routeing domain containing the ground BIS could be either an ERD or a TRD.

COMMENTARY

At present there is only one BIS onboard an aircraft. The Gatelink committee has discussed having a separate BIS to handle the higher throughput. This may cause problems in keeping the PIBs synchronized between the two routers. Note that the BIS discovery problem would still exist.

5.2 Inter-Domain Addressing

The application of the addressing plan presented in Chapter 2 of this specification guarantees the correct operation of IDRP since a Routeing Domain Identifier (RDI) consists of the six first fields of any NSAP. Thus the concatenation of the AFI, IDI, VER, ADM, RDF and ARS fields represents a unique routeing domain.

Domain Configuration Information is made available to IDRP through the use of managed objects. These managed objects are specified in Clause 11 of ISO 10747.

5.3 IDRP Protocol Elements

5.3.1 Structure and Content of BISPDUs

The PDUs used to exchange routeing information between BISs are as specified in ISO 10747 with the following clarifications.

5.3.2 KEEPALIVE PDU

The KEEPALIVE PDUs are exchanged to leave open a previously set BIS-BIS connection. They should be sent often enough as not to cause the Hold time timer advertised in the OPEN PDU to expire. They may also be used for the acknowledgement of received BISPDUs.

The KEEPALIVE timer should be set to a high value to preclude its expiration and thus avoid messages across the RF. KEEPALIVE PDUs must not be sent over the broadcast subnetworks (AVPAC, SATCOM, Mode-S, and HF) except as acknowledgement of other PDUs.

COMMENTARY

The mechanism for achieving this is under study. Further definition will be provided in a future supplement.

KEEPALIVE PDUs may be sent over the Gatelink subnetwork with a periodicity of 600 seconds.

5.4 Network Dependent Functions

The network dependent functions provide the interface between IDRP and the underlying CLNS described in the Chapter 3 of this specification.

5.4.1 Connection-Event.indication

A Connection-Event.indication is received from the local management entity when an ISO 8208-based subnet (AVPAC, SATCOM, Mode-S, or HF) establishes a connection to another router.

The parameters is: BIS NET; the NET of the BIS to which the connection is established.

This primitive will cause the NET to be inserted into the EXTERNAL-BIS-NEIGHBORS table, the Hold Time and Keep-Alive timers are set avoid expiration. See Appendix A.

5.4.2 Disconnect-Event.indication

A Disconnect-Event.indication will be sent from the local manager when the 8208-based RF subnetwork loses connectivity. This primitive will clear the NET from the EXTERNAL-BIS-NEIGHBORS table and cause a the stop event.

See Appendix A for Router Initiation procedures.

5.4.3 IN-Event.indication

This is a placeholder for the establishment of a Gatelink connection.

5.4.4 OUT-Event.indication

This is a placeholder for the termination of a Gatelink connection.

5.5 Policy Information Base

The Policy Information Base (PIB) can be used to select paths and to determine the dissemination of routeing information.

The internal database format of the PIB shall be a local matter. It is recommended that the policy syntax language as described in DIS 10747 Annex H be used to describe policy syntax and semantics.

5.5.1 Path Selection

A user may require policies to select a preferred path to a destination. These policies may be formed to allow only static solutions, i.e.,

5.0 INTER-DOMAIN ROUTING PROTOCOL (cont'd)

5.5.1 Path Selection (cont'd)

"For AIS traffic to the airline home routing domain, always choose preferred ground-service provider".

Note: Here there is no selection of next hop based on priority or QOS parameters.

If, however, the user is interested in routing based on quality of service (expense, capacity, transit delay, residual error probability), priority, and security ISO 10747 allows the user to set up policies to indicate these preferences as distinguishing attributes. The distinguishing attributes supported form a set of Routing Information Base (RIB) Attributes (RIB-ATTs), and Forwarding Information Base (FIB) entries must be provided for each selected RIB-Att combination.

5.5.1.1 Policies and IDRP Distinguishing Attributes

The following sets of distinguishing attributes are required as provided in the ICAO SICASP ATN manual:

(Traffic Type, transit delay, priority)
(Traffic Type, capacity, priority)
(Traffic Type, expense, priority)
(default)

These attributes are described below. Note that the use of these attributes will be based on the airline's policy requirements.

Note: The Capacity, Expense, and Transit Delay attributes are mapped from the ISO 8473 Quality of Service Maintenance Option field. The Priority attribute is mapped from the ISO 8473 Priority Option field. The Traffic Type attribute is mapped from the ISO 8473 Security Option field.

If an NPDU is received that does not match the supported RIB-Atts, the NDPU is discarded and an ISO 8473 Error Report PDU is sent indicating "Unsupported option not specified."

5.5.1.2 Use of Priority

In the current ISO 10747 standard, priority is used as a mechanism to set an allowable range of priorities for a path. For example, one can form a policy statement such as "For AIS traffic, route through my preferred ground service provider using the VHF subnetwork only if the priority is 'x' or greater".

5.5.1.3 Use of Transit Delay

If more than one path exists between the CMU and the destination end domain, one may select the optimimum path based on the transit delay characteristics of the path. With the exchange of UPDATE PDUs, the CMU will know the total end-to-end transit delay to reach an end-system. A policy statement may be:

"For AIS traffic, route through my preferred-ground service provider, and chose the path with a transit delay of 'x' or less for all priority ranges".

5.5.1.4 Use of Capacity

If more than one path exists between the CMU and the destination end domain, one may select the optimimum path based on the capacity characteristics of the path. With the exchange of UPDATE PDUs, the CMU will know the total end-to-end capacity to reach an end-system. A policy statement may be:

"For AIS traffic, route through my preferred ground-service provider, and chose the path with a capacity of "x' or more for all priority ranges".

Note: ISO DIS 10747 does not recommend a unit for this parameter. ICAO SICASP ISDG is currently investigating and will be proposing a unit.

5.5.1.5 Use of Expense

If more than one path exists between the CMU and the designation end domain, one may select the optimimum path based on the cost of transferring data over the path. With the exchange of UPDATE PDUs, the CMU will know the total end-to-end expense to reach an end-system. A policy statement may be:

"For AIS traffic, route through my preferred ground-service provider, and chose the path with an expense of 'x' or less for all priority ranges".

Note: ISO DIS 10747 does not recommend a unit for this parameter. ICAO SICASP ISDG is currently investigating and will be proposing a unit.

5.5.1.6 Use of Traffic Type

As defined in the ICAO SICASP ATN Manual, the Traffic Type may consist of combinations of the following values:

ATSC-OPS Traffic
ATSC-ADM Traffic
AISC-OPS Traffic
AISC-ADM Traffic
APC Traffic

Where,

ATSC	stands for Air Traffic Services Communication
ADM	stands for Administrative data (ADM)AISC stands for Aeronautical Industry Services Communication
APC	stands for Airlines Passenger Communications

For instance, if a subnetwork supports both administrative and operational ATC traffic only, it would have a traffic type of (ATSC-OPS & ATSC-ADM). The user's policies may chose the appropriate combinations of the attributes for these subnetworks.

Note: The current ISO DIS 10747 supports Source Specific Security and Destination Specific Security, but does not currently support Globally Unique Security. This oversight will be added as a ballot comment to DIS 10747.

5.0 INTER-DOMAIN ROUTING PROTOCOL (cont'd)

5.5.1.7 Default

The 'default' in ISO 10747 snytax refers to the empty set, where no IDRP distinguishing attributes are contained within the NPDU. An NPDU with no QOS, priority, or security parameters would be mapped to the 'default' FIB.

5.5.1.8 Subnetwork Preference

As part of policy, an airline may request a subnetwork preference list, for example an airline may specify "For ATC traffic, routing through the US FAA domains, use Mode S (only)". Changes to the current IDRP policy snytax are being written to allow policy to select a subnetwork (SNPA) preference.

5.5.1.8.1 Use of NEXT_HOP Attribute in UPDATE PDUs

If a local BIS needs to know the adjacent BIS's SNPA addresses, these addresses may be transferred in an UPDATE PDU using the NEXT_HOP attributes. This information may be advertised to other BISs.

> Note: The adjacent BIS{NET,SNPA] combinations should be acquired through the receipt of ISO 9542 Intermediate System Hello (ISH) PDUs.

5.5.1.9 Coordination Between IDRP Policies and Subnetwork Connectivity Policies

If subnetwork connectivity policies exist within subnetwork devices, these policies may require coordination with the IDRP policies.

5.5.1.10 Coordination of Policies

The policies a user selects will determine the exact combination of rib-atts supported, and the associated size of the IDRP databases. These policies should be coordinated with the appropriate ground domains.

5.5.2 Minimizing Aircraft Mobility Advertisement and Dissemination

The Policy Information Base (PIB) can be used to select paths and to determine the dissemination of routing information.

5.5.2.1 Path Advertisement

The CMU shall provide to each ATN RD to which it is currently connected, a single route to all NSAPs and NETs contained within the Mobile RD. For example, a CMU may indicate the NSAP prefix

47.0019.01.IATA Airline Designator.81

to advertise reachability of all ESs associated with the above prefix. This NSAP prefix may then form part of the overall policy statement,

"For AIS traffic, priority 'x' or greater, and transit delay 'X' or greater, route through preferred ground-service provider through VHF and advertise my reachability of 47.0019.01.IATA Airline Designator.81".

5.5.3 Distribution Lists

Along with path selection, the user's policies may indicate a distribution list of associated ground domains who may have knowledge (and communicate to) the airborne CMU. This distribution list may be generated based on the Traffic Type.

For example, the CMU may allow its mobile reachability to be advertised to:

1. The airline's "home" domain:
   47.0019.01.IATA Airline Designator.01
2. CAA ground domains (for ATC traffic)
   47.1001.01.@US.91
3. Associated ground service provider domains
   47.0019.01.Ground Service Provider Designator.01

i.e.,

"For AIS traffic, priority 'x' or greater, and transit delay "X" or greater, route through preferred ground-service provider through VHF and advertise my reachability of 47.0019.01.IATA Airline Designator.81" and distribute my reachability to my home domain (47.0019.01IATA Airline Designator .01) and my preferred ground service provider (47.0019.01Ground Service Provider Designator.01).

5.5.4 Route Aggregation

Instead of distributing full NSAP addresses, NSAP addresses may be aggregated into a NSAP prefix, and this prefix distributed to neighboring BISs.

For example, when advertising the NSAP prefixes in its own domain, the CMU may advertise:

47.0019.01.IATA Airline Designator.81

Also, the CMU may receive the NSAP prefix from a US FAA ground domain:

47.1001.01.@US.01

to indicate reachability of "all US FAA ground domains".

Aggregation reduces the amount of NSAP information exchanged, and allows policies to be generated on a wider-scale.

6.0 SUBNETWORK DEPENDENT CONVERGENCE

6.1 Introduction

This chapter describes the process to map connectionless oriented network layer protocols defined herein to the protocol used for the air-ground subnetworks. These protocols include ISO 8473, ISO 9542, and ISO 10589. Some air-ground subnetworks may not require all the services provided for in this chapter. The needs of each air-ground and avionics subnetworks are described individually in this chapter.

The need for subnetwork services underlying the ATN Network layer may be summarized as follows:

The avionics Network layer assumes the existence of a service interface using SN_UNITDATA support; that is, the ATN Network layer must be directly supported by either a connectionless-mode subnetwork or a connectionless-mode subnetwork dependent convergence facility (SNDCF).

The avionics Network layer assumes that the subnetwork quality of service (QOS) is either constant and known, or that it may be dynamically determined; this includes considerations of transit delay, protection against unauthorized access, cost determination and residual error probability.

In addition to the standard SNDCF capability defined in ISO 8473, the Air/Ground SNDCP must support the compression of ISO 8473 and ISO 9542 headers to create Subnetwork Dependent PDUs (SNDPDU) and the corresponding expansion of these SNDPDUs. This additional capability is used to support the transfer of NPDUs over the Air-Ground limited bandwidth subnetworks.

6.1.1 CLNS to CONS Convergence

When required, the SNDCF will converge Connection-Less Sub-Network Service primitives issued by the Sub-Network Service user (SNS-user) to the Connection-Oriented Network Service primitives available from the air-ground subnetwork. These procedures should be implemented in accordance with ISO 8473 Section 8.4.

A new virtual circuit may be opened in four circumstances as shown below:

1) When no suitable virtual circuit exists.

2) When all local reference IDs are used.

3) By explicit intervention by system management.

4) When the subnetwork type supports prioritized virtual circuits, and a higher priority virtual circuit is needed.

6.1.2 CLNS Header Compression

The SNDCP will provide a method to minimize the transfer of redundant header information over an established ISO 8208 virtual circuit. For a given NSAP source and destination pair used on a given virtual connection, the SNDCP will assign that pair a local reference ID. For each virtual circuit, each NSAP source/destination pair will be assigned a local reference ID in the range of 0 to 32767. The initiator of the message will assign the local reference ID. The assignment of local reference ID's greater than 127 will require the use of an additional octet. This will be indicated by setting the most significant bit of the local reference ID octet. The aircraft router will assign local reference ID's in the range of 0 to 63 or 128 to 16383. The ground router will assign ID's in the range of 64 to 127 or 16384 to 32767. Therefore, ground defined local reference ID's will have the second most significant bit of the local reference ID set. Both ground and airborne router may make use of all defined reference ID's.

The first (or initial) data NPDU to be sent with a new reference ID is sent in a noncompressed form, containing both the source/destination NSAP pair and an inserted option defining the local reference ID as shown below:

Option Code = H'05'
Option Length = H'1' or H'2'
Option Value = local reference ID

Length	Range of Local Reference ID
1	H'0' - H'7F'
2	H'80' -H'FFFF'

The NPDU used to define the local reference ID has a protocol ID of '1000 0001'. Subsequent NPDU's sent in a compressed mode containing the local reference ID have a protocol ID of '1100 0001'.

COMMENTARY

The value of '1100 0001' was chosen from the selector space "not categorized by this Technical Report" in ISO/TR 9577.

6.1.2.1 Additional Header for Derived NPDU

If segmentation is required for operation with a particular subnetwork, then all compressed DT NPDU headers are appended with three additional fields of information. The data unit ID, segment offset, and total length from the original, uncompressed DT NPDU header are encoded into the final 6 octets of the compressed DT NPDU header.

6.1.3 SATCOM-Specific Subnetwork Dependent Convergence

A separate virtual circuit is established to support each level of priority in use.

6.1.4 AVPAC-Specific Subnetwork Dependent Convergence

AVPAC virtual circuits are not required to support the priority option.

6.0 SUBNETWORK DEPENDENT CONVERGENCE (cont'd)

6.1.5 Mode-S Specific Subnetwork Dependent Convergence

The Mode-S subnetwork has two priority levels. The Mode-S specific dependent convergence needs to map the 16 subnetwork priorities into the two available for Mode-S.

6.1.6 HF Specific Subnetwork Dependent Convergence

There are no HF-specific requirements for convergence or compression currently identified.

6.1.7 Gatelink

Gatelink uses a connection-less subnetwork and does not require either convergence or compression. Refer to ARINC Specification 636 and Characteristic 751.

6.2 Air-Ground SNDC Facilities and Services

6.2.1 Facility for Conveying Service Characteristics

The SNDCF will support a facility for conveying QOS information to the SNS-user to inform or to report to the SNS-user about the QOS which can be expected, or the reasons for rejection. The means by which QOS information is conveyed from the SNDCF to the SNS-user is defined by the following three primitives:

1. SN-FACILITY request;

2. SN-FACILITY indication; and

3. SN-REPORT indication.

6.2.2 Air-Ground Mobile Subnetwork Service Provisions

Avionics as well as Air-Ground NPDUs are processed in their standard form within each avionics Router and end system.

COMMENTARY

These packets may carry a significant amount of header information. While this generally poses no problem over ground-based or avionics subnetworks, the load imposed on a limited-throughput mobile subnetwork would be excessive. Thus, the ATN architecture incorporates a special SNDCF for use in the limited-throughput mobile subnetwork environment.

The Air-Ground SNDCF makes certain assumptions regarding the underlying subnetwork service and access protocol techniques in order to compress NPDUs while in transit through a mobile subnetwork. The resulting packets are referred to as Subnetwork Dependent Protocol Data Units (SNDPDUs). The receiving SNDCF then re-creates standard NPDUs for further processing within the receiving ATN Network entity. This SNDCF architecture allows use of standard CLNP routers to interconnect with the mobile subnetwork while optimizing the use of limited mobile subnetwork bandwidth.

COMMENTARY

These provisions apply to air-ground subnetworks that operate over the RF. Gatelink is not included.

The Air-Ground subnetwork service will conform to the following provisions:

1. Air-Ground subnetworks will support peer-to-peer operations between SNS-users in a connection–mode fashion, using ISO 8208 as a Subnetwork Access Protocol.

2. The Air-Ground SNDCF will establish at least one mobile ISO 8208 connection for each pair of BISs. For subnetworks that support priority, an ISO 8208 connection will be requested by the SNDCF upon receipt of the first NPDU bearing a particular priority. For subnetworks that do not support priority, ISO 8208 connections will be requested by the avionics Network entity upon receipt of the first NPDU. Connections will be released by the avionics Router based on local subnetwork management considerations (e.g., cost of maintaining a connection, cost of establishing a connection, time to establish a connection, etc.). Quality of Service Maintenance (QoSM) parameters, if present, will not be linked to a particular mobile subnetwork connection, but rather will be carried with each converged ATN NPDU via the compressed SNDPDU header.

COMMENTARY

Priority is supported by the satellite subnetwork and is not supported by the Mode S or AVPAC subnetwork.

3. Intrinsic mobile subnetwork residual error probability is assumed to be of an acceptable level for support of the ISO 8208 SNAcP, and for support of the several ATN Network layer protocols. Converged NPDU headers carried via an Air-Ground subnetwork will be assumed to be correct upon receipt and that header checksums, if any, may be recalculated by the SNDCF upon receipt.

4. The "Segmentation" feature of the ATN IP may be used over mobile subnetworks; when converged to the ISO 8208 SNAcP, a M-bit sequence may further segment the PDU depending on minimum SNAcP packet size and user data requirements. Implementations whose Service Data Unit (SDU) size does not exceed the maximum PDU size selected for the SNAcP and are using a segmenting version of ISO 8473, may elect not to send the segmentation header. For SDUs larger than the maximum selected PDU size, segmentation may take place and the segmenting header will be sent as part of the converged PDU. See Section 6.1.

5. ISO 8473 packet reassembly and discard rules will apply in determining if the receiver can accommodate a segmented PDU.

6.0 SUBNETWORK DEPENDENT CONVERGENCE (cont'd)

6.2.2 Air-Ground Mobile Subnetwork Service Provisions (cont'd)

COMMENTARY

This feature is maintained to allow use of COTS OSI (e.g., GOSIP conformant) software either in Avionics or in ground based implementations as a stable basis for development.

6. Avionics Network entities will create ATN IP packets containing two IP options; namely Priority and Quality of Service Maintenance. Valid IP Priority will be carried in the least significant four bits of a one octet SNDPDU QOS field. The Quality of Service Maintenance parameter consists of four flags, carried in the most significant four bits of the SNDPDU QOS field.

7. The ISO 8208 D-bit will not be used for delivery confirmation.

6.2.3 Mobile SNDCF Protocol Identifiers

A protocol identifier will be used to identify the Network Layer protocols. The ATN Manual defines the format of SNPDUs.

6.2.4 Mobile SNDPDU Formats for ISO 8473 IP

The CLNP Data NPDU header will be compressed. Refer to the ATN Manual.

6.3 Avionics SNDCF

This section, and its subsections, defines the avionics SNDCF for the ARINC Specification 429 link layer, ARINC Specification 629 link layer and for an Onboard Local Area Network (OLAN).

In accordance with Annex A of ISO 8473, primitives defined for providing the underlying service used by the Internetworking Protocol (IP) map directly onto the DL_UNITDATA Request and Indication primitives defined for the Connectionless-mode Data Link Service. In the ES-IS avionics environment, the IP sublayer issues SN_UNITDATA primitives with an SN_Address parameter corresponding to the Williamsburg data link address; i.e. the ARINC 429 System Address Label. This essentially acts as a pass through function.

COMMENTARY

Although ARINC 429 is not a truly connectionless protocol, the Williamsburg version of ARINC 429 exhibits some connectionless link layer characteristics, and is treated as such in this document.

The ES-IS Routing Protocol (ISO 9542) is also supported through an SNDCF directly over the ARINC 429 interface between the onboard IS and ESs. The PDUs associated with the ES-IS Routing Protocol are the ESH (End System "Hello"), ISH (Intermediate System "Hello"), and the RD (Redirect) PDUs. The formats of the PDUs are defined in Section 4.3.2 of "ISO 9542 Protocol Functions and PDU Structures". They are generated by ISO 9542 protocol functions (see Section 4.3). In addition, an ISO 8208 Subnetwork Access Protocol (SNACP) does not exist between ISO 8473/9542 and Williamsburg on the avionics subnetwork.

COMMENTARY

Note that, in this case, ARINC 429 Williamsburg which is a data link layer protocol acts as the subnetwork access protocol for the avionics subnetwork.

Since the generation of ES-IS PDUs, as a function of ISO 9542, are well-defined as packet transmissions across this link, the function required by the SNDCF is minimal and only involves the mapping of primitives and link addresses.

6.3.1 Avionics ARINC 429 Link Layer

6.3.1.1 ARINC 429 Connectionless-mode Data Link Service

The following subsections describe the primitives and parameters associated with the ARINC 429 bit-oriented services. A primitive is an input to, or an output from the protocol state machine. No specific primitive implementation is implied in this document. Service primitive parameters specify the information that must be available to the receiving entity.

The Data Link Service (DLS) provides the means by which the DLSDUs are transmitted from one source DLSAP to a destination (sink) DLSAP in a single service access. In the abstract sense, the data link connectionless– mode service can be modelled as a permanent association between the two DLSAPs. It is self-contained in that all the information required to deliver the DLSDU is presented to the DLS provider, together with the user data to be transmitted. Thus no establishment or release of a data link connection is required.

The types of primitives needed for the Data Link connectionless mode data transmission service are:

DL_UNITDATA.request
DL_UNITDATA.indication

The DL_UNITDATA.request primitive, generated by the SNDCF, is passed to the link layer to request that a Link Protocol Data Unit (LPDU) be sent using connectionless procedures. The DL_UNITDATA.indication primitive, generated by the link layer, is passed to the SNDCF sublayer to indicate the arrival of an LPDU.

The only parameter required is the DL-DATA. This parameter allows the transmission of DL-DATA between Data Link Service users. The limit of octets sent and the configuration of DLSAP addresses are known by the DL entity on a priority basis (As specified in ARINC 429).

6.0 SUBNETWORK DEPENDENT CONVERGENCE (cont'd)

6.3.1.2 ARINC 429 Connectionless-mode Data Link Protocol

Refer to ARINC Specification 429, Section 2.5 for a complete protocol description of the ARINC 429 bit-oriented link layer protocol.

6.3.2 Avionics OLAN

6.3.2.1 Avionics OLAN Service

Avionics OLAN subnetworks are assumed to conform to ISO 8802-2 Class 1 service, meaning that they provide unacknowledged connectionless-mode service only. This service is precisely that needed by ISO 8473 at the subnetwork service interface.

The SNDCF performs a mapping of the OLAN service onto the underlying service assumed by ISO 8473. The mapping is as follows. The generation of an SN-UNITDATA Request by IP causes the SNDCF to generate the DL-UNITDATA Request to the data link layer. The receipt of a DL-UNITDATA Indication from the data link layer causes the SNDCF to generate the SN-UNITDATA Indication to IP. No explicit Subnetwork Dependent Convergence protocol control information is exchanged between Network-entities to provide this mapping of service.

The addresses used in the SN-UNITDATA request and indication primitives are the seven-octet SNPA, consisting of the six-octet Medium Access Control (MAC) address plus the one-octet LLC Service Access Point address.

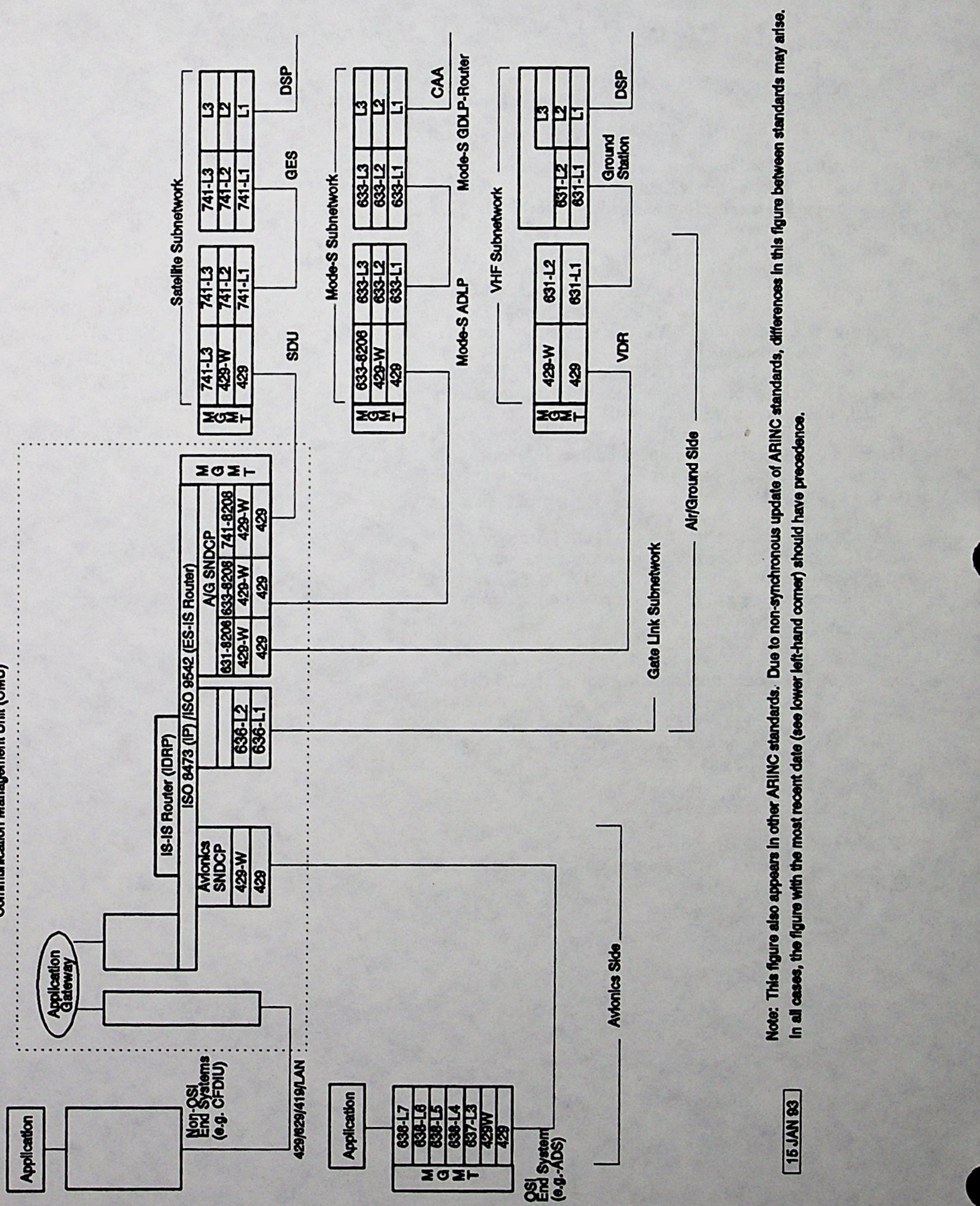
6.3.2.2 Avionics OLAN Protocol

Any OLAN protocol that supports the service definition as defined by ISO 8802-2 can be supported by the SNDCF defined in the section above. In particular, the above SNDCF can be used to support avionics FDDI as defined in ARINC Specification 636.

6.3.2.3 Ethernet LAN (ELAN)

This is a placeholder for the definition of the SNDCF to support an interface with subnet utilizing ELAN link layer.

ATTACHMENT 1
PROTOCOL ORGANIZATION



Note: This figure also appears in other ARINC standards. Due to non-synchronous update of ARINC standards, differences in this figure between standards may arise. In all cases, the figure with the most recent date (see lower left-hand corner) should have precedence.

15 JAN 93

Figure 1-1 Aircraft Protocol Organization

ATTACHMENT 1 (cont'd)
PROTOCOL ORGANIZATION

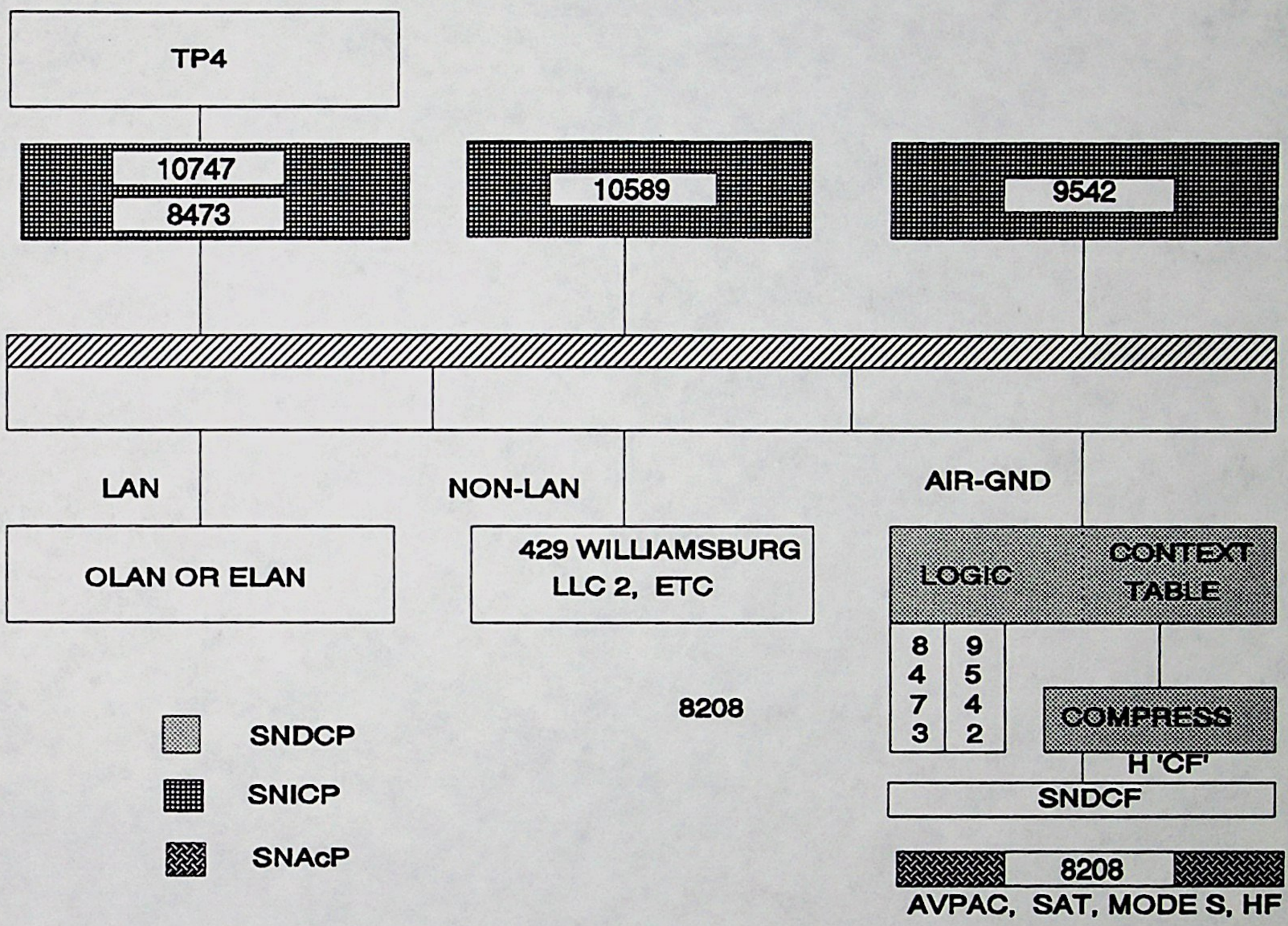


Figure 1-2 Subnetwork Dependence Convergence Protocol

ATTACHMENT 1 (cont'd)
PROTOCOL ORGANIZATION

Figure 1-3 Reserved

ATTACHMENT 2
INTERNETWORK LAYER

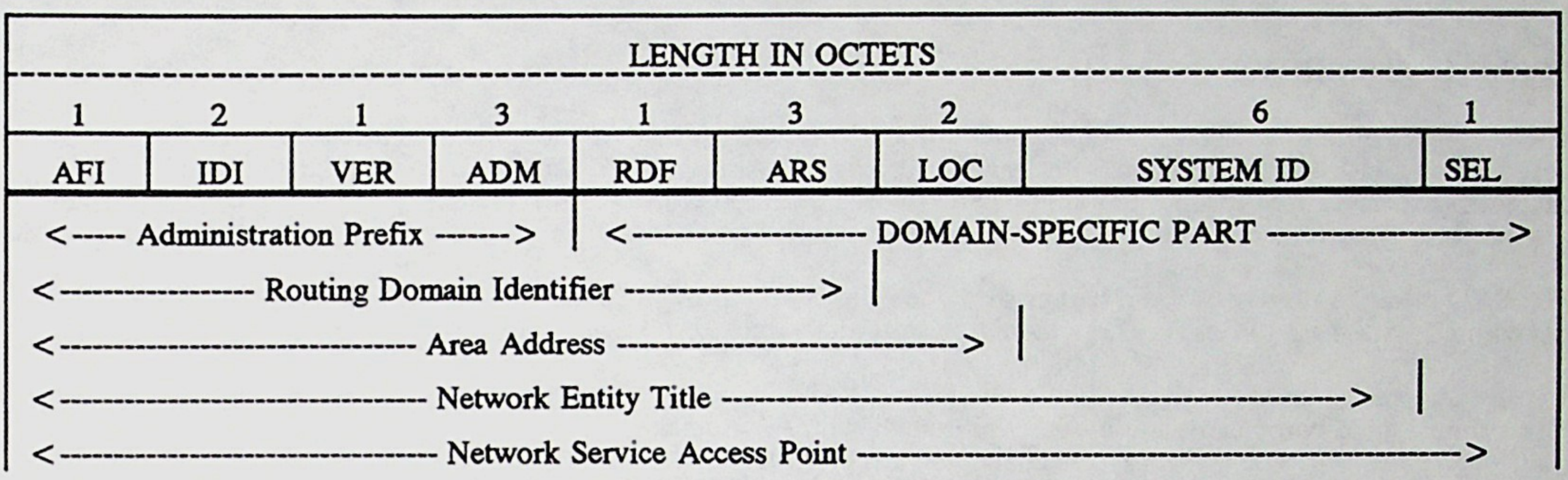


Table 2.1 ATN NSAP Field Descriptions

FIELD	ADMIN AUTHORITY	SIZE	DESCRIPTION
AFI	ISO	1 octet	binary "47" (current ICD)
IDI	ISO	2 octets	binary "0027" (ICAO and IATA ICD).
VER	ICAO	1 octet	Version number (aligned with US GOSIP).
ADM	IATA & ICAO	3 octets	ICAO or IATA organization ID.
RDF	ICAO	1 octet	Routing Domain Format. 1 octet format ID indicates fixed or mobile RD.
ARS	RDI=mobile: ICAO	3 octets	Area Routing Selector. 24-bit ICAO-registered aircraft ID.
	RDI=fixed: Owner of ADM		Area Routing Selector. Local issue.
LOC	Owner of ADM	2 octets	Subnetwork ID.
Sys ID	Owner of ADM	6 octets	System Identifier (See Section 2.2.1.2.6)
SEL	ISO	1 octet	Network user selector.

ATTACHMENT 2 (cont'd)
INTERNETWORK LAYER

FORMAT DESCRIPTION

The ATN NSAP address format should contain nine (9) fields. All fields should be right justified. Decimal or hexadecimal fields should be filled with leading "0" digits. Alphabetic fields should be filled with leading "@" characters. Unspecified leading bits in all fields should be filled with the binary value "0". Reserved bits and fields should not be interpreted or modified, and are assumed to be binary value zero.

The BCD numeric digit set should comprise the ten digits "0" through "9". BCD field components should be represented with 4-bit binary numbers taking on only the values zero through nine.

The hexadecimal numeric digit set should comprise the sixteen digits "0" through "9", and "a" through "f". Hexadecimal field components should be represented with 4-bit binary numbers.

The International Alphabet No. 5 (IA-5) codes is used to encode some IATA or ICAO address components.

The Base 37 binary encoding of alphanumerics which enumerate two or three digit alpha-numeric IATA or ICAO address components will include the @ sign as a null character. Thus, progressive coding in IA-5 sort order would be represented as follows:

Table 2.2 Base 37 Encoding

CODE	DECIMAL	HEXIDECIMAL
000	0	0
-	-	-
-	-	-
-	-	-
009	9	9
00@	10	-
00A	11	-
-	-	-
-	-	-
00Z	36	24
-	-	-
-	-	-
ZZZ	50,652	C5DC

ATTACHMENT 3
INTERNETWORK SERVICE

Table 3.1 Provision of Functions for Conformance

FUNCTION	SOURCE ES	ALL IS	DEST. ES
PDU Composition	M	M (Note 1)	M (Note 1)
PDU Decomposition	M	-	M
Header Format Analysis	-	M	M
PDU Lifetime Control	-	M	I
Route PDU	M	M	-
Forward PDU	M	M	M (Note 1)
Segment PDU	M	M	-
Reassemble PDU	-	N	M
Discard PDU	-	M	M
Error Reporting	M	M	M
Header Error Detection	M	M	M
Padding	-	I (Note 4)	M (Note 4)
Security	-	N (Note 3)	N (Note 3)
Complete Source Routing	-	N (Note 3)	-
Partial Source Routing	-	N (Note 3)	-
Complete Route Recording	-	N (Note 2)	-
Partial Route Recording	-	Y (Note 3)	-
QOS Maintenance	-	M	-
Priority	-	M	-
Congestion Notification	-	M	-

Legend:

- `-` Function not applicable
- I Implementation option
- M Mandatory function; this function must be implemented in the specified systems.
- N Function not to be supported
- Y Function is supported

Note 1: The support of the PDU Composition and Forward PDU functions are necessary for the generation of Error Report PDUs.

Note 2: If an implementation does not support this function and the function is selected in a PDU, the PDU shall be discarded. If the Error Report Flag is set, an ER PDU shall be generated and forwarded to the originating network entity.

Note 3: If an implementation does not support this function, and the function is selected by an option in a PDU, the function is not performed and the PDU is processed exactly as though the function had not been selected. The PDU shall not be discarded for this reason.

Note 4: See Section 3.3.2.5.1.

ATTACHMENT 3 (cont'd)
INTERNETWORK SERVICE

Initial PDU - Too large for subnetwork

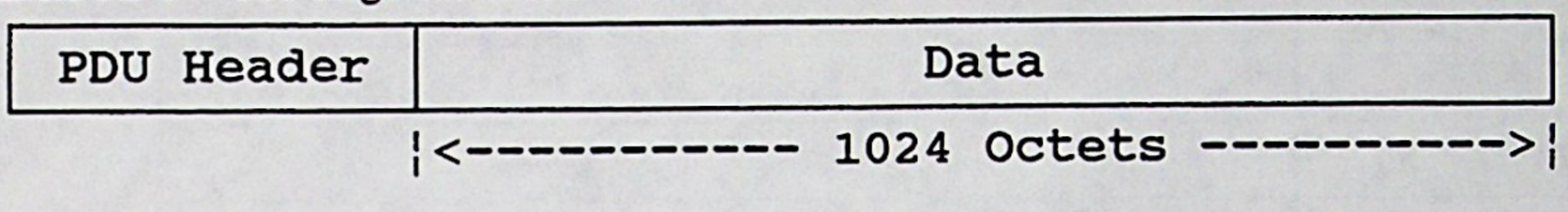
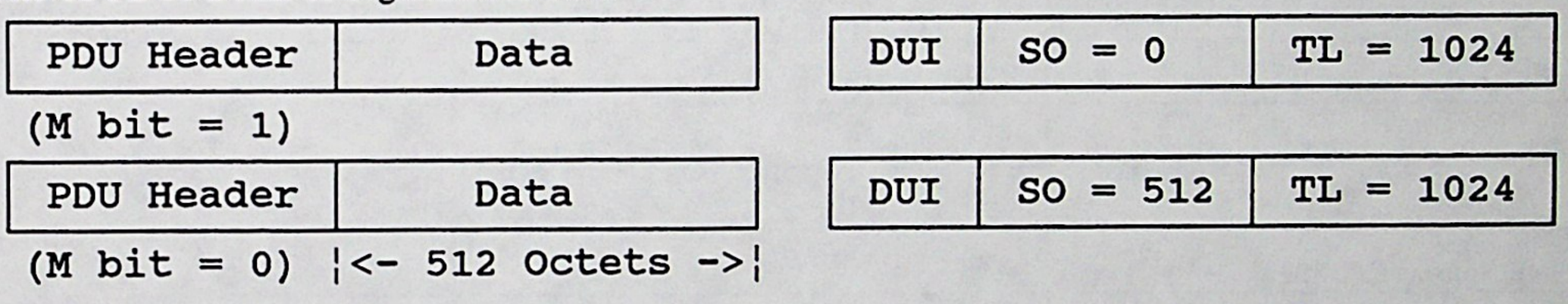


Figure 3-1A PDU Before Segmentation

Derived PDUs Detail of Segmentation Parts



Legend:

DUI	Data Unit Identifier: Same for all derived PDUs
SO	Segment Offset
TL	Total Data Length

Figure 3-1B PDU After Segmentation

Initial PDU Restored

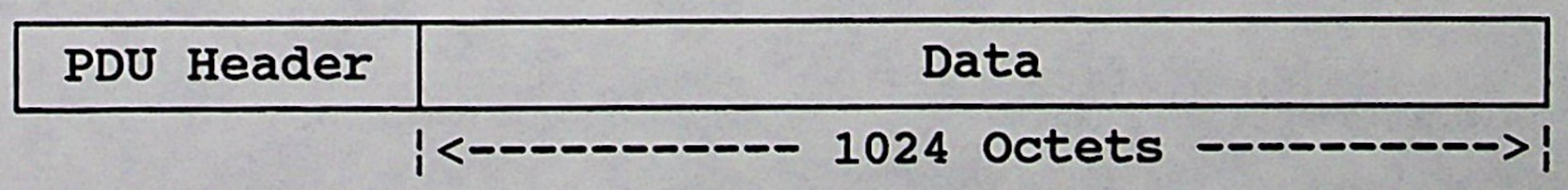


Figure 3-1C PDU After Reassembly

ATTACHMENT 3 (cont'd)
INTERNETWORK SERVICE

Table 3.2 ATN Priority Levels

The following table introduces air-ground message priority values. Not all air-ground subnetworks support different priority levels. Refer to the documentation of each individual subnetwork for details.

ASSIGNMENT (PER ATN MANUAL) ⟨1⟩	MESSAGE DESCRIPTION	CLNP VALUE	ENCODED VALUE
0	Urgent Network Management	14 (highest)	0000 1110
1 (lowest)	Distress Communications	13	0000 1101
2	Urgent Communications	12	0000 1100
3	Radio Direction Finding/Navigation	11	0000 1011
4	Flight Safety Communications	10	0000 1010
5	Meteorological Communications	9	0000 1001
6	Flight Regularity Communications	8	0000 1000
7	Aeronautical Information Services	7	0000 0111
8	Aeronautical Administrative Messages	6	0000 0110
9	Administrative Network Management	5	0000 0101
10	<reserved>	4	0000 0100
11	Urgent Priority Administrative, U.N. Charter Communications	3	0000 0011
12	High Priority Administrative, State/Government Communications	2	0000 0010
13	Normal Priority Administrative	1	0000 0001
14 (highest)	Low Priority Administrative	0 (lowest)	0000 0000

⟨1⟩ In the ATN Manual scheme, 0 represents highest priority level. In the AEEC standards, the higher number represents the higher priority.

COMMENTARY

The encoding scheme shown above was chosen to be consistent with ISO 8473. This results in a reverse encoding from that defined in ISO 8073.

ATTACHMENT 3 (cont'd)
INTERNETWORK SERVICE

Table 3.3 Quality of Service (QOS)

To be supplied	

ATTACHMENT 4
ES-IS PROTOCOLS

Table 4.1 Selected Provisions of ISO 9542

PROVISIONS OF ISO 9542	SYSTEM TYPE	
	ES	IS
Report Configuration	M	M
ESCT Generation	-	O
Record Configuration	M	M
ESCT Processing	O	-
Flush Old Configuration	M	M
Query Configuration	A	-
Configuration Response	A	-
Configuration Notification	O	O
Request Redirect	-	M
Record Redirect	M	-
Refresh Redirect	O	-
Flush Old Redirect	M	-
PDU Header Error Detection		
Checksum Validation	M	M
Checksum Generation	O	O
Protocol Error Processing	M	M

LEGEND:

- \- = Not applicable.
- A = Mandatory only for ESs connected to avionics subnetwork.
- M = Mandatory function; this function should be implemented.
- N = Non-Supported function
- O = Optionally implemented function

ATTACHMENT 5
IDRP FORMAT TABLES

Table 5.1 List of Air-Ground IDRP Managed Objects

NAME OF PARAMETER	VALUE
EXTERNAL - BIS - NEIGHBORS	List of NETs
INTERNAL - SYSTEMS	List of NSAP Prefixes
LOCAL - RDI	Unique RDI of the CMU
RDC - Config	
Maximum PDU Size	31 < value < 65536
Hold Time	> 1800 sec
Outstanding PDUs	1
Authentication Code	0 - Other values to be defined
Retransmission Timer	Default 5 seconds
Close WaitDelay Period	Default 10 seconds
RDTransitDelay	
RDLRE	
LocExpense	Not used
RIDAttsSet	Set RIB - Atts supported by the CMU

ATTACHMENT 6
QUEUE LENGTH AVERAGING ALGORITHM

The algorithm to determine average queue length makes use of the following variables:

t = Current time
t_i = time of i^{th} arrival or departure event
q_i = number of packets in the system after the event
T_0 = time at the beginning of the previous cycle
T_1 = time at the beginning of the current cycle

The algorithm consists of three components:

1. Queue Length Update: Beginning with $q_0 = 0$,
if the i^{th} event is an arrival event, $q_i = q_{i-1} + 1$,
if the i^{th} event is a departure event, $q_i = q_{i-1} - 1$

2. Queue Area (integral) update:

$$\text{Area of the previous cycle} = \Sigma\ q_{i-1}\ (t_i - t_{i-1})$$

$$t_i \in (T_0, T_1)$$

$$\text{Area of the current cycle} = \Sigma\ q_{i-1}\ (t_i - t_{i-1})$$

$$t_i \in (T_1, t)$$

3. Average Queue Length Update:

Average Queue length over the two cycles

$$\frac{\text{Area of the two cycles}}{\text{Time of the two cycles}} = \frac{\text{Area of the two cycles}}{t - T_0}$$

Note: This table has been included for the reader's convenience. Version 4 of the NIST/OIW Stable Implementors Agreements has precedence. Refer to Section 5.1 under Subsection e), "Optional functions are as follows:" for the applicable averaging information.

Note: Section 9.4.7 of ATN Manual defines a different implementation.

APPENDIX A
NETWORK LAYER MANAGEMENT INFORMATION BASE

A.1 Network Layer Managed Objects

This appendix describes the Network Layer (NL) managed objects (MO) that must be managed by local systems management, NL protocols, or Network Management applications in order for the NL protocols to operate correctly. The scope of this appendix includes the (MO) class, name bindings, attributes, parameters, behavior, notifications, and operations of each NL MO which is relevant to the NL protocols defined in this specification. The complete MO definitions for standardized OSI objects are defined in CD 10733 and CD 10747, and are not repeated in this standard. Where information on standard MOs is not provided or incomplete (such as IDRP and optional packages), a complete specification is included. In addition, complete object definitions are included for aeronautical specific objects such as the air/ground convergence protocol.

COMMENTARY

The material in this Appendix is subject to ongoing work.

Refer to ISO CD 10733 for descriptions of standardized NL MOs. The following NL MOs are included in this appendix:

The Network Subsystem Managed Object
The Network Entity Managed Object
The NSAP Managed Object
The CLNS Managed Object
The Circuit Managed Object
- Circuit ISO 9542 ES Package
- Circuit ISO 9542 IS Package
- Circuit ISO 8473-ISO 8208 SNDCF Package
- Circuit Idle Timer Package
- Circuit Reserve Timer Package
- Circuit Initial Minimum Timer Package
- Circuit ISO 8473-IS0 8802 SNDCF Package
- Circuit CODL Service Package
- Circuit CLDL Service Package
- Circuit ATN Air/Ground Convergence Package
- Circuit Williamsburg 429 Package

The CONS Managed Object
The X.25 PLE Managed Object
- ISO 8208 Online Registration Package

The X.25 PLE Initial Values Managed Object Class
The ISO 8208 Virtual Call Initial Values Managed Object
- ISO 8208 Receiving Window Rotation Recovery Procedures Packaged
- ISO 8208 Transmitting Window Rotation Recovery Procedures Package
- ISO 8208 Packet Retransmission Procedures Package

The Virtual Call Managed Object
The Switched Virtual Call Managed Object
The Permanent Virtual Circuit Managed Object
The IDRP Managed Object

A.2 The Network Subsystem Managed Object

The Network Subsystem MO must be present on each ES/IS. It exists to provide a container for the Network Entity MO. This MO is as defined in CD 10733 with the following clarifications:

Only one MO instance is allowed.

The CREATE and DELETE operations will not be allowed for avionic systems.

Only a single NET for the NL is allowed.

The NET should have the same abstract syntax as an ATN NSAP Address.

A.3 The Network Layer Entity Managed Object

(TBD)

A.4 The Network Service Access Point (NSAP) Managed Object

The NSAP MO must be present on all ES/IS. This MO is as defined in CD 10733 with the following clarifications:

The NSAP-MO-Name ATTRIBUTE value should be an ATN NSAP Address.

There must be one instance of this MO for each Network Service User.

The TransportClientRelationship should be an asymmetric service relationship where the NL is the service provider and the transport or higher layer is the service user.

The TransportClientRelationship ATTRIBUTE value should be a set of exactly one Distinguished Name which uniquely identifies the network service user.

A.5 The Connectionless-mode Network Service (CLNS) Managed Object

The CLNS MO must be present on each ES/IS. This MO is as defined in CD 10733 with the following clarifications:

Only one MO instance is allowed.

The CREATE and DELETE operations will not be allowed for avionic systems.

The Enable and Disable actions are not allowed for avionic systems.

A.6 The Circuit [Subnetwork Point of Attachment (SNPA)] Managed Object

The CIRCUIT (SNPA) MO must be present on all ES/ISs. The operation of specific subnetwork protocols over a particular CIRCUIT (SNPA) are managed through the inclusion of the specific protocol PACKAGE when an instance of this MO is created. This MO is as defined in CD 10733 with the following clarifications:

One instance of this MO must be present for each CIRCUIT (SNPA) of the ES/IS.

APPENDIX A (cont'd)
NETWORK LAYER MANAGEMENT INFORMATION BASE

The CIRCUIT (SNPA) Default SDU size is XXX for the A/G link and implementation specific for the avionic subnetworks.

The CIRCUIT (SNPA)-MO-Name value must be XXXX.

The parameters for the enable and disable actions must be specified, and the form of the CIRCUIT (SNPA)-MO-Name must be specified.

A.6.1 CIRCUIT (SNPA)-ISO9542ESPackage PACKAGE

The CIRCUIT (SNPA)-ISO9542ESPackage PACKAGE must be present on all avionic ESs. This Package is as defined in CD 10733 with the following clarifications:

(TBD)

A.6.2 CIRCUIT (SNPA)-ISO9542ISPackage PACKAGE

The CIRCUIT (SNPA)-ISO9542ISPackage PACKAGE must be present on all ISs. This Package is as defined in CD 1073♫3 with the following clarification:

An IsReachabilityChange ATTRIBUTE must be included in this Package to support IS to IS operation over the air/ground link.

A.6.3 CIRCUIT (SNPA)-ISO8208Package PACKAGE

The CIRCUIT (SNPA)-ISO8208Package PACKAGE must be present on all ES/ISs which have CIRCUIT (SNPA)s to air/ground subnetworks. This PACKAGE is as defined in CD 10733 with the following clarifications:

(TBD)

A.6.4 Circuit Idle Timer Package

(TBD)

A.6.5 Circuit Reserve Timer Package

(TBD)

A.6.6 Circuit Initial Minimum Timer Package

(TBD)

A.6.7 CIRCUIT (SNPA)-ISO8802Package PACKAGE

The CIRCUIT (SNPA)-ISO8802Package is optional and only present with the CIRCUIT (SNPA) MO in all ESs/ISs which are attached to an ISO 8802 Local Area Network. This package is as defined in CD 10733 with the following clarifications:

(TBD) (Notifications for this MO must be defined.)

A.6.8 Circuit CODL Service Package

(TBD)

A.6.9 Circuit CLDL Service Package

(TBD)

A.6.10 CIRCUIT(SNPA)-AtnAgConvergenceProtocol Package PACKAGE

CIRCUIT (SNPA)-AtnAgConvergenceProtocolPackage must be present with the CIRCUIT (SNPA) MO in all ESs/ISs which are attached to an air/ground subnetwork. This package is an ATN specific package and is defined as follows:

(TBD)

Full GDMO definitions for this MO are found in Attachment 6.

A.6.11 CIRCUIT (SNPA)-429WilliamsburgPackage PACKAGE

The CIRCUIT (SNPA)-429WilliamsburgPackage is optional and only present in ESs/ISs, which attaches to a subnetwork using Williamsburg 429 link layer protocol. This package is an avionics specific package and is defined as follows:

(TBD)

Full GDMO definitions for this MO are found in Attachment 6.

A.7 Connection Mode Network Service (CONS) Managed Object

(TBD)

A.7.1 ISO 8208 Managed Object (MO)

The ISO 8208 Managed Object (MO) must be present in all ESs/ISs which are attached to an air/ground link. This MO is as defined in CD 10733 with the following clarifications:

Creation/Deletion is not allowed.

Only one instance of this MO may exist in a system.

The single value "ISO8208" is allowed for the ISO8208-MO-Name ATTRIBUTE.

A.7.2 (TBD)

A.8 The X.25 PLE Managed Object

The X.25 PLE MO must be present in all ESs/ISs which are attached to an air/ground link. Multiple instances of this MO may exist. This MO is as defined in CD 10733 with the following clarifications:

(TBD)

APPENDIX A (cont'd)
NETWORK LAYER MANAGEMENT INFORMATION BASE

A.9 X.25 PLE Initial Values Managed Object Class

(TBD)

A.10 ISO 8208 Virtual Call Initial Values Managed Object

The ISO8208VirtualCallIVMO exists in order to permit the initial values of a virtual call to be specified in advance by systems management. This MO must be present in all systems that are attached to air/ground links. Multiple instances of this MO may exist in a system. When a virtual call is desired, the values of the proposed packet size and proposed window size may be specified by specifying an instance of this MO which has the desired values. This MO is as defined in CD 10733 with the following clarifications:

(TBD)

A.10.1 ISO 8208 Receiving Window Rotation Recovery Procedures Package

(TBD)

A.10.2 ISO 8208 Transmitting Window Rotation Recovery Procedures Package

(TBD)

A.10.3 ISO 8208 Packet Retransmission Procedures Package

(TBD)

A.11 The Virtual Call Managed Object

The Virtual Call MO is a generic MO from which both the Switched Virtual Call and the Permanent Virtual Circuit MOs are derived. This MO is never instantiated. It must be present in all ES/ISs which are attached to air/ground links. This MO is as defined in CD 10733 with the following clarifications:

(TBD)

A.12 The Switched Virtual Call Managed Object

The switchedVirtual Call MO is derived from the VirtualCall MO. An instance of this MO is created by the operation of the X.25 PLE. One instance of this MO must exist for each VC which has been established. This MO must be present in all ES/ISs which are attached to air/ground links. This MO is as defined in CD 10733 with the following clarifications:

> An instance of this MO is created only upon successful establishment of a call.
>
> The callingAddressExtension ATTRIBUTE will always be an ATN NSAP address.

A.13 The Permanent Virtual Circuit Managed Object

The permanentVirtualCircuit MO is derived from the VirtualCall MO. An instance of this MO is created and deleted by systems management. One instance of this MO must exist for each Permanent Virtual Circuit (PVCs). This MO is only present if PVCs are supported. This MO is as defined in CD 10733 with the following clarifications:

An instance of this MO is created and deleted only by management action.

A.14 The InterDomain Routing Protocol Managed Object

The implementation of Inter-Domain Routing Protocol (IDRP) is optional. See Chapter 5, Inter-Domain Routing Protocol.

The managed object definitions for IDRP are contained in the IDRP Committee Draft (CD) 10747. The managed object definitions allow systems management to monitor and control the operation of the inter-domain routing functions in a BIS. If IDRP is implemented, the following objects defined in IDRP CD 10747 should be supported:

(TBD)

Full GDMO definitions for the idrp MO are found in Attachment 6.

A.14.1 The IDRP Config Managed Object

The idrp_config MO is derived from Technical and Office Protocols (TOP) and is named by the networkEntity MO. This MO defines the configuration of the IDRP on a BIS. One instance of this MO should exist on each IS which supports IDRP. This MO should exist inherently in an IS which supports IDRP and creation/deletion should not be allowed by systems management. This MO should be instantiated when an IS is initialized. This MO is as defined in CD 10747 with the following clarifications:

> An instance of this MO is created when a system initializes.
>
> The startevent and stopevent actions may be used by a systems management entity to request a start of communication with a remote BIS peer. Otherwise, BIS peer communications should be initiated by receipt of an ISO 9542 ISH PDU.
>
> The RD QOS attribute values (i.e., RDTransitDelay, RDLRE, LocExpense) should not include the values for inter-domain links (i.e., the air/ground link).
>
> The RDC-Config attribute should contain a null value.
>
> The Local-RDI should contain an ATN RDI.

APPENDIX A (cont'd)
NETWORK LAYER MANAGEMENT INFORMATION BASE

COMMENTARY

The Object Identifiers for all definitions are not complete.

As currently defined, the only operation that can be performed on the attributes is GET. Whether the SET operation will be required for some of the attributes for avionic BIS's is for further study.

The notifications that are currently defined may not be sufficient. Further analysis is required.

Limits should be placed on attribute values for the ATN.

A.14.2 Local BIS Managed Objects for BIS

The following MO's are derived from the idrp.config MANAGED OBJECT CLASS:

A.14.2.1 INTERNAL-BIS

Information within the INTERNAL-BIS MO allows a BIS to identify the location and identity of all other BISs within its routing domain.

A.14.2.2 INTRA-IS

Information within the INTRA-IS MO permits a BIS to identify the adjacent systems to which it can deliver inbound routed network Protocol Data Units (PDU's) whose destination is within the routing domain.

A.14.2.3 EXTERNAL-BIS-NEIGHBORS

Information within the EXTERNAL-BIS-NEIGHBORS MO contains a list of the location and identity of each BIS located in an adjacent Routing Domain, reachable via a single subnetwork hop.

A.14.2.4 INTERNAL-SYSTEMS

The contents within the INTERNAL-SYSTEMS MO are used by the BIS to construct network reachability information which lists the NSAP prefixes that apply to the systems contained within the routing domain.

A.14.2.5 Local-RDI

Information within the Local-RDI MO contains the Routing Domain Identifier of the routing domain in which the BIS is located.

A.14.2.6 RDC-Config

The RDC-Config MO information identifies all the Routing Domain Confederations (RDCs) to which the Routing Domain (RD) of the local BIS belongs, and describes the nesting relationships that exist between them.

A.14.2.7 LocalSNPAs

The LocalSNPAs MO contains the list of this BIS's SNPAs.

A.14.2.8 MultiExit

The MultiExit MO indicates whether this BIS will use the MULTI_EXIT_DISC attribute to decide between otherwise identical routes. The MultiExit parameter is used as the default value for the multi_exit_disc function in policy decisions.

A.14.2.9 Routeserver

The routeserver MO indicates whether this BIS may set the "IDRP_Server_Allowed" field in the NEXT_HOP attribute to X"FF" for BIS to BIS UPDATE BISPDUs. If this variable is true, then in accordance with local policy, the IDRP_Server_Allowed field may be set on some UPDATE BISPDUs that this BIS sends. If this attribute is set to false, then no UPDATE BISPDUs will be sent by this BIS with NEXT_HOP attributes containing an "IDRP_Serverflag" equal to X"FF".

A.14.2.10 MaximumPDUsize

The MaximumPDUsize MO field contains a 2 octet unsigned integer that is the maximum number of octets that this BIS is able to handle in an incoming BIS-PDU. Every BIS is required to support a preassigned minimum number of PDUs.

A.14.2.11 HoldTime

The HoldTime MO field contains a 2 octet unsigned integer that is the maximum number of seconds that may elapse between the receipt of successive KEEPALIVE, UPDATE, and/or CHECKSUM PDUs.

The HoldTime MO should have a value of 1800 seconds. KEEPALIVE PDUs are expected every 600 seconds.

A.14.2.12 OutstandingPDUs

The OutstandingPDUs MO field contains a one octet unsigned integer that is the maximum number of BIS-PDUs that may be sent to this BIS without receiving an acknowledgment.

A.14.2.13 AuthenticationCode

The AuthenticationCode MO field contains a one octet unsigned integer that indicates the authentication mechanism being used.

See Chapter 5, Inter-Domain Routing Protocol, for a definition of the mechanism by which authentication is to be accomplished.

APPENDIX A (cont'd)
NETWORK LAYER MANAGEMENT INFORMATION BASE

A.14.2.14 RetransmissionTimer

The RetransmissionTimer MO field contains the length of time (in seconds) considered 'reasonable' for the round trip time characteristics of a BIS-PDU connection. Timer values should be dynamically calculated, allowing a reasonable amount of time for a return acknowledgment to be received.

A.14.2.15 CloseWaitDelayPeriod

The CloseWaitDelayPeriod MO field contains the length of time (in seconds) considered reasonable before receiving a CEASE PDU, or STOP event. If the timer expires, the state should change to CLOSED.

A.14.2.16 RDTransitDelay

The RDTransitDelay MO field contains the length of time (in increments of 500 ms) of the average transit delay associated with the local RD that would be experienced by a Subnetwork Service Data Unit (SNSDU) size of 512 octets while traversing the RD.

A.14.2.17 RDLRE

The Routing Domain Local Residual Error (RDLRE) MO value is determined by the average ratio of lost, duplicated, or incorrectly delivered SNSDUs to the total number of SNSDUs transmitted by the SNDCF during a measurement period.

A.14.2.18 LocExpense

The LocExpense MO contains the value of the Expense associated with traveling a given local routing domain.

A.14.2.19 RIBAttsSet

The RIBAttsSet MO information is the enumerated set of the Routing Information Base (RIB) attributes supported by this BIS.

A.14.2.20 Capacity

The Capacity MO indicates the traffic carrying capacity of this Routing Domain.

A.14.2.21 Priority

The Priority MO indicates the lowest value of the ISO 8473 priority parameter that this RD will provide forwarding services for.

A.14.2.22 Version

This version MO indicates the IDRP protocol version that this machine defaults to using.

A.14.2.23 maxRIBIntegrityCheck

The maxRIBIntegrityCheck MO contains the maximum time in seconds between checking of the Adj-RIBs-In by a local mechanism. If corrupt Adj-RIB-In is detected, the BIS should purge the offending Adj-RIB-In.

A.14.2.24 maxIntegrity Timer

The maxIntegrity Timer MO indicates the timer that measures in seconds the time remaining until the Adj-RIBs-In must be checked by a local mechanism. If a corrupt Adj-RIB-In is detected, the BIS should purge the offending Adj-RIB-In.

A.14.3 Adjacent BIS Peer Managed Objects

The adjacentBIS MO is derived from Top and is named by the idrp_Config MO. This MO defines the attributes and parameters of the connections that a BIS has with adjacent BIS's. One instance of this MO should exist for each adjacent BIS connection. This MO may not be created or deleted. This MO should be instantiated when a BIS connection is initiated. This MO is as defined in IDRP CD 10747 with the following clarifications:

An instance of this MO is created when an OPEN PDU is initiated.

A.14.3.1 BIS NET

The BIS_NET MO contains the remote BIS NET of this BIS to BIS connection.

A.14.3.2 BIS RDI

The BIS_RDI MO contains the remote BIS RDI of this BIS to BIS connection.

A.14.3.3 BIS RDC

The BIS_RDC MO contains the remote BIS RDC of this BIS to BIS connection.

A.14.3.4 BISnegotiatedversion

The BISnegotiatedversion MO contains the negotiated version of the IDRP protocol that this BIS to BIS connection is using.

A.14.3.5 BISpeerSNPAs

The BISpeerSNPAs MO contains the SNPAs announced by the remote BIS of this BIS to BIS connection.

A.14.3.6 Authentication Type

The Authentication_type MO contains the remote BIS sent in the OPEN BISPDU in this BIS to BIS connection.

A.14.3.7 State

The State MO contains the current state of BIS to BIS communication in the local BIS.

A.14.3.8 Lastseqnosent

The Lastseqnosent MO contains the last sequence number sent to the remote BIS from this local BIS on this BIS to BIS connection.

APPENDIX A (cont'd)
NETWORK LAYER MANAGEMENT INFORMATION BASE

A.14.3.9 Lastseqnorecv

The Lastseqnorecv MO contains the last sequence number received from the remote BIS by the local BIS on this BIS to BIS connection.

A.14.3.10 Lastacksent

The Lastacksent MO contains the number of the last ack sent to the remote BIS from this local BIS on this BIS to BIS connection.

A.14.3.11 Lastackrecv

The Lastackrecv MO contains the number of the last ack received from the remote BIS by this local BIS on this BIS to BIS connection.

A.14.3.12 updatesIn

The updatesIn MO contains the number of UPDATE BISPDUs received by this BIS on this BIS to BIS connection.

A.14.3.13 updatesOut

The updatesOut MO contains the number of UPDATE BISPDUs sent by this BIS on this BIS to BIS connection.

A.14.3.14 totalBISPDUsIn

The totalBISPDUsIn MO contains the number of BISPDUs received by this BIS from the remote BIS on this BIS to BIS connection.

A.14.3.15 totalBISPDUsOut

The totalBISPDUsOut MO contains the number of BISPDUs sent by this BIS to the remote BIS on this BIS to BIS connection.

A.14.3.16 KeepalivesSinceLastUpdate

The KeepalivesSinceLastUpdate MO contains the number of KEEPALIVE BISPDUs received by this BIS from the remote BIS since this last UPDATE BISPDU.

APPENDIX B
SYSTEM IDENTIFIER GUIDELINES

B.1 System ID Guidelines

There are a number of approaches for allocating/administering the System ID portion of the NSAP address, each with some advantages and disadvantages. For avionics equipment used in the mobile airborne routing domain alternative approaches should be evaluated against how well they satisfy the following list of requirements.

For avionics equipment deployed in the mobile airborne routing domain, the allocation of System IDs NSAP addresses:

1) must uniquely and unambiguously identify the end system containing the addressed Network Entity for level 1, as defined in ISO 9575, routing procedures to operate properly.
2) should allow avionics equipment to replaced or moved between aircraft without manual intervention to reconfigure the System ID value or requiring updates to airborne or ground-based directory tables/servers.
3) should allow multiple instances of the same "type" of equipment (such as a printer, side display, etc.) to be simultaneously installed and moved freely and transparently between aircraft installation sites.
4) should allow portable avionics equipment (such as a PMATs) to be temporarily attached to the airborne routing domain without causing address collisions.
5) should minimize the burden of administrating the address space.

For LAN-based systems, a simple and straightforward method for meeting criteria #1, #4 and #5 above, is to adopt the 6 octet universally administered, individual MAC address (assigned at the factory) for use as the System ID value. Since this MAC address is globally unique, the System ID is assured to be globally unique as long as all LAN-based avionics equipment use this approach to define their System ID values.

This approach is known as embedding the MAC address within the NSAP address. It has been viewed by many as the preferred method for administering System IDs in an aeronautical telecommunications environment. Its major advantage is that it minimizes the burden of administering the System ID address space. Unfortunately, this approach has major draw backs for most of the avionics equipment in the airborne environment. The draw backs relate to maintaining accurate directory information when a network reconfiguration occurs and result in the approach not satisfying requirements #2 and #3 above.

In the avionics environment, any time the Network Entity Title of an end system (in avionics terminology a line replaceable unit or LRU) changes, a network reconfiguration can be considered to have occurred. If the above approach is used, the Network Entity Title essentially changes any time the network interface is replaced or the LRU itself is replaced due to a failure or for some other reason. The change in Network Entity Title results in changing the addressing information needed (by a remote application) to access applications which are served by the local Network Entity. Any end system, on the aircraft or on the ground, wishing to initiate communications with the application supported by the local Network Entity would have to be appraised of these changes in order for communication to occur. There are currently no mechanisms whereby this can automatically occur and the implied manual updates to the directory tables of airborne LRUs is untenable.

A variation on the above approach, which overcomes the directory update problems, is to use a scheme which allocates the same "logically-assigned" MAC address value to all LRUs of an identical "type". Therefore, if a failure occurs and the LRU is replaced, the System ID does not change[footnote 1]. When combined with the auto-configuration aspects of creating the local Network Entity Title (see Chapter 2 of this specification), this approach allows equipment to be replaced or moved from aircraft to aircraft in a completely transparent way, thus satisfying criteria #2.

The key to this scheme is the logically-assigned MAC address. The MAC address is a 6-octet value which conforms to the IEEE-administered scheme for assigning MAC addresses and therefore the values derived will be globally unique. It is a logical address because it is a value which is shared among all equipment of a given "type" (e.g. FMC, MAT, Network Printer, etc.). This address value is never used as a MAC address in any real equipment. Rather, it is used only as the value for the System ID and since the address value is globally unique (in the context of IEEE MAC addresses), it insures that no address "collisions" will occur if the equipment using this value as a System ID co-exists with equipment which has used the first alternative discussed (embedding the real MAC address as the System ID value). In the avionics environment, it is very likely that PMATs will use a scheme which embeds MAC addresses[footnote 2] and therefore, allocating the System ID value using this approach insures that requirement #4 is satisfied. It also serves to minimize the administrative burden of guaranteeing uniqueness in an environment where portable equipment is routinely connected to the network.

The IEEE-administered scheme for allocating universally administered MAC address, uses a 22-bit organizationally unique identifier (OUI) to guarantee the global uniqueness of the addresses allocated. Therefore, one method to derive the logically-assigned address value is for the avionics industry to acquire an OUI from IEEE[footnote 3] and use the value in a scheme to allocate System IDs. This approach is illustrated below:

System ID portion of the NSAP Address:

I/G	U/L	Avionics Industry OUI	Equipment Type
1 bit	1 bit	22 bits	24 bits

The I/G and U/L fields are defined by IEEE and correspond to individual/group and universal/local address respectively. The last 24 bits of the System ID are available for allocation to the different types of equipment that may be installed on an aircraft.

Since the logically-assigned MAC address is shared among all equipment of the same type, an additional

APPENDIX B (cont'd)
SYSTEM IDENTIFIER GUIDELINES

mechanism is necessary for the scheme to be viable when more than one instance of a particular type of LAN equipment is installed in an aircraft. This would allow criteria #3 to be met by, for example, allowing the same printer (as indicated by type) to be installed in either a cockpit location (cockpit printer) or a cabin location (cabin printer).

This objective is readily met by decomposing the last 24 bits of the System ID into 2 subfields, one corresponding to different types of equipment and the other corresponding to the instance of equipment type. The instance field would normally be set to zero. Where multiple instances of the same type of an LRU exist (or have the potential to exist) on the aircraft, the instance field would be used to distinguish the instance or location of the LRU. By using a location dependant approach, such as program pins to add an offset into the instance field, equipment of the same type can be moved freely (perhaps even during flight) between the locations without any manual intervention to modify the System ID. A reasonable decomposition of the field might be to allocated 16 bits for equipment "type", (providing the over 65K types) and 8 bits for equipment "instance" (providing up to 256 instances).

The primary draw back of this approach is the up front administrative work required to acquire an OUI value and assign values to the type and instance fields however, once completed the scheme is pretty much free from administrative overhead.

1 Note that this does not imply that the MAC address of the LRU which is replaced does not change. It in fact does change. But this level of network reconfiguration is transparent because of the ES-to-IS protocol.

2 Since a PMAT will always initiate communications (rather than be a responder), this type of equipment may very likely have a System ID value which imbeds its local, universally administered, individual IEEE MAC address. In this case, the directory update problem is avoided because, in the process of initiating communications, the remote peer application is provided with the addressing information it needs to respond to the PMAT's request.

3 The real requirement for this OUI is that it not be used to allocated real MAC address values. An OUI could be obtained by one or more of the aeronautical organizational entities and used to administer their own System ID address space or, if appropriate, "donated" for industry use, in which case the administration of System IDs could occur in a document such as PP 637 or by an industry recognized registration authority.

APPENDIX C
GLOSSARY

ACARS	Aircraft Communication Addressing and Reporting System
ADM	Administration
AEEC	Airlines Electronic Engineering Committee
AFI	Authority and Format Indicator
AOP	Aeronautical OSI Profiles
ARS	Area Routing Selector
ATA	Air Transport Association
ATN	Aeronautical Telecommunications Network
AVPAC	Aviation VHF Packet Communications
BCD	Binary Coded Decimal
BIS	Boundary Intermediate Systems
BSNPA	Better Subnetworking Point of Attachment
CE	Congestion Experienced
CI	Configuration Information
CLNP	ConnectionLess-mode Network Service Protocol
CLNS	ConnectionLess Network Service
CMU	Communications Management Unit
DCE	Data Circuit Equipment
DSP	Domain Specific Part
DTE	Data Terminal Equipment
DUID	Data Unit Identification
ES	End System
ESCT	End System Configuration Timer
ER	Error Report
FMC	Flight Management Computer
GOSIP	Government Open Systems Interconnection Profile
HT	Holding Timer
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICD	International Code Designator
IDI	Initial Domain Indicator
IDP	Initial Domain Part
IDRP	Inter-Domain Routing Protocol
IEEE	Institute of Electrical and Electronic Engineers
IP	Internetwork Protocols
IS	Intermediate Systems
ISH	Intermediate System (IS) Hello
ISO	International Organization for Standardization
LAN	Local Area Network
LNP	ConnectLess Network Protocol
LOC	Location Identifier
LSAP	Link System Access Point
LQA	Lowest Quality
MIB	Management Information Base
MOPS	Minimum Operational Performance Standards
MU	Management Unit
NET	Network Entity Titles
NIST	National Institute of Standards and Technology
NLPID	Network Layer Protocol ID
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Parts
NSDU	Network Service Data Unit
OSI	Open Systems Interconnection
PCI	Protocol Control Information
PDU	Protocol Data Unit
RDF	Routing Domain Format
RDI	Routing Domain Identifier
RI	Route Redirection Information
SARPS	Standards and Recommended Practices
SATCOM	Satellite Communications
SEL	Selector
SNAcP	Subnetwork Access Protocol
SNDC	Subnetwork Dependent Convergence Protocol
SNDCF	Subnetwork Dependent Convergence

APPENDIX C (cont'd)
GLOSSARY

SNDCP	Subnetwork Dependent Convergence Protocol
SNICP	Subnetwork Independent Convergence Protocol
SNPA	Subnetwork Point of Attachment
SYS	System Identifier
TRD	Transit Routing Domain
QOS	Quality of Service
VER	Version

APPENDIX D
ROUTING INITIATION EVENTS

D.1 Introduction

This paper identifies the routing initiation procedures that are needed in an airborne ATN router to begin operation over the various ATN subnetworks. These routers and subnetworks are currently being developed, and the following initialization procedures are needed within the router to properly use the subnetworks.

When using conventional routers, the subnetwork between routers is fixed, and the router's address at the other end of the subnetwork is known. When a dynamic routing protocol mechanism is not used, the system manager must explicitly enter the information in order for the router to establish the connection to the distant router. (The system manager must type in the port number and address of the other router.)

The mobile nature of the ATN air-ground subnetworks does not allow fixed subnets between routers. The subnetworks connect and disconnect autonomously, and the router at the other end of the subnetwork is not known. The connection of subnetworks and discovery of router identity needs to be automatic.

The air-ground subnetworks (AVPAC, SATCOM, Mode-S, and Gatelink) have peculiarities that require different startup procedures in order to establish router-to-router communication over them. The differences are listed below, but each ends up with the proper routing information getting into the IDRP/CLNS routing tables. Exactly how this is done is the subject of this paper.

D.2 Subnetwork Descriptions

The ATN VHF-based subnetwork, AVPAC, will begin lab testing early in 1993, with flight testing in late 1993. SATCOM Data Level 2 units are just now being qualified and will begin flight operation soon. The ATN satellite-based subnetwork units, SATCOM Data Level 3, are not currently being built. The ATN radar-based subnetwork, Mode-S, will begin flight testing in late 1993. The ATN LAN connection from parked aircraft to the airport gate, Gatelink, is currently being designed. The HF subnetwork definition is not complete yet, and is not included in this paper.

ISDG has identified the network management entities that reside within different portions of the system. The router's management entity, IS_SME, is responsible for managing the router protocols in conjunction with the subnetwork availability. Each of the subnetworks' management entities, generically called SN_SMEs, manage the peculiarities of the subnetwork, and reports status as appropriate to the IS_SME.

D.2.1 Subnetwork Differences

The subnetworks each have different properties associated with the startup process that need special handling. The IS_SME in the router manages the startup of the subnetworks in the ATN. These differences include:

Initial Call Request:

AVPAC, SATCOM, and Gatelink are initiated by the aircraft;

Mode-S is initiated by the ground station.

SNAcP:

AVPAC uses 8208 DTE-DTE as the subnetwork access protocol;

SATCOM and Mode-S use 8208 DTE-DCE as the subnetwork access protocol;

Gatelink uses LLC1 as the subnetwork access protocol.

Link startup and IS Hello:

AVPAC and SATCOM send the link startup messages, then the 8208 Call Request with the ISH in the Fast Select field;

Mode-S combines the link startup with the 8208 call request, then sends the ISH separately;

Gatelink sends only the ISH.

Subnetwork Up Event (for avionics):

AVPAC and SATCOM are up when the Call Connected packet is received;

Mode-S is up when the Call Accepted packet is sent;

Gatelink is up when SMT sends 'Ring-Op' indication primitive.

Packaging:

AVPAC VDR contains protocols up through the link layer, the 8208 DTE layer and Link Management Entity are in the CMU;

SATCOM Data Level 3 SDU contains all protocols up through the 8208 DCE sub-network layer and the SN_SME, the 8208 DTE is in the CMU;

Mode-S ADLP contains all protocols up through the 8208 DCE sub-network layer and no SN_SME, the 8208 DTE is in the CMU (Note: the packaging for the Mode-S ADLP is still being debated).

Gatelink is completely internal to the router.

The layering of the protocol entities is shown in Figure 1.

D.2.2 Assumptions

Bandwidth is limited over the air/ground links. The transmission of PDUs should be minimized.

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

The AVPAC 8208 Call Request must wait for the link to be set up, since certain packet layer parameters depend on the link speed (e.g., packet size). The transfer of these parameter values may be simplified by a priori knowledge.

The CMU must distribute the ICAO 24-bit aircraft identifier to the link level process of the subnetworks.

The link-up primitive indicates that the subnetwork link level process has identified a peer entity through which it may be possible to contact a router.

The router initiation event, called the join/leave event in Mode-S, indicates that the packet level process has established an 8208 connection with a ground router.

D.3 Routing Initiation Procedures

All air-ground subnetworks (except gatelink) use the ICAO 24-bit address of the aircraft as the link level address. The transponder/TCAS unit is the source of the ICAO-24 bit address. It needs to propagate the address to the CMU, which forwards it to AVPAC, SATCOM, and other subnetworks as needed. Thus, the routing initiation begins with:

- The 24-bit ICAO address is read by the transponder (from the service connector), and the transponder sends this 24-bit ICAO address to the CMU.

The following sections describe the current method by which each subnetwork starts up. Note: Just the portions of subnetwork startup that pertain to routing are listed, other items (such as self-tests) are not shown.

D.3.1 AVPAC and VDR Initiation

Figure D-2 (MSC AVPAC) shows the primitives that are exchanged onboard the aircraft and the PDUs exchanged air/ground upon AVPAC subnetwork startup. Following is the textual description of the primitives.

VDR & link initiation:

1. Upon startup, VDR reads discrete to determine if it is to be in data (or voice) mode. If data, it listens to the 429 bus to detect the master CMU address.

2. VDR sends a 429 status word to the master CMU with a bit set indicating 'download requested'.

3. CMU/LME responds to VDR local manager with various parameter set commands to initialize the VDR with the 27-bit AVPAC address, frequency, data rate, and other communication parameters.

4. The VDR starts forwarding received frames (containing ground station address and signal quality parameter) to the LME/CMU.

AVPAC routing initiation:

5. LME begins building dynamic PECT table by listening to transmissions from ground stations.

6. Once it has identified an acceptable ground station, the LME sends a DL_CONNECT.request primitive to the AVLC specifying the address of the ground station with which it is to establish a link and other parameters.

7. AVLC sends link level connect pdu (XID_CMD) and receives link level connect response (XID_RSP) establishing link level connection with a ground station.

8. AVLC sends a DL_CONNECT.indication primitive to the LME indicating the address of the ground station with which a link has been established and other communication parameters.

9. LME sends Link_Up primitive to IS_SME.

10. 9542 protocol entity generates ISH PDU and sends it to SNDCF.

11. SNDCF sends SN_Call.request primitive to the DTE entity. The Called DTE address is the 'Default Service Provider Router' DTE address. The calling DTE address is the AEEC 631 DTE address of the aircraft. The user data contains the ISH PDU.

12. DTE entity sends Call Request PDU (with the parameters as specified in the incoming SN_Call.request primitive and Fast Select field containing the ISH PDU) over the established link level connection to the ground station. The ground station relays it to the DTE entity entity in the air/ground router.

13. DTE entity in the air/ground router sends the Call Connected PDU to the DTE entity in the airborne router.

14. LME updates dynamic PECT with connection information.

15. SNDCF sends "Subnetwork up" primitive to IS_SME and sends the ISH PDU to the 9542 entity.

D.3.2 SATCOM Initialization

Figure D-3 (MSC SATCOM) shows the primitives that are exchanged onboard the aircraft and PDUs exchanged air/ground upon Satcom subnetwork startup. Following is the textual description of the primitives.

SDU log-on:

1. SDU sends a status word to the CMU indicating 'Download Requested'.

2. CMU puts the aircraft's 24-bit ICAO address on the 429 bus (broadcast continually).

3. SDU uses the static Owner Requirements Table (or lat/long position information) to select a frequency.

4. SDU Link Layer listens on the specified P channel frequencies for a carrier (or listens for data).

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

D.3.2 SATCOM Initialization (cont'd)

5. SDU Link Layer acquires a P channel.

6. SDU Link Layer sends a Logon request over Rmsc channel to GES to establish link level connection.

7. SDU Link Layer receives Logon confirm on Pmsc channel.

SATCOM routing initiation:

8. SDU Link Layer send Status Change Report to SN_SME.

9. The SN_SME, upon detection of SDU log-on, sends a Log-on Connectivity Report to the IS_SME containing the identity of the log-on GES. This report may, for example, be transmitted in the user data of an 8208 Call Request packet (with fast select requested) sent by the SN_SME to the IS_SME.

10. IS_SME clears the call and writes the Logon information to a table.

11. The 9542 sublayer, upon expiration of its local configuration timer, sends an SN_UNITDATA.request primitive to the SNDCF with user data containing its own ISH PDU and destination address set to ALL ISs.

12. CMU/SNDCF sends SN_Call.req to airborne DTE entity, destination address is a ground router specified in the Reachable SNPA column of the Routing Initiation Table.

13. DTE entity sends Call Request (with parameters as specified in the incoming SN_Call.request primitive) to a reachable air/ground router. It then receives a Call Connected packet containing the ground-initiated ISH PDUs.

14. DTE entity sends SN_Call.confirm primitive (with the ground-initiated ISH PDU in the user data field) to SNDCF.

15. SNDCF sends SN_UNITDATA.ind primitive to IS_SME/9542 containing NET of ground router.

    Note: Steps 12-15 occur for each SNPA entry indexed by the GES ID in the Routing Initiation Table.

D.3.3 Mode-S Initialization

Figure D-4 (MSC Mode_S) shows the primitives that are exchanged onboard the aircraft and PDUs exchanged air/ground upon Mode-S subnetwork startup. Following is the textual description of the primitives. Before operation begins, the GDLP generates and sends to the sensors a route packet containing "sensor id: DTE Address" pair.

Mode-S link initialization:

1. Upon initialization, ADLP clears its local "Mode-S Interrogator:Ground DTE address" table.

2. ADLP downloads to transponder the capability of aircraft.

3. Ground sensor sweeps aircraft with an All-Call request.

4. Aircraft transponder responds to All-Call request with an All-Call reply (containing the 24-bit aircraft id and capability).

5. Sensor receives aircraft response and forwards to GDLP the address and capability of aircraft.

6. Sensor uplinks route packet.

7. ADLP receives router packet and updates its local "Mode-S Interrogator:Ground DTE address" table as appropriate.

Mode-S routing initiation:

8. GDLP sends a SN_event (subnet up, link addr, DTE addr) to the ground router.

9. Ground router builds ISH PDU and sends it to the SNDCF (in the router).

10. Ground SNDCF uplinks 8208 Call Request.

11. Air DTE entity/SNDCF receives Incoming Call and responds with Call Accepted.

12. Ground SNDCF receives Call Accepted and sends ISH PDU.

13. Avionics SNDCF/router receives ISH and sends ISH PDU in downlink.

14. Avionics SNDCF/SN_SME sends SN_event(subnetwork up, ISH) to IS_SME.

D.3.4 Gatelink Initialization

Figure 5 (MSC Gatelink) shows the primitives that are exchanged onboard the aircraft and PDUs exchanged over the Gatelink upon Gatelink subnetwork startup. Following is the textual description of the primitives.

Gatelink LAN establishment:

1. Upon In-Event, power on the ATU if needed.

2. IS_SME sends SMT_Connect_Request to SMT.

3. SMT sees other neighbors & establishes the FDDI ring.

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

Gatelink routing initiation:

4. SMT sends SMT_Ring_Op primitive to IS_SME.

5. IS_SME (or 9542) broadcasts ISH PDU to 'all routers'.

6. Ground router receives ISH & responds with an ISH PDU.

7. Upon receipt of ISH PDU response, IS_SME declares Gatelink subnetwork up.

The (gatelink-specific) application may be started at this time, or the application may be constructed to send application-level connect requests periodically, requesting the quality of service that can only be satisfied with gatelink. In this case, the application's connect requests would go unanswered until the gatelink sub-network was active.

D.3.5 HF Initialization

To be supplied.

D.3.6 Common Subnetwork Initialization

When any subnetwork establishes communication with its peer and exchanges ISH PDUs with the other router, it sends a "subnetwork-up" primitive to the IS_SME. The IS_SME needs to establish the BIS-BIS connection with the other router, and the steps are:

1. IS_SME receives (internal) "subnetwork-up" primitive from SN_SME, or by other means, determines that the subnetwork is up.

2. IS_SME puts the other router's NET into the IDRP External-Bis-Neighbors table.

3. IS_SME sends start event to IDRP state machine.

D.4 Conclusions

Based on the above methods of subnetwork startup, the Specification and Design Language description of the IS_SME is identified in Figure 6.

The "subnetwork up" primitive is conceptual and is not passed across an exposed interface as suggested in Flimsy #3.

Since Flimsy #3 was written, the AEEC has decided that the VDR will contain protocol layers up through the link layer, and the packet layer and link management entity will reside in the CMU.

This work is continuing in the AEEC CMU working group, in coordination with the AEEC AVPAC subnetwork group. The Satcom and Mode-S working groups (both RTCA and SICASP) need to provide input.

D.5 Recommendations

Several action items would help reach agreement on this topic.

1. Complete the description of the IS_SME in SDL. Also, describe the function of the SN_SME in SDL. The use of a formal specification language would force a rigorous definition of the management entity and also allow use of tools to determine completeness and lack of deadlock situations. SDL also requires the definition of parameters to the events and primitives.

2. Specify all management tables in GDMO descriptions. This includes the AVPAC Peer Entity Contact Table, Satcom Owner Requirements Table and Router Initiation Table, and Mode-S Interrogator/Ground DTE Address Table.

3. Network management actions and results should be based on a common network management framework that is addressed, where possible, at CLNP. The use of DTE addresses and selectors for subnetwork management primitives should be discouraged.

4. Determine address format for 9542 broadcast NET.

5. Standardize on the event terminology and precisely define the events. The ATN manual is largely Mode-S influenced, hence the use of the term join/leave event. There are two different events in AVPAC and Satcom, a link-up event that indicates the link layer has detected a ground station, and a subnetwork-up event indicating that the packet layer has established an 8208 connection to a ground router.

6. Determine effect of subnetwork keep-alive messages to CMU. The ATN Manual recommends the use of keep-alive messages from the subnetwork processor to the CMU (even though the use is not rigorously defined). If the CMU does not get a 'subnetwork is still up' message from the subnetwork processor, the routing table entry is cleared and the subnetwork is reset. The use of this mechanism should be determined by the AEEC committee.

D.6 Bibliography

Flimsy #3, *ATN Routing Initiation Over Air-Ground Subnetworks*, SICASP ISDG, Flimsy #3, August 14, 1991

AEEC 631, *Aviation VHF Packet Communications (AVPAC)*, AEEC, September, 1992

AEEC 637, *Draft 8 of Project Paper 637, "Internetworking Specification"*, AEEC, August 28, 1992

AEEC 750, *VHF Data Radio*, AEEC

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

D.6 Bibliography (cont'd)

DO-181A, *Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/MODE S) Airborne Equipment*, RTCA, January 1992

DO-203A, *Minimum Operational Performance Standards for the Mode-S Airborne Data Link Processor*, RTCA, 24 September 1992

ARINC 741P2-1, *Aviation Satellite Communication System, Part 2, System Design and Equipment Functional Description*, ARINC, July 31, 1992

D.7 Nomenclature

AVPAC hardware:

VDR - VHF Data Radio
CMU - Communication Management Unit
GS - ground station

AVPAC software:

AVLC - AVPAC implementation of HDLC link level protocol
LME - Link Management Entity (called SN_SME by SICASP)
PECT - Peer Entity Contact Table

SATCOM Hardware:

AES - aircraft earth station
GES - ground earth station
SDU - Satellite Data Unit

Mode-S:

ADLP - Airborne Data Link Processor
GDLP - Ground Data Link Processor
Sensor - ground radar site
Transponder - airborne radar receiver

Gatelink:

ATU - Airborne Transceiver Unit
GTU - Ground Transceiver Unit
LAN - Local Area Network

Router:

IS_SME - Intermediate System System Management Entity
IDRP - Interdomain Routing Protocol

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

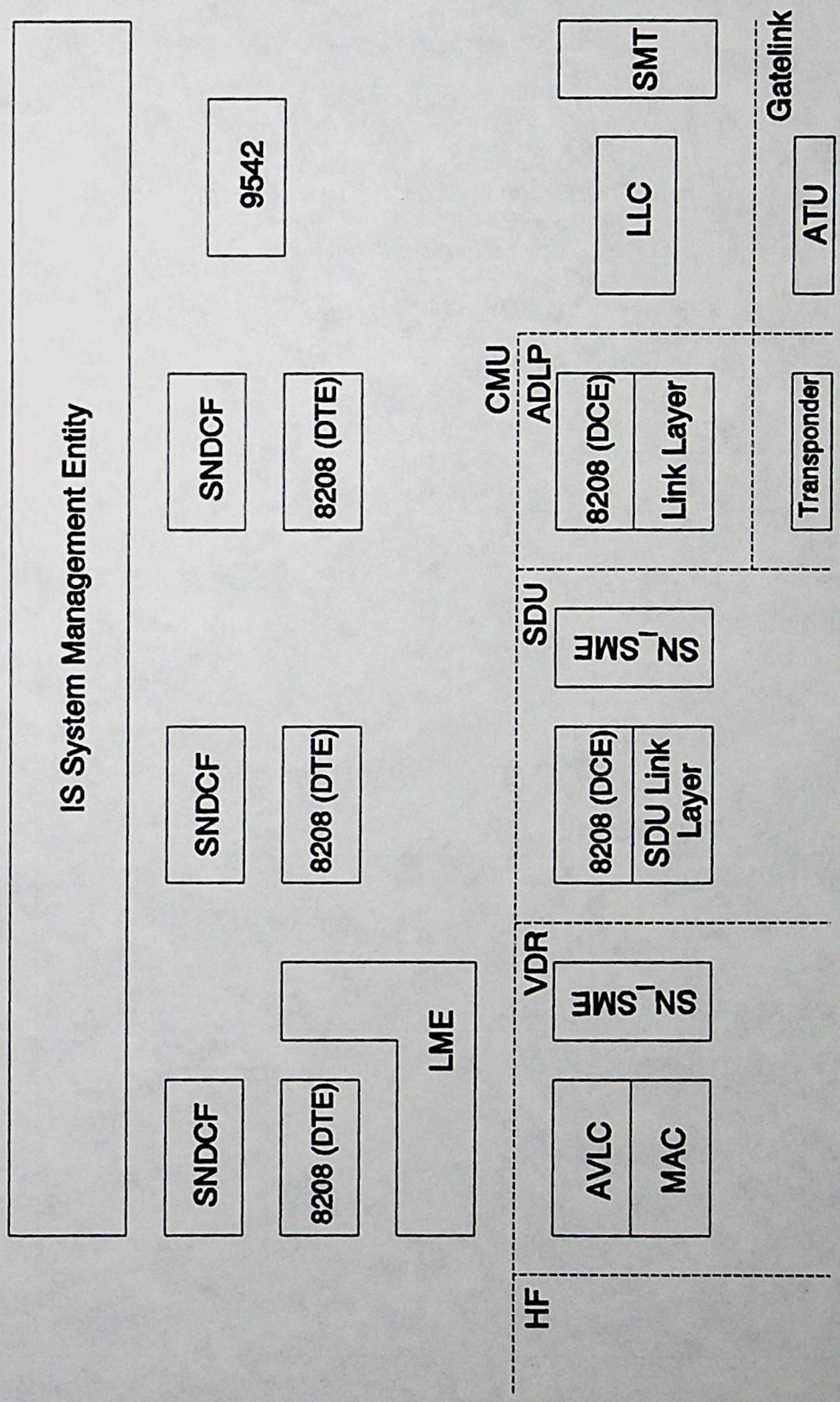


Figure D-1 System Management Entity Relationships

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

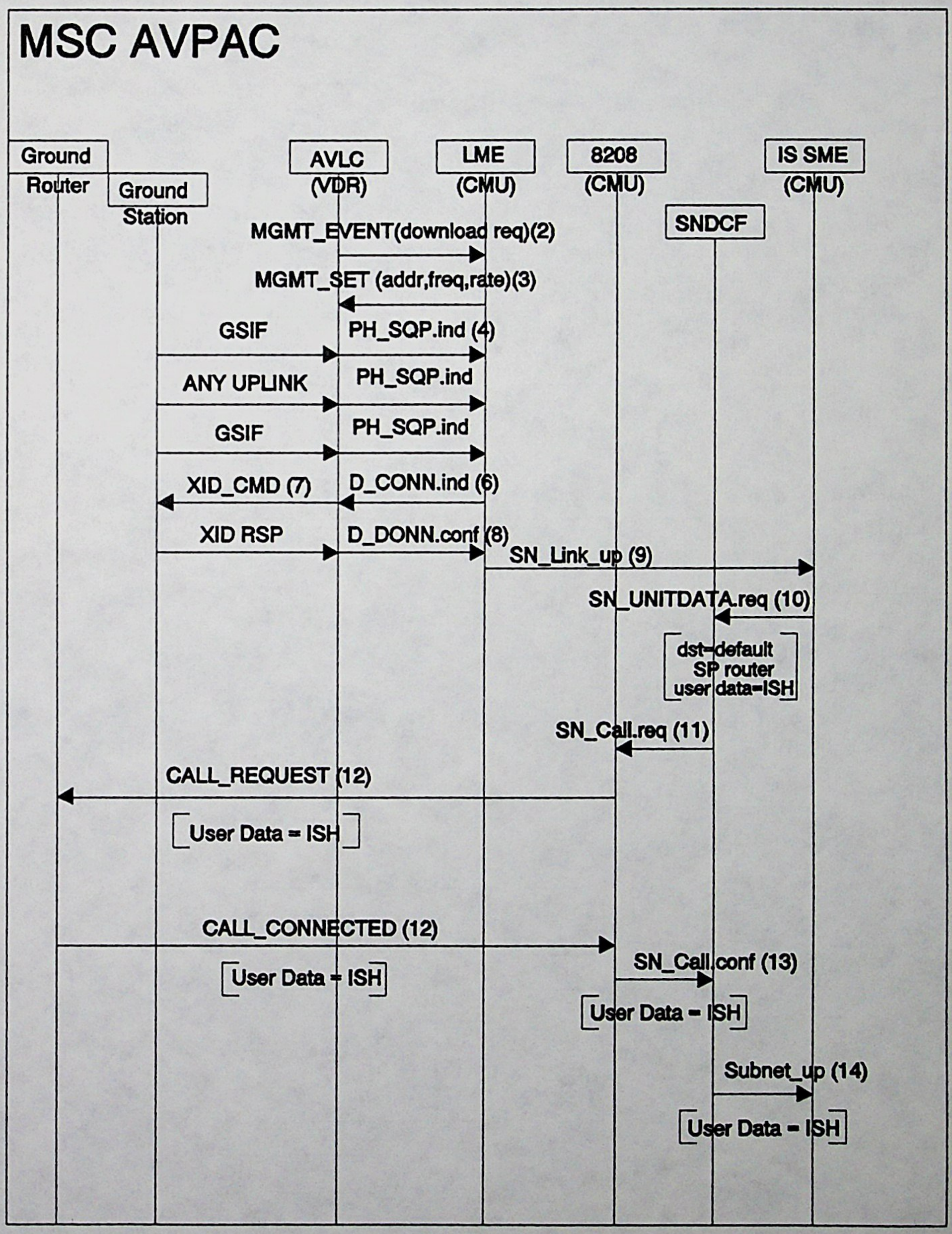


Figure D-2 MSC AVPAC

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

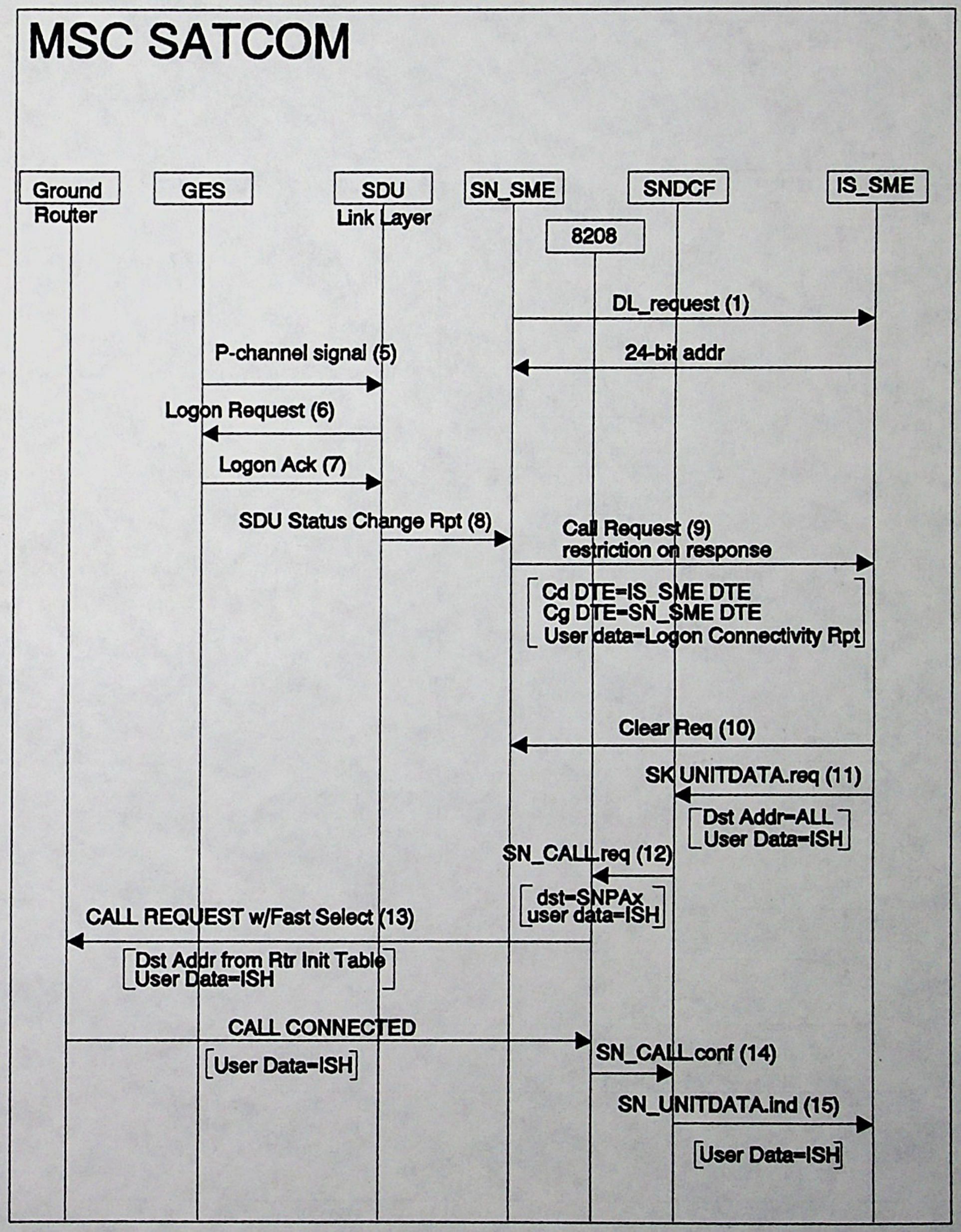


Figure D-3 MSC SATCOM

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

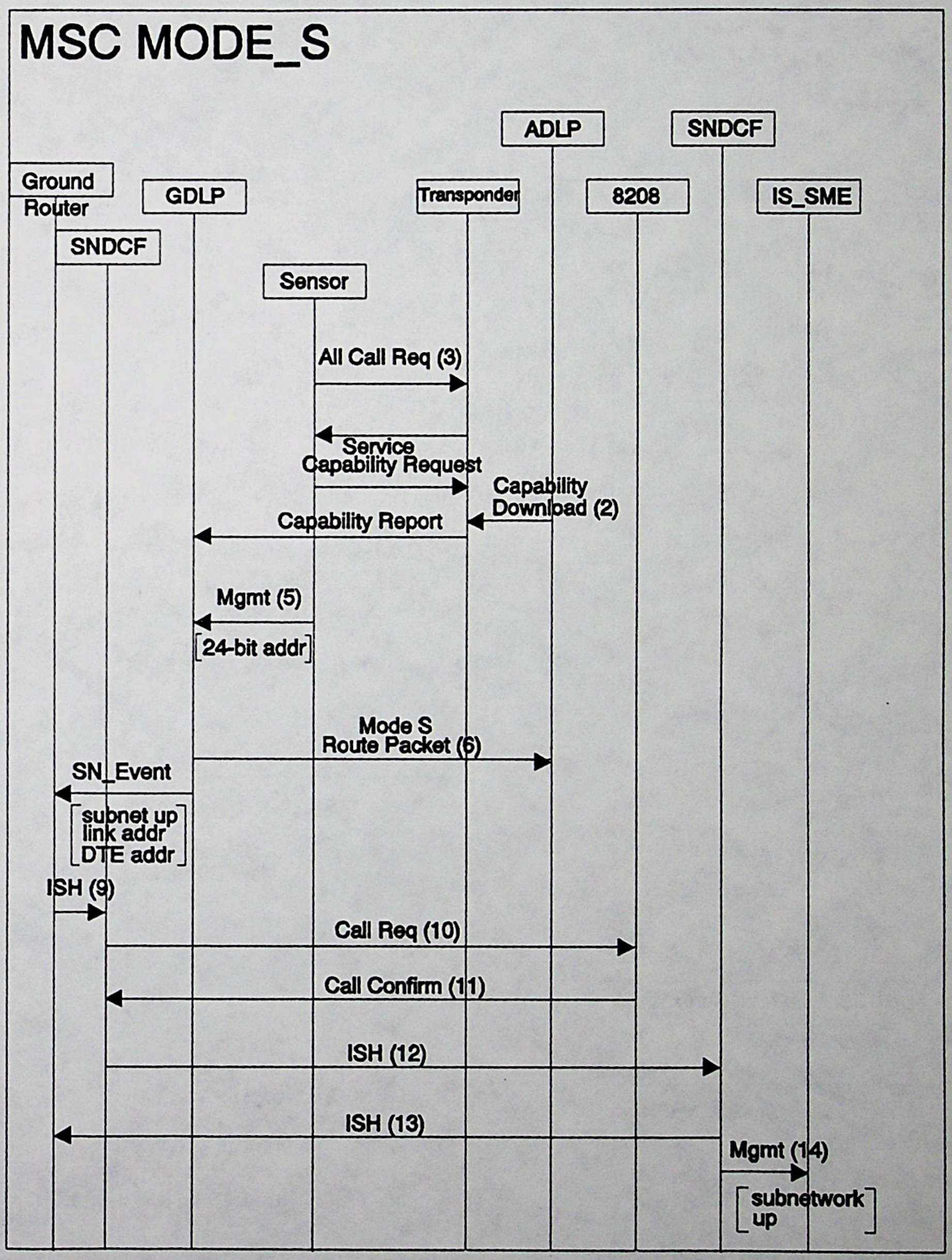


Figure D-4 MSC Mode_S

APPENDIX D (cont'd)
ROUTING INITIATION EVENTS

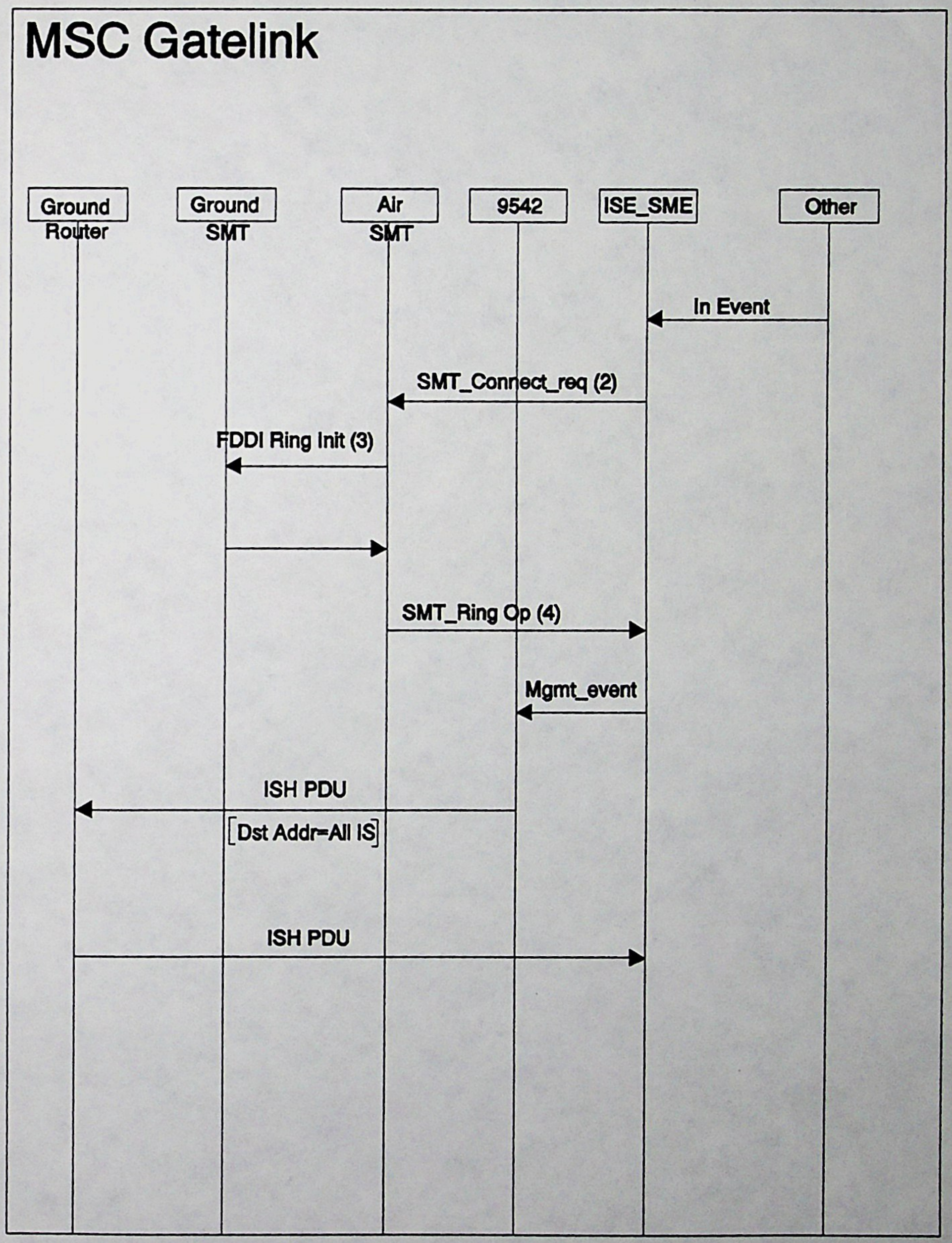


Figure D-5 MSC Gatelink