ICAO

Doc 9880

Technical Specifications for ATN using ISO/OSI Standards and Protocols

Second edition, 2016

Part III – Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS)

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Doc 9880
AN/466

Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols

Part III — Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS)

Second Edition — 2016

International Civil Aviation Organization

Published in English only by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

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

Doc 9880, ***Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols***
Part III, ***Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS)***
Order Number: 9880P3
ISBN 978-92-9258-142-8

AMENDMENTS

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

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

TABLE OF CONTENTS

FOREWORD[1]

This manual contains the detailed technical specifications for the ATN based on relevant standards and protocols established for open systems interconnection (OSI) by the International Organization for Standardization (ISO) and the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T). A separate manual, the *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols* (Doc 9896), addresses detailed technical specifications for the ATN based on standards developed for the IPS by the Internet Society (ISOC). Standards and Recommended Practices (SARPs) for the ATN/IPS are contained in Annex 10 — *Aeronautical Telecommunications,* Volume III — *Communication Systems*. Where necessary and to avoid duplication of material, Doc 9896 refers to this manual.

Editorial practices in this document are as follows:

- The detailed technical specifications in this manual that include the operative verb “shall” are essential to be implemented to secure proper operation of the ATN.

- The detailed technical specifications in this manual that include the operative verb “should” are recommended for implementation in the ATN. However, particular implementations may not require this specification to be implemented.

- The detailed technical specifications in this manual that include the operative verb “may” are optional.

This manual is published in the following parts:

Part I: Air-Ground Applications (replaces Doc 9705, Sub-volume II)

Part II: Ground-Ground Applications — Air Traffic Services Message Handling Services (ATSMHS) (replaces Doc 9705, Sub-volume III)

Part III: Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS) (For the moment, Part III of this manual replaces Doc 9705, Sub-volume IV. It will also replace Doc 9705, Sub-volume V once the text of Chapter 3, which is currently being developed, is available.)

Part IV: Directory Services, Security and Identifier Registration (replaces Doc 9705, Sub-volumes I, VII, VIII and IX).

[1] The first edition of this manual amended and replaced the third edition of the *Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN) (*Doc 9705).

Structure of Part III:

This part of Doc 9880 contains technical provisions for the upper layer communications service (ULCS) and the Internet communications service (ICS). It is structured as follows:

Chapter 1: INTRODUCTION

Chapter 2: UPPER LAYER COMMUNICATIONS SERVICE (ULCS)

Chapter 3: INTERNET COMMUNICATIONS SERVICE (ICS)

ACRONYMS AND ABBREVIATIONS

AAC	Aeronautical administrative communications
AARE	A-Associate-response
AARQ	A-Associate-request
ABRT	A-Abort
ACP	Aeronautical Communications Panel
ACSE	Association control service element
ADS-C	Automatic dependent surveillance — contract
AE	Application entity
AE-title	Application entity title
AINSC	Aeronautical industry service communication
ALS	Application layer structure
Amdt	Amendment
AOC	Aeronautical operational control
APC	Aeronautical passenger communications
APDU	Application protocol data unit
App	Application
APRL	ATN profile requirements list
AP-title	Application process title
ASE	Application service element
ASN.1	Abstract Syntax Notation One
ASO	Application service object
ATM	Air traffic management
ATN	Aeronautical telecommunication network
ATS	Air traffic services
ATSC	Air traffic service communications
BIS	Boundary intermediate system
CF	Control function
CLDS	Connectionless dialogue service
CLNP	Connectionless network protocol
CM	Context management
Cnf	Confirmation
CNS	Communications, navigation and surveillance
CPDLC	Controller-pilot data link communications
CRL	Certificate revocation list
DS	Dialogue service
ERD	End routing domain
FU	Functional unit
IA5	International Alphabet Number 5
ICAO	International Civil Aviation Organization
ICS	Internet communications service
ID	Identification
IDRP	Inter-domain routing protocol
IEC	International Electrotechnical Commission
Ind	Indication
IPS	Internet Protocol Suite
ISO	International Organization for Standardization

ITU-T	International Telecommunication Union — Telecommunication Standardization Sector
MAC	Message authentication code
NET	Network entity title
NOR	No orderly release
NPDU	Network protocol data unit
NSAP	Network service access point
OID	Object identifier
OSI	Open systems interconnection
OSIE	OSI environment
PDU	Protocol data unit
PDV	Presentation data value
PER	Packed Encoding Rules
PICS	Protocol implementation conformance statement
PPM	Presentation protocol machine
PPUD	Presentation protocol data unit
PRL	Profile requirements list
PSAP	Presentation service access point
QoS	Quality of Service
RD	Routing domain
RDC	Routing domain confederation
RDI	Routing domain identifier
Req	Request
RER	Residual error rate
RLRE	A-Release-Response
RLRQ	A-Release-Request
Rsp	Response
SAC	Short accept
SACC	Short accept continue
SARPs	Standards and Recommended Practices
SCN	Short connect
S-FU	Session functional unit
SNAcP	Subnetwork access protocol
SNDCF	Subnetwork dependent convergence function
SNICF	Subnetwork independent convergence function
SNPA	Subnetwork point of attachment
SNSDU	Subnetwork service data unit
SPDU	Session protocol data unit
SPM	Session protocol machine
SRF	Short refuse
SRFC	Short refuse continue
SSAP	Session service access point
SSR	Secondary surveillance radar
TS	Transport service
TRD	Transit routing domain
TSAP	Transport service access point
UL	Upper layer
ULCS	Upper layer communications service

DEFINITIONS

Abstract service interface. The abstract interface between the application entity (AE) and the application-user.

Abstract Syntax Notation One (ASN.1). Abstract Syntax Notation One is defined in ISO/IEC 8824-1. The purpose of this notation is to enable data types to be defined, and values of those types specified, without determining their actual representation (encoding) for transfer by protocols.

Addressing plan. A plan that provides common address syntax and management of global addresses for the unambiguous identification of all end and intermediate systems in accordance with the rules prescribed in ISO/IEC 7498-3 and ISO/IEC TR 10730.

Aeronautical telecommunication network (ATN). A global internetwork architecture that allows ground, air-ground and avionic data subnetworks to exchange digital data for the safety of air navigation and for the regular, efficient and economic operation of air traffic services.

Aircraft address. A unique combination of twenty-four bits available for assignment to an aircraft for the purpose of air-ground communications, navigation and surveillance.

Application. The ultimate use of an information system, as distinguished from the system itself.

Application entity (AE). Part of an application process that is concerned with communications within the OSI environment. An application may be supported by multiple AEs (see ISO/IEC 9545 for further details).

Application entity qualifier. That part of the AE-title that unambiguously identifies the particular application entity.

Application entity service interface. The interface between the application-users and the application service provider.

Application entity title. An unambiguous name for an application entity.

Application layer. The seventh layer of the OSI reference model that controls application-user access to the communication system and provides services to perform a logical association to other applications.

Application layer structure (ALS). The application layer structure refers to the internal architecture of the OSI application layer as described in ISO/IEC 9545.

Application process (AP). A set of resources, including processing resources, within a real open system which may be used to perform a particular information processing activity.

Application protocol data unit (APDU). An application protocol data unit is an (N) PDU, where N refers to the application layer. An APDU is the basic unit of information exchanged between the airborne application and the ground application.

Application service. The abstract interface between the (N) service and the (N) service user, where N refers to the application layer; thus it is the boundary between the AE and the application-user.

Application service element (ASE). The element in the communication system that executes the application specific protocol. In other words, it processes the application specific service primitive sequencing actions, message creation, timer management, and error and exception handling. The application's ASE interfaces only with the application's control function.

Application service element (ASE) service interface. The abstract interface through which the ASE service is accessed.

Note.— In version 1 of the ADS application, the ADS-ASE service interface coincides with the ADS-AE abstract service interface.

Application service object (ASO). An active element within (or equivalent to the whole of) the application entity embodying a set of capabilities defined for the application layer that corresponds to a specific ASO-type (without any extra capabilities being used). An ASO is a combination of application service elements (ASEs) and ASOs that perform a specific function. An ASO that provides the functions of the establishment and data transfer phases is considered a complete protocol.

Application-user. That abstract part of the aircraft or ground system that performs the non-communication-related functions of the application.

Association control service element (ACSE). The association control service element is the common mechanism in the application layer structure (ALS) for establishing and releasing application service object (ASO) associations.

ATN application. Refers to an application that is designed to operate over the aeronautical telecommunication network (ATN) communication services.

ATN communication services. Composed of the Internet communications service and the upper layer communications service.

ATN environment. The environment that relates to functional and operational aspects of the ATN as a complete end-to-end communication system.

ATN profile requirements list (APRL). APRLs identify, in a tabular form, requirements together with the options and parameters for protocols used in the ATN. The supplier of an ATN protocol implementation claiming to conform to the ATN technical requirements must indicate conformance to those requirements by preparing a protocol implementation conformance statement (PICS) based on the set of APRLs.

ATN security services. A set of information security provisions allowing the receiving end system or intermediate system to unambiguously identify (i.e. authenticate) the source of the received information and to verify the integrity of that information.

Authorized path. A communication path that the administrator(s) of the routing domain(s) has predefined as suitable for a given traffic type and category.

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

Circuit mode. A configuration of the communications network which gives the appearance to the application of a dedicated transmission path.

Context management (CM) application. An ATN application that provides a logon service allowing initial aircraft introduction into the ATN and a directory of all other data link applications on the aircraft. It also includes functionality to forward addresses between ATS units.

Note.— Context management is a recognized OSI presentation layer term. The OSI use and the ATN use have nothing in common.

Control function (CF). That abstract part of the AE that performs the mapping between the ASE service primitives, the association control service element (ACSE) service primitives and other elements within the application entity.

Dialogue. A cooperative relationship between elements that enables communication and joint operation.

Dialogue service (DS). The lower service boundary of an ASE; the service allows two ASEs to communicate, e.g. a CM ground-ASE to communicate with a CM air-ASE.

Directory. A facility that supports on request the retrieval of address information or the resolution of application names.

Directory service (DIR). A service, based on the ITU-T X.500 series of recommendations, providing access to, and management of, structured information relevant to the operation of the ATN and its users.

End system (ES). A system that contains the OSI seven layers and contains one or more end-user application processes.

End-to-end. Pertaining or relating to an entire communication path, typically from (1) the interface between the information source and the communication system at the transmitting end to (2) the interface between the communication system and the information user or processor or application at the receiving end.

End-user. An ultimate source and/or consumer of information.

Entity. An active element in any layer which can be either a software entity (such as a process) or a hardware entity (such as an intelligent I/O chip).

Ground application service element (ground-ASE). An abstract part of the ground system that performs the communication-related functions of the application.

Ground user (ground-user). The abstract part of the ground system that performs the non-communication-related functions of the application.

Message element. A component of a message used to define the context of the information exchanged.

Message element identifier. The ASN.1 tag of the ATCUplinkMsgElementId or the ATCDownlinkMsgElementId.

Packed Encoding Rules (PER). Encoding rules, as defined in ISO/IEC 8825-2, that have been designed to minimize the number of bits transmitted.

Point-to-point. Pertaining or relating to the interconnection of two devices, particularly end-user instruments. A communication path of service intended to connect two discrete end-users; as distinguished from broadcast or multipoint service.

Presentation address (PA). The presentation address must, as a minimum, include a network service access point (NSAP) address and a transport service access point (TSAP) selector and may include a presentation service access point (PSAP) selector and session service access point (SSAP) selector based on the addressing structure adopted within the end system (ES) and whether the application requires the OSI session or presentation protocol.

Presentation data value (PDV). The unit of information specified in an abstract syntax, which is transferred by the OSI presentation service (ISO/IEC 8822).

Presentation layer. The layer of the OSI reference model that controls the coding, format and appearance of the data transferred to and from the application layer.

Presentation service access point (PSAP) selector. The element of the presentation address that identifies the user of the presentation protocol entity.

Priority (P). The relative importance of a particular protocol data unit (PDU) relative to other PDUs in transit and used to allocate resources which become scarce during the transfer process.

Protocol implementation conformance statement (PICS). A protocol implementation conformance statement enables conformance testing of protocols. As recommended by ISO/IEC 9646-2, PICS pro forma, tailored to ATN context, have been developed as ATN profile requirements lists (APRLs) to provide an effective basis for conformance testing of implementations.

Quality of service (QOS). The information relating to data transfer characteristics used by various communication protocols to achieve various levels of performance for network users.

Residual error rate (RER). The ratio of messages mis-delivered, non-delivered or delivered with an error undetected by the system, to the total number of messages delivered to the system during a measurement period (adapted from ISO/IEC 8072).

Note.— For the ATN, detected mis-delivered and non-delivered messages are not included in the ratio.

Route. The set of addresses that identifies the destinations reachable over the router and information about the route's path, including the QOS and security available over the route.

Service primitive. A function of an application service element (ASE) that is not broken down further into subfunctions and is presented as part of the abstract service interface (i.e. request, indication, response or confirmation).

Service provider. An entity at a layer that provides services to the layer above. These services are provided at service access points through the use of service primitives.

Session layer. The layer of the OSI reference model that establishes the rules of dialogue between two end-user entities.

Session service access point (SSAP) selector. The element of the session address that identifies the user of the session protocol entity.

Transport layer. The fourth layer of the OSI reference model which ensures that the data are reliably delivered to the correct destination regardless of which network layer protocol and underlying subnetworks are being used.

Transport protocol class 4 (TP-4). Transport protocol class 4 is defined in ISO/IEC 8073 and profiled for ATN context to provide the connection mode transport service as described in ISO/IEC 8072.

Transport service access point (TSAP). The logical access point to the transport layer.

Transport service access point (TSAP) address. The complete communication address which unambiguously defines a transport service user. The TSAP address comprises the NSAP address and a TSAP selector.

Transport service data unit (TSDU). The data presented to the transport layer for transmission over the ATN Internet communications service.

Upper layer communications service (ULCS). A term pertaining to the session, presentation and application layers of the OSI reference model.

Chapter 1

INTRODUCTION

1.1 OVERVIEW

1.1.1 General

Included in this part of Doc 9880 are technical provisions for the upper layer communications service (ULCS) and the Internet communications service (ICS).

1.1.2 Upper layer communications service (ULCS)

The ULCS allows aeronautical telecommunication network (ATN) applications to specify their peer-to-peer communication requirements by use of the common abstract ATN dialogue service (DS). It specifies the protocols necessary to establish an association between peer application entities, to encode and transfer data, and to perform an orderly or abrupt release of the association. It specifies a minimal profile of the open systems interconnection (OSI) session and presentation layers. In addition, it includes application naming and addressing provisions.

1.1.3 Internet communications service (ICS)

The ATN ICS is provided to the upper layer architecture. The ICS is made up of the Internet routing architecture, which itself is composed of routing domains, administrative domains, routing domain confederations, the ATN backbone, ATN islands, etc. It is based on the ISO connectionless network protocol (CLNP), ISO connection-oriented transport protocol (Class 4) and the inter-domain routing information exchange protocol (IDRP). Using these, it supports the various candidate ground-ground and air-ground subnetworks of the ATN in order to ensure successful inter-operation of ATN intermediate systems and the subnetworks to which they are attached. It also provides mechanisms for priority handling, policy-based routing, the exchange of routing information and compression techniques to enable the efficient use of the limited bandwidth available over such air-ground subnetworks.

1.2 REFERENCES

1.2.1 Throughout this manual, any references to the ATN ICS technical provisions are references to Chapter 3 of this part of Doc 9880.

1.2.2 In Chapter 2, the reference (“Ref.”) column of a number of tables makes reference to the protocol implementation conformance statement (PICS) pro forma tables (ISO/IEC 8327-2 | ITU-T Rec. X.245 (1995), ISO/IEC 8823-2 | ITU-T Rec. X.246 (1996) and ISO/IEC 8650-2 | ITU-T Rec. X.247 (1996)).

1.2.3 Any references to the ATN Priority Table are references to Table 3-1: “Mapping of ATN communication priorities” in Annex 10 — *Aeronautical Telecommunications*, Volume III — *Communication Systems*. The table has been reproduced in this part of Doc 9880 as Table 1-1 for ease of reference.

Table 1-1. Mapping of ATN communication priorities

Message categories	*ATN application*	*Corresponding protocol priority*	
		Transport layer priority	*Network layer priority*
Network/systems management		0	14
Distress communications		1	13
Urgent communications		2	12
High-priority flight safety messages	CPDLC, ADS-C	3	11
Normal-priority flight safety messages		4	10
Meteorological communications		5	9
Flight regularity communications	DLIC, ATSMHS	6	8
Aeronautical information service messages		7	7
Network/systems administration	DIR	8	6
Aeronautical administrative messages		9	5
<unassigned>		10	4
Urgent-priority administrative and U.N. Charter communications		11	3
High-priority administrative and State/Government communications		12	2
Normal-priority administrative communications		13	1
Low-priority administrative communications and aeronautical passenger communications		14	0
Note.— The network layer priorities shown in the table apply only to connectionless network priority and do not apply to subnetwork priority.			

Chapter 2

UPPER LAYER COMMUNICATIONS SERVICE (ULCS)

2.1 INTRODUCTION

2.1.1 Overview

This chapter is designed as follows:

- Section 2.1 — INTRODUCTION: Besides outlining the material covered in Chapter 2, this section contains the purpose and structure of the ULCS specification, and a background to its functionality. In addition, it provides conventions related to the ULCS.

- Section 2.2 — DIALOGUE SERVICE (DS) DESCRIPTION: The abstract service that is defined for application specifications to refer to in order to provide a common connection-oriented communications service is described in this section.

- Section 2.3 — APPLICATION ENTITY (AE) DESCRIPTION: This section describes the AE and specifies the control function (CF) that coordinates the operation of the various application service elements (ASEs). It also describes the names that are assigned to various upper layer entities.

- Section 2.4 — SESSION LAYER REQUIREMENTS: This section describes the requirements for the OSI session layer, in the form of a profile requirements list (PRL).

- Section 2.5 — PRESENTATION LAYER REQUIREMENTS: This section describes the requirements for the OSI presentation layer, in the form of a PRL.

- Section 2.6 — ACSE SPECIFICATION: The requirements for the association control service element (ACSE) are covered in this section.

- Section 2.7 — CONNECTIONLESS DIALOGUE SERVICE (CLDS) AND PROFILE: This section is a placeholder for a connectionless service that is not currently needed by any application in this manual.

- Section 2.8 — ATN MESSAGE INTEGRITY CHECK ALGORITHM: This section discusses the proof that can be provided when the integrity sequence is computed and verified.

2.1.2 Scope and objectives

2.1.2.1 The ATN upper layer (UL) specification defines the dialogue service (DS) used by certain ATN applications. This specification is designed to optimize the use of communications bandwidth, and consequently it restricts the functionality available from the OSI session and presentation layers.

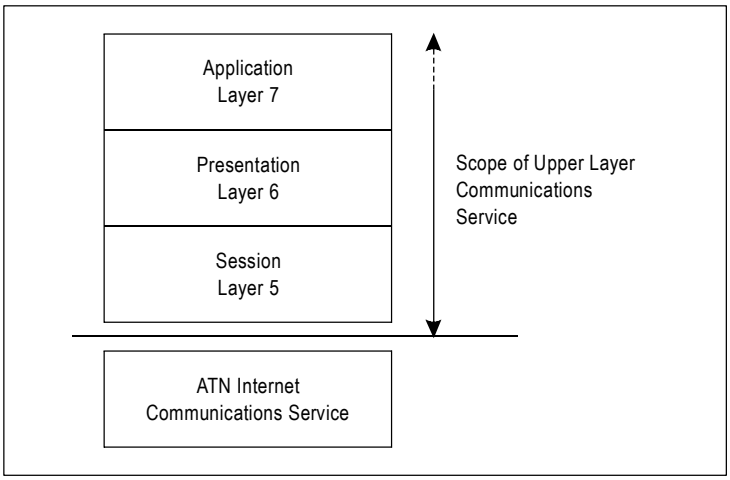
2.1.2.2 The ATN requirements are addressed for session layer (Layer 5), presentation layer (Layer 6) and a part of application layer (Layer 7) of the OSI reference model. Figure 2-1 shows a conceptual view of the scope of the ULCS.

The remaining part of the application layer is the province of the individual ATN applications.

2.1.2.3 The ULCS specification includes a profile for the protocols in the upper layers, an AE structure and a number of common application services.

2.1.3 Background

The communication aspects of the ATN applications are modelled as AEs (see 2.1.4.2). Figure 2-2 illustrates an example of the application layer structure for the ATN applications.



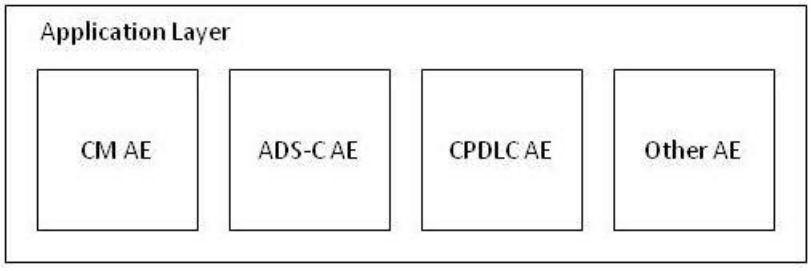


Figure 2-2. Conceptual view of the application layer

2.1.4 Upper layer functionality

2.1.4.1 Upper layer profile overview

2.1.4.1.1 A profile is specified for the connection-oriented protocols of the session layer, the presentation layer and the association control service element (ACSE).

2.1.4.1.2 The session portion of the specified profile is based on the efficiency enhancements to the session protocol that are standardized in ISO/IEC 8327-1: 1996 / Amdt 1: 1997 | ITU-T Rec. X.225 (1995)/Amdt 1 (1997).

2.1.4.1.3 The presentation portion of the specified profile is based on the efficiency enhancements to the presentation protocol that are standardized in ISO/IEC 8823-1: 1994 / Amdt 1: 1997 | ITU-T Rec. X.226 (1994)/Amdt 1 (1997).

2.1.4.1.4 As a consequence of using the session and presentation protocol efficiency enhancements, the protocol control information transferred by these protocols amounts to two octets in each direction during the connection establishment phase, and zero octets at all other times.

2.1.4.1.5 The ACSE portion of the specified profile is based on ISO/IEC 8650-1: 1996 | ITU-T Rec. X.227 (1995), including the extensibility notation as specified in Amendment 1 to that standard.

2.1.4.2 AE structure

2.1.4.2.1 The specified AE structure is based on the application layer structure defined in ISO/IEC 9545 | ITU-T Rec. X.207 (1993), where the concepts of application service element (ASE), application service object (ASO) and control function (CF) are defined.

2.1.4.2.2 Figure 2-3 shows the generic structure of an AE, with arrows representing the abstract service boundaries of the various elements. The “upper” service boundary is the abstract service that is provided by an ASE to its user(s). The “lower” service boundary is the abstract service that is provided to the ASE by the CF.

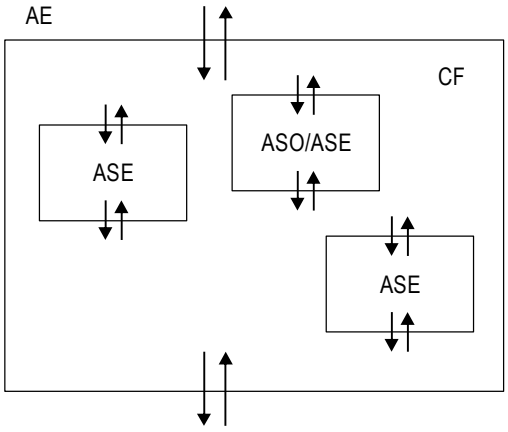


Figure 2-3. Generic AE structure

2.1.4.2.3 The ASE is an element engineered to perform a required task. ISO/IEC 9545 | ITU-T Rec. X.207 describes how two or more ASEs may be combined, together with a CF, to coordinate their operation to form an ASO. In turn, an ASO may be combined with other ASOs or ASEs with a CF to form larger ASOs. The AE is the outermost ASO.

2.1.4.3 Application services

2.1.4.3.1 For each of the current ATN applications, there exists a specific ASE, which is defined in the relevant ATN application specification. The generic name “ATN-App ASE” is used for these specific ASEs.

2.1.4.3.2 Various abstract services are specified. The services are provided at abstract service boundaries. The abstract service provided by the AE to the application-user (i.e. the service provided at the upper boundary of the AE) is specified in 2.3. In the AE structure specified here, this service is a pass-through to the ATN-App ASE.

2.1.4.3.3 Figure 2-4 shows the AE structure that is used to model the ATN applications (see 2.3 for a more detailed description).

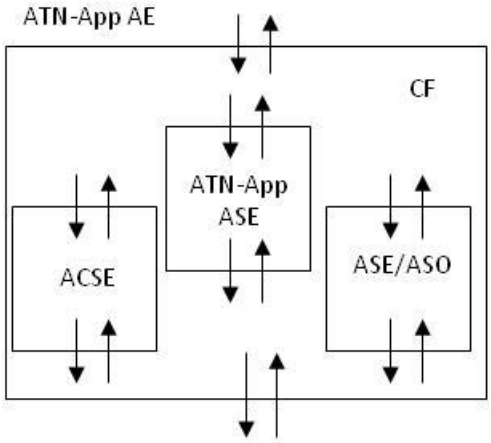


Figure 2-4. ATN-specific AE structure

2.1.4.3.4 The DS, as defined in 2.2, is the abstract service that the ATN-App ASEs use to interact with the ULCS. That is, the DS is the combination of specific internal primitives made available by the CF at the lower boundary of the ATN ASE/ASO — it is the application’s “world view”. In order to provide the DS, the CF uses the services of ACSE.

2.1.5 Conventions

2.1.5.1 In the tables of service primitives used throughout the ULCS specification, the presence/absence of each parameter is described by one of the following values:

blank not present;

C conditional upon some predicate explained in the text;

C(=) conditional upon the value of the parameter to the immediate left being both present and equal;

M mandatory;

M(=) mandatory, and equal to the value of the parameter to the immediate left; or

U user option.

2.1.5.2 The following abbreviations are used in the various service descriptions and protocol tables:

Req request; an invocation of a service primitive initiated from the user of an abstract service and submitted to the service for action;

Ind indication; an invocation of a service primitive delivered from the abstract service to a user of the service;

Rsp response; an invocation of a service primitive submitted by the user of an abstract service in response to a previous indication, in the case of a confirmed service; and

Cnf confirmation; an invocation of a service primitive delivered from the abstract service to a user of the service, which confirms that a previous request primitive from that user has been acted upon by the service, in the case of a confirmed service.

2.1.5.3 An unconfirmed service allows a single data transfer in one direction without the semantics of a response in the opposite direction.

2.1.5.4 A confirmed service provides confirmation to a service user of the outcome of an invocation of that service, e.g. that a data transfer initiated by that user was delivered to its peer user.

2.1.5.5 An abstract service is a syntactical description of a parameter that does not imply a specific implementation.

2.2 DIALOGUE SERVICE (DS) DESCRIPTION

2.2.1 Scope of the DS

2.2.1.1 Implementations of the ATN-App ASE, together with the UL elements, that provide the DS shall exhibit the behaviour defined in this abstract service definition.

2.2.1.2 The DS is the abstract service that is used by an ATN-App ASE at its lower service boundary. There is no requirement to implement the DS in any product. In general, ATN end systems are designed in such a way that it is impossible to detect (from external access) whether or not an interface corresponding to the DS has been built.

2.2.1.3 The DS is described from the viewpoint of the ATN-App ASE, using abstract service definition conventions. The abstract service definition is a descriptive technique used to specify the behaviour exhibited by part of the ATN application layer. Specifications of ASEs, such as the specifications of ADS-C, CPDLC and CM, may include common functionality by reference to the DS. The DS allows ATN-App ASEs to be specified without the need to consider some of the complexities of various aspects of the underlying communications.

2.2.1.4 The DS supports a communication relationship between two peers for a duration that exists until the peers agree to terminate the relationship or the relationship is aborted.

2.2.1.5 The DS defines a service that may be used to support an ATN-App ASE at its lower service boundary. Such an ASE is denoted a “DS-user”. The DS-user can be specified to use the DS in a variety of ways that can be defined in terms of reliability characteristics. A number of user-visible service levels can thus be offered, including, for example, the ones listed below:

a) an unconfirmed service, which allows individual messages to be transmitted after a dialogue has been set up; and

b) a confirmed service, which provides end-to-end confirmation that a message sent by one DS-user was received and acknowledged by the peer DS-user.

2.2.1.6 An implementation of the DS-provider will typically be responsible for the detection of errors such as:

a) an invalid primitive (primitive unknown or error in parameter(s));

b) an invalid sequence (primitive issued at an inappropriate time);

c) insufficient resources on submission;

d) an invalid or unreachable recipient on submission;

e) a data field that is too large on receive (local implementation constraint has been exceeded); and

f) an invalid or unreachable recipient on receive.

2.2.1.7 An implementation of an ATN application that makes use of the DS has to be designed with error-handling procedures for local error conditions.

2.2.2 Service primitives

Implementations that claim to support the DS functionality shall exhibit the behaviour defined by the service primitives in Table 2-1. Table 2-2 lists the parameters used when invoking the services.

2.2.3 Service definition

2.2.3.1 Sequence of primitives

2.2.3.1.1 Implementations that claim to support the DS functionality shall exhibit behaviour allowing two communicating DS-users to:

a) establish a dialogue;

b) exchange user data;

c) terminate a dialogue in an orderly or abnormal fashion; and

d) be informed of a DS abnormal dialogue termination due to the underlying communications failure,

consistent with the appropriate use of the corresponding service primitives.

Table 2-1. Summary of DS primitives

Service	*Description*
D-START	This is a confirmed service used to establish the binding between the communicating DS-users.
D-DATA	This unconfirmed service is used by a DS-user to send a message from that DS-user to the peer DS-user.
D-END	This is a confirmed service used to provide the orderly unbinding between the communicating DS-users, such that any data in transit between the partners is delivered before the unbinding takes effect.
D-ABORT	This unconfirmed service can be invoked to abort the relationship between the communicating DS-users. Any data in transit between them may be lost.
D-P-ABORT	This unconfirmed service is used to indicate to the DS-user that the DS-provider has aborted the relationship with the peer DS-user. Any data in transit between the communicating DS-users may be lost.
D-UNIT-DATA	This unconfirmed service is used to send a single data item from one peer DS-user to another. Any problem in delivering the data item to the recipient will not be signalled to the originator. This service is specified in 2.7.

Table 2-2. Parameters of the DS primitives

Service	*Parameters*
D-START	Called Peer ID Calling Peer ID DS-user Version Number Security Requirements Quality of Service Result Reject Source User Data
D-DATA	User Data
D-END	Result User Data
D-ABORT	Originator User Data
D-P-ABORT	(No parameters)

2.2.3.1.2 Either DS-user may send data at any time after the initial D-START exchange, by using the D-DATA service. Under normal circumstances, a dialogue is released by a DS-user invoking the D-END service. A dialogue is abnormally released with the D-ABORT service. If the underlying service provider abnormally releases the dialogue, the DS-users that are aware of the dialogue will be notified with the D-P-ABORT service.

2.2.3.1.3 For the purposes of this service definition, it is only valid for the DS-user to issue and receive primitives for one dialogue according to the permitted sequences of DS primitives shown in Table 2-3, where intersections marked "Y" show possible primitives that may occur after the primitive in the column heading.

Table 2-3. Sequence of DS primitives for one dialogue initiated by one DS-user

The DS primitive X → may be followed by the DS primitive Y	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
1 D-START req													
2 D-START cnf (accepted)	Y												
3 D-START ind								Y		Y	Y	Y	Y
4 D-START rsp (accepted)			Y										
5 D-DATA req		Y		Y	Y	Y			Y				
6 D-DATA ind		Y		Y	Y	Y	Y						
7 D-END req		Y		Y	Y	Y							
8 D-END cnf (accepted)							Y						
9 D-END ind		Y		Y	Y	Y							
10 D-END rsp (accepted)									Y				
11 D-ABORT req	Y	Y	Y	Y	Y	Y	Y		Y				
12 D-ABORT ind	Y	Y	Y	Y	Y	Y	Y		Y				
13 D-P-ABORT ind	Y	Y	Y	Y	Y	Y	Y		Y				

2.2.3.1.4 For compactness, each DS primitive is given a number in the column headings in Table 2-3; the numbers have the meanings assigned in the row headings. For simplicity, where D-START and D-END response and confirmation primitives are used, Table 2-3 only shows the case where the D-START or D-END request is accepted by the peer. If the D-START request is rejected, then the DS-user may not issue or receive any other primitives apart from a D-START request or indication. If the D-END request is rejected, then the DS-user may continue to issue and receive primitives as if the dialogue had just been established. A D-START request results in a new instance of communication with the peer DS-user, so it could occur at any time. Table 2-3 only applies to a single instance of communication.

2.2.3.2 The D-START service

2.2.3.2.1 The behaviour defined by the D-START service primitive shall be provided to enable the setting up of a dialogue between two DS-users.

2.2.3.2.2 D-START is a confirmed service that is invoked by a DS-user (the dialogue initiator) to start a dialogue with a peer DS-user. D-START request, indication, response and confirmation primitives are defined as illustrated in Figure 2-5.

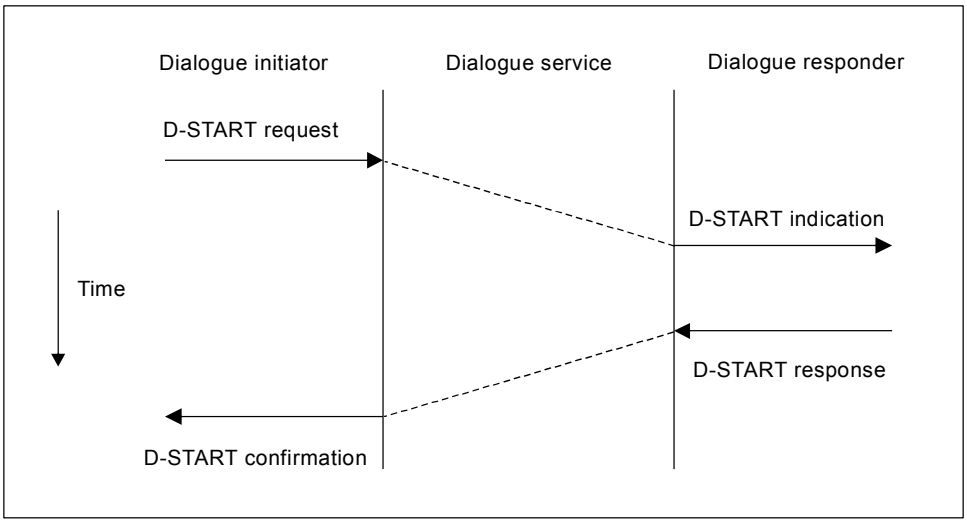


Figure 2-5. D-START sequence diagram

2.2.3.2.3 The initiating DS-user issues a D-START request primitive. It is not then valid to issue any other primitives (except D-ABORT) until a D-START confirmation is received. When the responding DS-user receives the D-START indication primitive, it must decide whether or not to accept this instantiation of the DS. It may issue only a D-START response or a D-ABORT request primitive. The D-START response and confirmation primitives contain a Result parameter, which defines whether the responding DS-user accepts or rejects the request. If the responding DS-user accepts the request, then the dialogue is established. If it rejects the request, then no dialogue exists. The parameters of the D-START primitives are specified in Table 2-4, and they are explained in more detail in paragraphs 2.2.3.2.4 to 2.2.3.2.14.

Table 2-4. D-START parameters

Parameter name	*Req*	*Ind*	*Rsp*	*Cnf*
Called Peer ID	M			
Calling Peer ID	U	C(=)		
DS-user Version Number	U	C(=)	U	C(=)
Security Requirements	U	M(=)	U	M(=)
Quality of Service	M	M(=)	U	M(=)
Result			M	M
Reject Source				C
User Data	U	C(=)	U	C(=)

2.2.3.2.4 The Called Peer ID parameter is used in the D-START service to specify the name of the intended peer DS-user, and it takes an abstract value corresponding to either a 24-bit ICAO aircraft address or an ICAO facility designator.

2.2.3.2.5 The DS-user may optionally request that the name of the initiating DS-user be conveyed to the peer DS-user in the D-START service. The presence of the Calling Peer ID in the D-START indication primitive is conditional

upon it being specified by the DS-user in the D-START request primitive. The syntax of the Calling Peer ID is identical to the corresponding Called parameters described in 2.2.3.2.4.

2.2.3.2.6 The DS-user version number allows peer DS-users to exchange version information. The parameter is optional in the request and response primitives. Its presence in the indication primitive is conditional upon it being specified by the DS-user in the request primitive, and its presence in the confirmation primitive is conditional upon it being specified by the DS-user in the response primitive. If present, the DS-user version number may take any abstract value in the range of 1 to 255.

2.2.3.2.7 The Security Requirements parameter allows peer DS-users to agree on the type of secured dialogue. The parameter is optional in the request and response primitives, and its omission by the DS-user is equivalent to the abstract value “no security”. In this version of the protocol, the Security Requirements parameter can only take the value “no security”.

2.2.3.2.8 The Quality of Service (QOS) parameter allows the initiating DS-user to specify in the request primitive its requirements for the QOS to be provided for the dialogue. For ATN, the parameter is not modified by the DS-provider so the value in the indication primitive is equal to the value in the request primitive. The QOS parameter in the response primitive is assumed by the CF to be equal to the value in the indication primitive. The value of the QOS parameter in the confirmation primitive is equal to that present or assumed in the response primitive. The following QOS parameters may be specified:

a) Routing Class — valid values are defined in the ATN ICS technical provisions;

b) Priority — valid values are defined in the ATN Priority Table; and

c) Residual Error Rate (RER) — valid values are defined in the connection mode transport service QOS section of the ATN ICS technical provisions (not significant for ATSC applications).

2.2.3.2.9 If the Routing Class parameter is not provided by the DS-user in the D-START request primitive, and the DS-user is an ATS application as specified in Parts I or II of this manual, then the default value “ATSC: no traffic type policy preference” is assumed. If the DS-user is not one of these ATS applications, then the default traffic type “general communications” is assumed.

2.2.3.2.10 If a Priority value is not provided by the DS-user in the D-START request primitive, then the default value “network/systems administration” is assumed.

2.2.3.2.11 For the RER parameter, a low error rate corresponds to a high quality connection, and a high error rate corresponds to a low quality connection. For ATSC applications, the highest available integrity level is always selected. Other types of applications may select the required integrity level in the D-START request, e.g. for compatibility with basic ISO | ITU-T transport service (TS) providers that do not support the ATN enhanced transport checksum.

2.2.3.2.12 The Result parameter specifies whether the requested dialogue start has been accepted. It can take one of the following abstract values:

a) accepted;

b) rejected (transient); or

c) rejected (permanent).

2.2.3.2.13 The Reject Source parameter is present if the Result parameter has one of the values “rejected (transient)” or “rejected (permanent)”. It specifies who rejected the start of the dialogue and can have one of the following abstract values:

a) DS-user; or

b) DS-provider.

2.2.3.2.14 The User Data parameter allows the peer DS-users to exchange data during the D-START service invocation. Its presence in the indication primitive is conditional upon it being specified by the DS-user in the request primitive, and its presence in the confirmation primitive is conditional upon it being specified by the DS-user in the response primitive.

2.2.3.3 The D-DATA service

2.2.3.3.1 The behaviour defined by the D-DATA service primitive shall be provided to enable the exchange of information between two DS-users.

2.2.3.3.2 D-DATA is an unconfirmed service that provides data transfer between peer DS-users. The D-START service must first have been successfully completed to establish the communication relationship between the peers. Request and indication primitives are defined as illustrated in Figure 2-6.

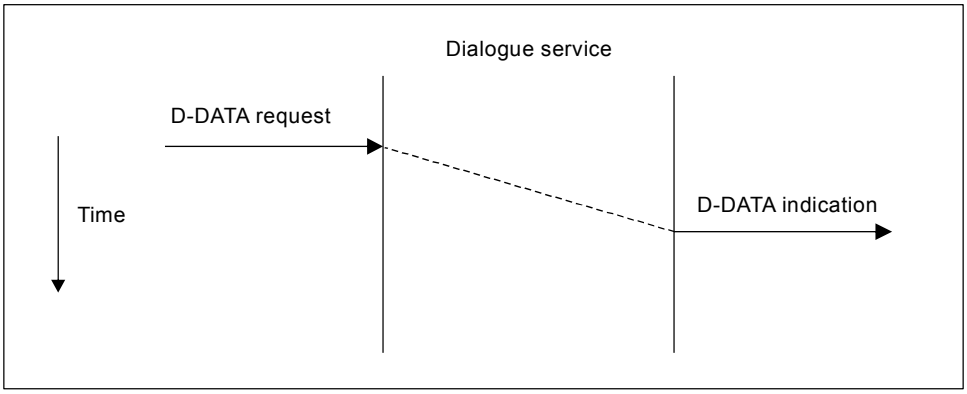


Figure 2-6. D-DATA sequence diagram

2.2.3.3.3 The parameters of the D-DATA primitives are specified in Table 2-5.

Table 2-5. D-DATA parameters

Parameter name	*Req*	*Ind*
User Data	M	M(=)

2.2.3.3.4 The User Data parameter contains the data to be transferred from a DS-user to its peer, using an existing dialogue.

2.2.3.4 The D-END service

2.2.3.4.1 The behaviour defined by the D-END service primitive shall be provided to enable the orderly termination of a dialogue between two DS-users.

2.2.3.4.2 D-END is a confirmed service that causes the end of a dialogue. It may be invoked by either of the communicating partners. When the D-END service is invoked, the DS performs an orderly release, whereby any service previously invoked is completed before the dialogue is terminated. The D-END service defines request, indication, response and confirmation primitives as illustrated in Figure 2-7.

2.2.3.4.3 The DS-user that wishes to terminate the dialogue issues a D-END request primitive. After issuing a D-END request primitive, the DS-user must not then issue any other service primitive (except D-ABORT, if required) until a D-END confirmation is received. After issuing a D-END request primitive, the DS-user must be prepared to continue receiving D-DATA indications from the peer user until a D-END confirmation primitive is received.

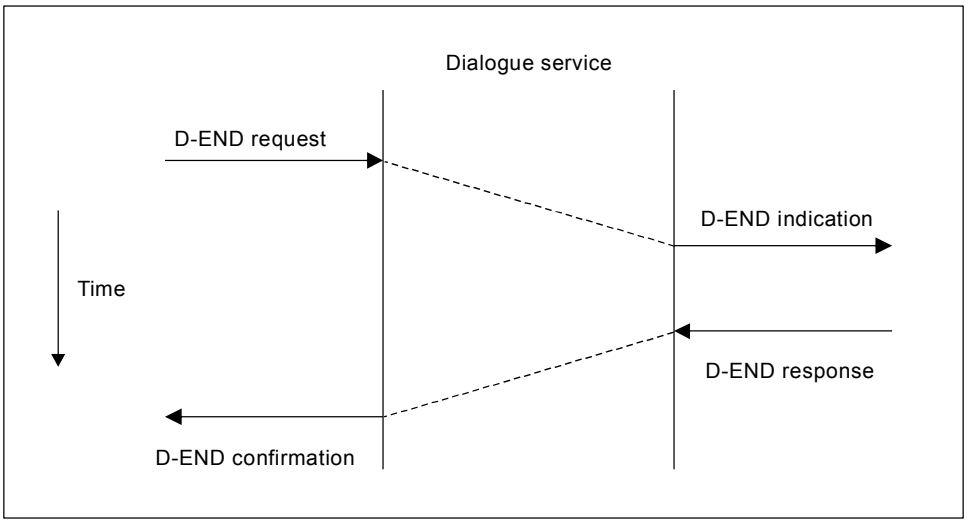


Figure 2-7. D-END sequence diagram

2.2.3.4.4 If the D-END confirmation contains a result code of “accepted”, then the dialogue no longer exists. If the D-END confirmation contains a result code of “rejected”, then the peer DS-user does not wish to terminate the dialogue, and both DS-users are free to use the dialogue as if the D-END service had never been invoked.

2.2.3.4.5 When a DS-user receives a D-END indication primitive, it may continue to send data using the D-DATA service, but it may at some time issue a D-END response primitive with a result code of “accepted” or “rejected”. After issuing a D-END response primitive with a result code of “accepted”, a DS-user must not issue any other service primitive, as the dialogue no longer exists. After issuing a D-END response primitive with a result code of “rejected”, a DS-user may issue any other service primitive as if the D-END service had never been invoked.

2.2.3.4.6 The parameters of the D-END primitives are specified in Table 2-6.

Table 2-6. D-END parameters

Parameter name	*Req*	*Ind*	*Rsp*	*Cnf*
Result			M	M(=)
User Data	U	C(=)	U	C(=)

2.2.3.4.7 The Result parameter specifies whether or not the requested dialogue end has been accepted. It can take one of the abstract values “accepted” or “rejected”.

2.2.3.4.8 The User Data parameter contains the data to be transferred from a DS-user to its peer, using an existing dialogue. Its presence in the confirmation primitive is conditional upon it being specified by the DS-user in the response primitive.

2.2.3.4.9 In the event of a service disruption (e.g. by D-P-ABORT), the invoker of the D-END response primitive will never know that any associated user data failed to be delivered, as the service is already terminated.

2.2.3.4.10 A D-END collision occurs when both peers issue a D-END request primitive almost simultaneously, such that neither peer has yet received the D-END indication primitive corresponding to the remote peer’s D-END request. The collision is handled by the CF on behalf of the DS-user. However, one result of the collision handling is that any user data present in the D-END request will be delivered to the peer in a D-END confirmation primitive rather than in the usual D-END indication. This means that the peer will be unable to react to the contents of the User Data parameter, as the dialogue will have terminated. When a DS-user application is designed such that either peer may terminate the dialogue, then the application cannot require a response to any user data that is sent on a D-END request primitive. Figure 2-8 illustrates the D-END collision from the viewpoint of the two DS-users.

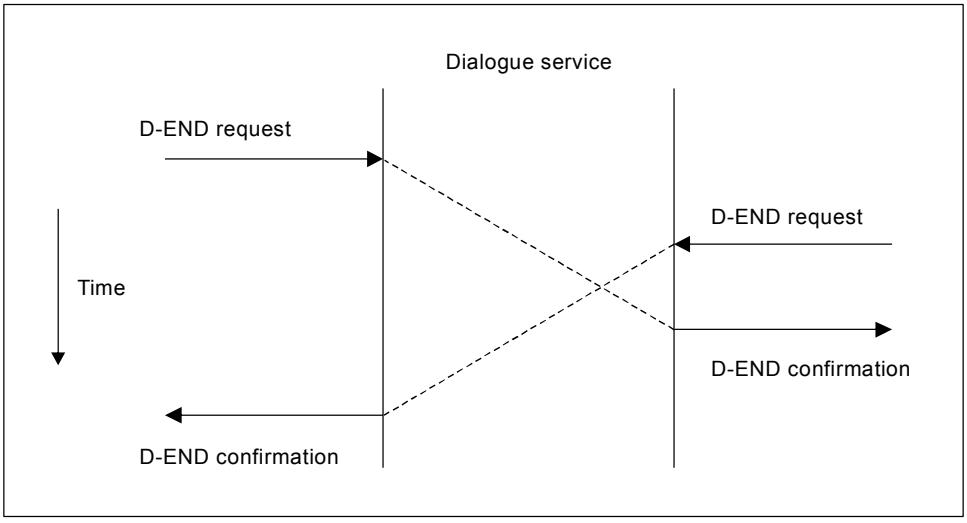


Figure 2-8. D-END collision sequence diagram (DS-user view)

2.2.3.5 The D-ABORT service

2.2.3.5.1 The behaviour defined by the D-ABORT service primitive shall be provided to enable the abnormal release of a dialogue between two DS-users, by either DS-user.

2.2.3.5.2 The D-ABORT service request and indication primitives are defined as illustrated in Figure 2-9.

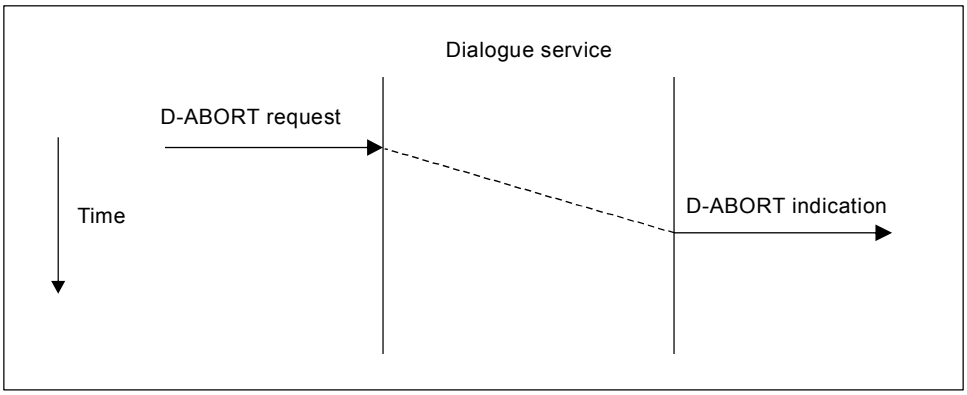


Figure 2-9. D-ABORT sequence diagram

2.2.3.5.3 When a dialogue is aborted, data in transfer may be lost. The parameters of the D-ABORT primitives are specified in Table 2-7.

Table 2-7. D-ABORT parameters

Parameter name	*Req*	*Ind*
Originator	U	C(=)
User Data	U	C(=)

2.2.3.5.4 The Originator parameter is used to distinguish the source of the abort. Its presence in the indication primitive is conditional upon it being specified by the DS-user in the request primitive. It can take one of the following abstract values:

a) User — the abort originated from the application-user; or

b) Provider — the abort originated in the ATN-App AE (including the ATN-App ASE).

2.2.3.5.5 If the D-ABORT Originator parameter is not specified, the default value “provider” is assumed.

2.2.3.5.6 The User Data parameter contains the data to be transferred from a DS-user to its peer, using an existing dialogue. Its presence in the indication primitive is conditional upon it being specified by the DS-user in the request primitive. There is no guarantee that the peer will receive the user data; the sender will not be informed if the user data is not delivered.

2.2.3.6 The D-P-ABORT service

2.2.3.6.1 The behaviour defined by the D-P-ABORT service primitive shall be provided to indicate an abnormal release of a dialogue by the supporting communications service.

2.2.3.6.2 For the D-P-ABORT service, only an indication primitive is defined, as illustrated in Figure 2-10.

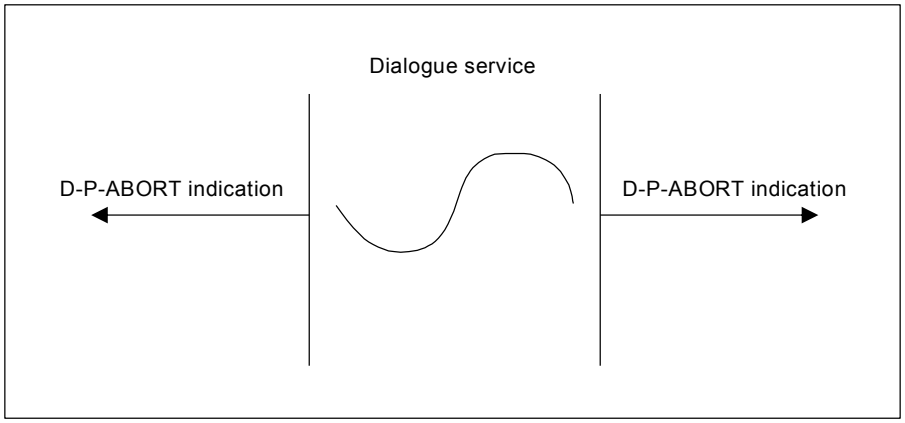


Figure 2-10. D-P-ABORT sequence diagram

2.2.3.6.3 The D-P-ABORT service allows the supporting communications service to indicate to the DS-users that it aborted the dialogue. When the dialogue is aborted, any data in transit may be lost. The D-P-ABORT primitive has no parameters.

2.3 APPLICATION ENTITY (AE) DESCRIPTION

2.3.1 Introduction

2.3.1.1 As indicated in 2.1, the AE is described in terms of the service that it displays to the application-user, and in terms of the CF that mediates the interactions of the components of the AE.

2.3.1.2 The ATN-App AE shall exhibit external behaviour as if implemented according to the model shown in Figure 2-11, with the protocols defined in the ACSE and the ATN-App ASE specifications.

2.3.1.3 Figure 2-11 indicates which paragraph in this chapter describes the behaviour of the CF in response to events at various service boundaries.

2.3.1.4 Functionality could be increased in future versions of the ATN upper layer architecture by the addition of ASEs or ASOs other than those shown in Figure 2-11. ACSE provides the basic mechanisms for establishing and releasing an application association. The service provided by the ATN-App AE represents an abstract description of the application programming interface seen by the application-user. The CF of the ATN-App AE specifies how the interactions at the ATN-App AE service boundary invoke the appropriate service primitives of the constituent ASEs, which in turn generate the actual protocol. The CF also specifies how the constituent ASEs interact with the supporting communications service.

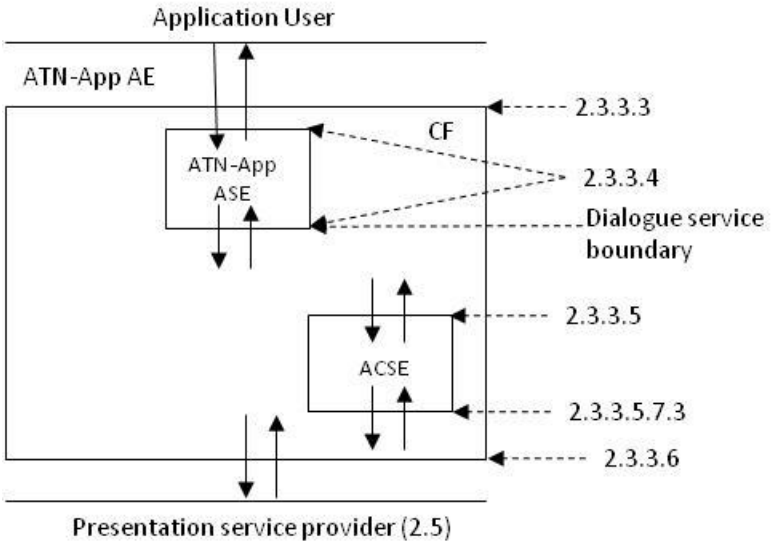


Figure 2-11. Components of ATN-App AE

2.3.1.5 A CF specification is not a service definition of the ATN-App AE or its components. It only defines the actions of the CF as a result of service invocations visible to the CF. Thus, the specification is organized around specifying the response of the CF to these inputs. Section 2.3.3.3 specifies the actions that result from the inputs of the Application-user. Section 2.3.3.4 specifies the actions that result from the service invocations of the ATN-App ASE component ASE. Section 2.3.3.5 (including 2.3.3.5.7.3) specifies the actions that result from the service invocations of the ACSE component ASE. Section 2.3.3.6 specifies the actions that result from the inputs of the supporting service.

2.3.1.6 The CF specification describes the overall behaviour of the ATN-App AE. It is not a requirement that an identifiable CF entity be realized in an implementation.

2.3.1.7 This CF specification assumes that the embedded ASEs (ATN-App ASE and ACSE) are modelled as atomic entities, such that when an input event is invoked by the CF, that event is processed to completion by the ASE and the CF responds to any resulting output events from the ASE, all within the same logical processing thread. This model avoids the need to specify further transient states within the CF. It does not imply any particular implementation architecture.

2.3.1.8 In the current version of the ATN upper layers, the service interface presented to the application-user is a simple pass-through to the ATN-App ASE. That is, the Application-user passes request and response primitives directly to, and receives indication and confirmation primitives directly from, the ATN-App ASE.

2.3.1.9 For the purposes of this specification, the ATN-App AE is modelled such that a new instance of communication (effectively a new AE invocation) is implicitly created for:

a) each request from the AE-user that will require a new association (i.e. that will result in a D-START request being invoked); and

b) each indication from the underlying communications service that a new connection is requested.

The AE invocation ceases to exist when the underlying communications service connection is disconnected and the CF

is idle (i.e. in the NULL state).

2.3.2 Application level naming and context definition

2.3.2.1 ATN upper layers naming hierarchy

2.3.2.1.1 Names, in the form of object identifiers (OIDs), are assigned in the upper layers to the defined ATN entities.

2.3.2.1.2 The upper nodes of the ATN naming hierarchy are defined in Part IV of this manual. The portion of the ATN naming hierarchy relevant to the ULCS is illustrated in Figure 2-12.

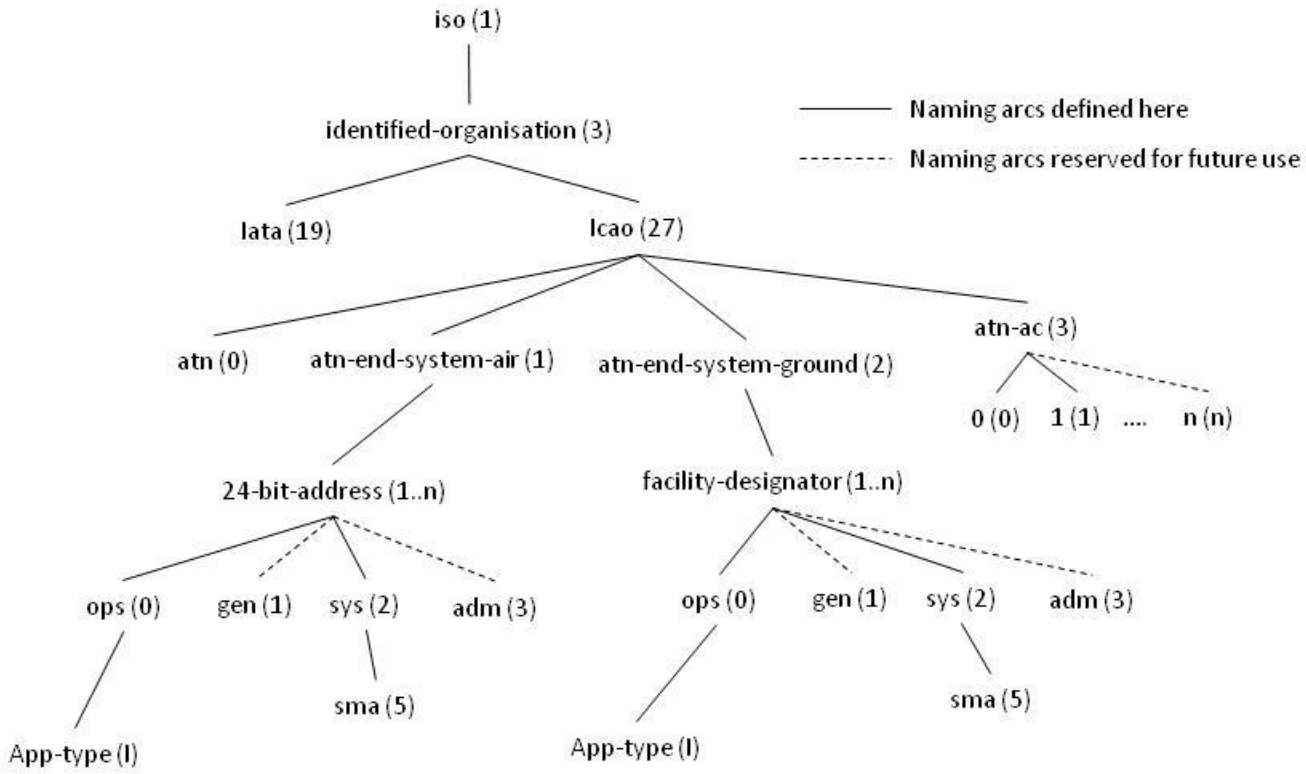


Figure 2-12. ATN naming hierarchy

2.3.2.1.3 The root nodes of the naming subtrees relevant to the ULCS are shown in Table 2-8.

Table 2-8. Naming roots of the upper layers

Name and numeric value	*Description*
atn-end-system-air (1)	ATN aircraft end systems. The following OID component beneath this arc is a 24-bit ICAO aircraft address.
atn-end-system-ground (2)	ATN ground end systems. The following OID component beneath this arc is an ICAO facility designator.
atn-ac (3)	ATN application context names.

2.3.2.2 Application process titles (AP-titles)

2.3.2.2.1 AP-titles are allocated underneath either of the following OID arcs:

a) { atn-end-system-air (1) }; or

b) { atn-end-system-ground (2) }.

2.3.2.2.2 Immediately subordinate to the OID arc in 2.3.2.2.1 a) or b) is an arc whose value is an INTEGER derived from either the 24-bit ICAO aircraft address or the ICAO facility designator, as described in 2.3.2.4. Immediately beneath that arc is an arc whose value is determined by the category of the ATN application. At present, only the following names and values are defined for the application category:

a) { ops (0) } — for operational applications; and

b) { sys (2) } — for system management applications.

2.3.2.2.3 Subordinate to the application category arc is an arc whose value is determined by the type of the ATN application process (e.g. ads-c(0) and cm(1)), as defined in Part IV of this manual.

2.3.2.2.4 Each application process type on each ATN end system shall be assigned an unambiguous AP-title.

2.3.2.2.5 The AP-title shall be an OID type (i.e. an AP-title-form2 as defined in ISO/IEC 8650-1: 1996 | ITU-T Rec. X.227 (1995)).

2.3.2.2.6 AP-titles shall be expressed in either of the following forms:

a) {iso(1) identified-organization(3) icao(27) atn-end-system-air(1) <end-system-id>(n) category(m) <app-type>(k)}; or

b) {iso(1) identified-organization(3) icao(27) atn-end-system-ground(2) <end-system-id>(n) category(m) <app-type>(k)}

where:

<end-system-id>	is the ICAO 24-bit address for aircraft end systems, or the ICAO facility designator for ground end systems;
(n)	is an INTEGER value derived from the <end-system-id>; *Note.— The algorithm for deriving the INTEGER n from the <end-system-id> is defined in 2.3.2.4.*
<category>	is the application category, either ops (operational) or sys (system management);
(m)	is the INTEGER value corresponding to the application category ops(0) or sys(2);
<app-type>	is the application type; and
(k)	is the INTEGER value corresponding to the application type, and it takes one of the values specified in Part IV of this manual.

2.3.2.2.7 The app-type arc of the AP-title OID represents the ATN application type (e.g. ADS-C and CM) and shall take one of the values specified in Part IV of this manual.

2.3.2.2.8 Part IV of this manual contains the global register of all standard ATN application types. Table 2-9 in this part shows how the names and numeric values that are assigned in Part IV are used in the construction of ATN AP-titles.

Table 2-9. Examples of ATN AP-titles

ATN ASE type (see Note)	*AP-title*
ADS-C-air ASE	iso(1) identified-organization(3) icao(27) atn-end-system-air(1) <aircraft id>(n) ops(0) ads-c(0)
CM-ground ASE	iso(1) identified-organization(3) icao(27) atn-end-system-ground(2) “ABCDEFGH”(n) ops(0) cm(1)
Note.— Refer to Part IV of this manual for a complete list of ASE types.	

2.3.2.3 Application entity titles (AE-titles)

2.3.2.3.1 Each ATN application entity shall be assigned an unambiguous AE-title.

2.3.2.3.2 For ATN, an AE-title shall be an OID type as defined in ISO/IEC 8824-1 | ITU-T Rec. X.680 (1995) (i.e. an AE-title-form2 as defined in ISO/IEC 8650-1: 1996 | ITU-T Rec. X.227 (1995)).

2.3.2.3.3 The AE-title is composed of an AP-title and an AE-qualifier. The AE-qualifier further qualifies the AP-title such that it identifies a given application type on a specific end system at a given location.

2.3.2.3.3.1 The AE-qualifier component of the AE-title shall be an INTEGER type (i.e. an AE-qualifier-form2 as defined in ISO/IEC 8650-1: 1996 | ITU-T Rec. X.227 (1995)).

2.3.2.3.3.2 The AE-qualifier value arc of the AE-title OID shall be an unambiguous system identifier with a value as specified in 2.3.2.4.

2.3.2.3.4 Thus, AE-titles conforming to this definition shall be in either of the following forms:

a) { iso(1) identified-organization(3) icao(27) atn-end-system-air(1) <end-system-id>(n) category(m) <app-type>(k) [<ae-qualifier>(j)] }; or

b) { iso(1) identified-organization(3) icao(27) atn-end-system-ground(2) <end-system-id>(n) category(m) <app-type>(k) [<ae-qualifier>(j)] }

where:

<end-system-id> is the ICAO 24-bit address for aircraft end systems, or the ICAO facility designator for ground end systems;

(n) is an INTEGER value derived from the <end-system-id>;

Note.— The algorithm for deriving the INTEGER n from the <end-system-id> is defined in 2.3.2.4.

<category> is the application category, either ops (operational) or sys (system management);

(m) is the INTEGER value corresponding to the application category, ops(0) or sys(2);

<app-type> is the name form application type as specified in Part IV of this manual;

(k) is the INTEGER value corresponding to the application type, and it takes one of the values specified in Part IV of this manual;

Note.— The algorithm for deriving the INTEGER k from the <ae-qualifier> is defined in 2.3.2.4.

<ae-qualifier> is the unambiguous system identifier; and

(j) is the INTEGER value corresponding to the application from Part IV.

2.3.2.4 Encoding of end system identifiers

2.3.2.4.1 Where <end-system-id> appears as a component of an OID, the encoding of the OID subidentifier value is obtained as defined in the following text of this section.

2.3.2.4.2 For ground stations, the <end-system-id> is derived from a four- to eight-character facility designator, e.g. “LFPODLHX”. The syntax of the first four characters is defined in *Location Indicators* (Doc 7910) (the value “0000" is reserved). The syntax of the remaining characters is defined in *Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services* (Doc 8585).

2.3.2.4.3 For aircraft, the <end-system-id> naming arc shall be the binary value of the 24 bits comprising the ICAO aircraft identifier, expressed as an INTEGER in the range of (0 to (2^{24}-1) and encoded as an OID subidentifier as defined in ISO/IEC 8825-1 | ITU-T Rec. X.690 (1995).

2.3.2.4.4 For ground stations, the encoding of the <end-system-id> naming arc shall be derived from the ICAO facility designator, which is a sequence of characters from the restricted character set (A to Z), as follows:

a) Each character is encoded into one octet where:

1) the most significant bit (bit 8) indicates whether the character is the last in the sequence — it is set to zero in the last octet and to one in each preceding octet;

2) the next most significant bit (bit 7) is set to zero; and

3) the six least significant bits (bits 6 to 1) contain the character encoded as a 6-bit value such that A is encoded as the binary value 000001, B is encoded as 000010, and so on up to Z which is encoded as 011010.

b) The <end-system-id> is the concatenation of the octets in a).

2.3.2.4.4.1 The coding in 2.3.2.4.4 gives compatibility with the Basic Encoding Rules for an OID subidentifier in

ISO/IEC 8825-1 | ITU-T Rec. X.690 (1995). The character coding is equivalent to the “6-bit ASCII” subset of International Alphabet Number 5 (IA5) defined by ITU, which is adopted in SSR Mode S specifications. If required, the encoding can be extended to include numeric characters, with 0 to 9 encoded as binary values 110000 to 111001, respectively, and the space character can be encoded as binary value 100000.

2.3.2.4.4.2 Conceptually, bits 7 to 1 from each of these octets are concatenated to form an unsigned binary number whose most significant bit is bit 7 of the first octet and whose least significant bit is bit 1 of the last octet.

2.3.2.5 Application context names

2.3.2.5.1 The application context describes the ASE/ASO types that are present in the AE, including those aspects not distinguished by the ASO type (e.g. version and policy aspects). The abstract syntax of the APDUs and the CF are described in this section. The application context name is an identifier that is used to refer to a defined application context. The syntax of the application context name is defined in ISO/IEC 8650-1: 1996 | ITU-T Rec. X.227 (1995) as an OID.

2.3.2.5.2 The application context name is used in this manual only to distinguish between different versions of an application context within the scope of a given AE type, as identified by the AE-title.

2.3.2.5.3 The application context name shall be used to indicate the version and policy aspects relative to the AE with which it is associated.

2.3.2.5.4 Each application context shall be assigned an application context name.

2.3.2.5.5 Application context names shall have the following structure:

{iso (1) identified-organization(3) icao(27) atn-ac(3) version-<n> (n)}

where:

n is an INTEGER in the range of 0 to 255, with the value n = 0 reserved for use by the CF.

2.3.2.6 Presentation context identification

2.3.2.6.1 The null-encoding presentation protocol option has been selected for the most efficient encoding of presentation PDUs, as defined in 2.5. As a consequence, the conventional presentation protocol mechanisms, which enable users of the presentation service to distinguish the presentation context of received APDUs, are not available. Therefore, an alternative application layer mechanism is defined in this section.

2.3.2.6.2 All user data that is passed across the presentation service boundary shall be encoded using the unaligned variant of the Packed Encoding Rules (PER) for ASN.1 (ISO/IEC 8825-2 | ITU-T Rec. X.691 (1995)).

2.3.2.6.3 When in the data transfer phase, in order to be able to distinguish APDUs that are defined in different abstract syntax modules, the presentation user data encoding shall assume the full-encoding option of ISO/IEC 8823-1 | ITU-T Rec. X.226 (1994), augmented with the PER-visible constraints defined in ISO/IEC 8823-1: 1994/Amdt 1: 1997 | ITU-T Rec. X.226 (1994)/Amdt 1 (1997), as follows:

```
Fully-encoded-data ::= SEQUENCE SIZE (1, ...) OF PDV-list
-- contains one or more presentation-data-value-list (PDV-list) values
```

```
PDV-list ::= SEQUENCE
{ transfer-syntax-name              Transfer-syntax-name OPTIONAL,
presentation-context-identifier     Presentation-context-identifier,
presentation-data-values CHOICE
        { single-ASN1-type          [0] ABSTRACT-SYNTAX.&Type(CONSTRAINED BY
                                    {-- Type corresponding to presentation context identifier -- }) ,
        octet-aligned               [1] IMPLICIT OCTET STRING,
        arbitrary                   [2] IMPLICIT BIT STRING }
-- contains one or more presentation data values from the same
-- presentation context.
        }
Transfer-syntax-name                ::= OBJECT IDENTIFIER
                                    -- not used for ATN Upper Layers
Presentation-context-identifier::= INTEGER (1..127, ... )
```

2.3.2.6.3.1 Note that ISO/IEC 8823-1 | ITU-T Rec. X.226 specifies two choices for the encoding of user data: either simply-encoded-data or fully-encoded-data. For ATN, presentation user data is equivalent to fully-encoded-data and NOT to ISO/IEC 8823-1 | ITU-T Rec. X.226 user data. That is, the bit to indicate the CHOICE of simple or full encoding is NOT encoded.

2.3.2.6.3.2 The use of full encoding is specified in order to overcome the fact that:

a) the use of presentation protocol efficiency enhancements removes the ability of the presentation layer to perform the necessary demarcation; and

b) the use of ASN.1 PER means that it would not have been possible to assign unique ASN.1 tag values to individual APDUs to distinguish between them, as PER does not encode tags.

2.3.2.6.4 Only the presentation-context-identifier and presentation-data-values fields shall be present in the encoded presentation user data.

2.3.2.6.5 Only the “arbitrary” (BIT STRING) choice for presentation-data-values in the PDV-list SEQUENCE shall be used in the encoded presentation user data.

2.3.2.6.6 A bit-oriented encoding shall be applied, such that no padding bits are appended to the encoded BIT STRING value, and the length determinant of the BIT STRING encoding equates to the number of significant bits. This means that data encoded by ATN ASEs, when embedded in presentation-data-values, are treated by the CF as normal BIT STRING values, not in general as an integral number of octets. Padding to an octet boundary only applies to the outermost fully-encoded-data value that is passed across the presentation service boundary.

2.3.2.6.7 The values of presentation-context-identifier, which are pre-defined in Table 2-10, shall be used in the encoding of presentation user data; the presentation-context-identifiers are not dynamically assigned by the presentation service.

Table 2-10. Presentation context identifiers

Presentation-context-identifier value	*Short name*	*Description*
1	acse-apdu	ACSE abstract syntax as defined in ISO/IEC 8650-1: 1996 /Amdt 1: 1997 | ITU-T Rec. X.227 (1995)/Amdt 1 (1996)

Presentation-context-identifier value	*Short name*	*Description*
2		Reserved for future use
3	user-ase-apdu	Abstract syntax as defined in individual ATN application specifications
Other		Reserved for future use

2.3.2.6.8 With the sole exception of the P-CONNECT service (which is used exclusively by ACSE), upon receiving user data from the presentation service, the CF shall:

a) decode the fully-encoded-data and use the presentation-context-identifier value to determine the target ASE;

b) if the target ASE is ACSE, decode the header of the embedded presentation-data-value to determine the APDU type; and

c) if the decoding in a) or b) fails for any reason (presentation-context-identifier not recognized; presentation-data-value does not use the “arbitrary” CHOICE value; or unrecognized APDU type), then issue a P-U-ABORT request to the supporting service and behave as if a P-U-ABORT indication with no parameters has been received; otherwise

d) if the decoding in a) and b) does not fail, pass the presentation-data-value (i.e. acse-apdu or user-ase-apdu) to the target ASE by invoking the appropriate indication or confirmation primitive at the lower ASE service boundary, as specified in 2.3.3.

2.3.2.6.9 Except for P-CONNECT primitives issued by ACSE, when an ASE issues a request or response primitive at its lower service boundary that would otherwise map onto a presentation service primitive, the CF shall:

a) embed the user data into a fully-encoded-data type, using the presentation-context-identifier value corresponding to the source ASE; and

b) pass the fully-encoded user data to the presentation service by invoking the appropriate primitive, as specified in 2.3.3.

2.3.2.6.10 Between peer ATN-App AEs, a single default presentation context shall be used; this is known by bilateral agreement.

2.3.2.6.11 All component abstract syntax modules (e.g. ATN-App-ASE and ACSE) are considered merged into one. It is the job of the CF to merge and split contexts, since ATN does not use presentation layer context handling services.

2.3.2.6.12 ASN.1 PER (basic, unaligned variant) are used to provide the transfer syntax for the single abstract syntax.

2.3.2.6.13 Clause 7.9 of the PER Standard is not applicable to ATN for the following reasons:

a) EXTERNAL values are fully resolved since all abstract syntaxes are known *a priori.*

b) When carried in the (null) presentation protocol, “full encoding” with the BIT STRING choice alternative is used.

2.3.2.6.14 The “outermost value” referred to in Clause 10.1.1 of the PER Standard is interpreted in ATN context as the encoded data that passes over the presentation service boundary. Padding bits are appended to achieve octet alignment at this boundary.

2.3.3 Control function specification

2.3.3.1 ATN-App CF state definitions

The ATN-App AE shall behave as if it has a CF that can exist only in one of the following states:

a) NULL (STA0) — This is the state of the CF when there is no association in existence.

b) ASSOCIATION PENDING (STA1) — The CF enters this state when either the ATN-App ASE has made a request to establish a dialogue and is waiting for notification from its peer, OR an indication has been received that the peer has made a request to establish a dialogue.

c) DATA TRANSFER (STA2) — The CF enters this state once the establishment phase is complete. An association has successfully been established, and the communicating partners are free to send and receive data.

d) RELEASE PENDING (STA3) — The CF enters this state when either the ATN-App ASE has requested the termination of the dialogue, OR an indication has been received that the peer has made a request to terminate the dialogue.

e) RELEASE COLLISION (STA4) — The CF enters this state when both communicating partners have requested the termination of the dialogue almost simultaneously.

2.3.3.2 CF state table

2.3.3.2.1 The ATN-App AE CF shall behave as if it has a CF in accordance with the state table specified in Table 2-11, which shows diagrammatically the state transitions and actions performed by the CF in response to incoming events. See Table 2-12 for the predicates used in Table 2-11.

2.3.3.2.2 The following conventions are used in Table 2-11:

a) Incoming events are shown in the first two columns of the state table, and they are enumerated in Table 2-13.

b) When an input event occurs and the state table indicates an action, the CF performs that action.

c) Each cell in the state table shows:

1) optionally one or more predicates denoted “pN”, where N is an integer. The state and action that follow the predicate are only valid if the predicate is TRUE. The inverse (logical NOT) of a predicate is indicated by the prefix “~” (tilde character), the combination (logical AND) of two or more predicates is indicated by the symbol “&” (ampersand), and the choice of two or more predicates (logical OR) is indicated by the symbol “|” (vertical bar);

2) the new state that the CF enters after the action has been performed; and

3) the action, if any, that the CF performs. The possible actions are outlined in Table 2-14.

d) Blank cells indicate error conditions.

e) When an input event occurs and the state table indicates a state transition, the CF enters the new state after any associated action has been performed.

2.3.3.2.3 When interacting with embedded ASEs (ATN-App ASE or ACSE) and the specified action is to invoke an ASE request or response primitive, the following steps are taken:

a) the primitive invocation causes an input event to be generated for subsequent processing by the ASE;

b) the CF processing continues, and any CF state transition is performed before any action is taken by the ASE in response to the invoked primitive;

c) the ASE then behaves atomically, such that the input event is processed to completion by the ASE; and

d) the CF then responds to any resulting output events from the ASE before any other CF input events are processed.

2.3.3.2.4 The provision in 2.3.3.2.3 avoids the need to specify numerous transient states within the CF. It describes a model of the CF in order to achieve the required external behaviour. It does not imply any particular implementation architecture.

2.3.3.2.5 The following occurrences of input events, and combinations of input events and CF states shall be treated as error conditions:

a) the occurrence of an input event other than those listed in Table 2-13; or

b) a combination of an input event and a CF state that corresponds to a blank cell in Table 2-11; or

c) a combination of an input event and a CF state that corresponds to a cell in Table 2-11 containing one or more predicates, none of which evaluates to TRUE.

2.3.3.2.6 The error handling shall result in the association (if one exists) being aborted and a notification being given to the application-user.

2.3.3.2.7 In the event of a conflict between the actions implied by the state table and the textual statements made elsewhere in this document, the textual statements shall take precedence.

Table 2-11. ATN-App CF state table (see also Table 2-12)

State →	*STA0*	*STA1*	*STA2*	*STA3*	*STA4*
Event source	*Event*	*Null*	*Assoc. Pending*	*Data Transfer*	*Release Pending*	*Release Collision*

Event source	*State →* *Event*	*STA0* *Null*	*STA1* *Assoc. Pending*	*STA2* *Data Transfer*	*STA3* *Release Pending*	*STA4* *Release Collision*
From ATN-App	ATN-APP function req	STA0 ATN-App ASE req	STA1 ATN-App ASE req	STA2 ATN-App ASE req	STA3 ATN-App ASE req	STA4 ATN-App ASE req
	ATN-APP function rsp	STA0 ATN-App ASE rsp	STA1 ATN-App ASE rsp	STA2 ATN-App ASE rsp	STA3 ATN-App ASE rsp	STA4 ATN-App ASE rsp
From ATN-App ASE (upper)	ATN-APP function ind	STA0 ATN-App ind	STA1 ATN-App ind	STA2 ATN-App ind	STA3 ATN-App ind	STA4 ATN-App ind
	ATN-APP function cnf	STA0 ATN-App cnf	STA1 ATN-App cnf	STA2 ATN-App cnf	STA3 ATN-App cnf	STA4 ATN-App cnf
From ATN-App ASE (lower)	D-START req	p0 : STA1 A-ASSOC req				
From ATN-App ASE (lower)	D-START rsp+		~p1: STA1 A-ASSOC rsp+			
	D-START rsp-		~p1: STA1 A-ASSOC rsp-			
	D-DATA req			STA2 P-DATA req (user)	~p2: STA3 P-DATA req (user)	
	D-END req			STA3 A-RELEASE req		
	D-END rsp+				~p2: STA3 A-RELEASE rsp+	
	D-END rsp-				~p2: STA3 A-RELEASE rsp-	
	D-ABORT req		STA1 A-ABORT req	STA2 A-ABORT req	STA3 A-ABORT req	STA4 A-ABORT req
From ACSE (upper)	A-ASSOCIATE ind		STA1 D-START ind			
	A-ASSOCIATE cnf+		STA2 D-START cnf+			
	A-ASSOCIATE cnf-		STA0 D-START cnf-			
	A-RELEASE ind				STA3 D-END ind	p1: STA4 A-RELEASE rsp+ ~p1: STA4
	A-RELEASE cnf+				STA0 D-END cnf+ P-U-ABORT req	p1: STA0 D-END cnf+ P-U-ABORT req ~p1: STA4 D-END cnf+ A-RELEASE rsp+

Event source	*State →* *Event*	*STA0* *Null*	*STA1* *Assoc. Pending*	*STA2* *Data Transfer*	*STA3* *Release Pending*	*STA4* *Release Collision*
	A-RELEASE cnf-				STA2 D-END cnf-	
	A-ABORT ind		STA0 D-ABORT ind	STA0 D-ABORT ind	STA0 D-ABORT ind	STA0 D-ABORT ind
	A-P-ABORT ind		STA0 D-P-ABORT ind	STA0 D-P-ABORT ind	STA0 D-P-ABORT ind	STA0 D-P-ABORT ind
From ACSE (lower)	P-CONNECT req		STA1 P-CONN req			
	P-CONNECT rsp+		STA2 P-CONN rsp+			
	P-CONNECT rsp-		STA0 P-CONN rsp-			
	P-RELEASE req				STA3 P-DATA req (RLRQ)	
	P-RELEASE rsp+				STA0 P-DATA req (RLRE+)	p1: STA4 P-DATA req (RLRE+) ~p1: STA0 P-DATA req (RLRE+)
	P-RELEASE rsp-				STA2 P-DATA req (RLRE-)	
	P-U-ABORT req (data)	STA0 P-U-ABORT req	STA0 P-U-ABORT req	STA0 P-DATA req (ABRT)	STA0 P-U-ABORT req	STA0 P-U-ABORT req
	P-U-ABORT req (no data)		STA0 P-U-ABORT req	STA0 P-U-ABORT req	STA0 P-U-ABORT req	STA0 P-U-ABORT req
From supporting service	P-CONNECT ind	p0: STA1 P-CONN ind				
	P-CONNECT cnf+		STA1 P-CONN cnf+			
	P-CONNECT cnf-		STA1 P-CONN cnf-			
	P-DATA ind (RLRQ)	p3: STA0		STA3 P-RELEASE ind	p2: STA4 P-RELEASE ind	
	P-DATA ind (RLRE+)	p3: STA0			STA3 P-RELEASE cnf+	STA4 P-RELEASE cnf+
	P-DATA ind (RLRE-)	p3: STA0			STA3 P-RELEASE cnf-	
	P-DATA ind (ABRT)	p3: STA0 P-U-ABORT req ~p3: STA0		STA2 P-U-ABORT ind P-U-ABORT req	STA3 P-U-ABORT ind P-U-ABORT req	STA4 P-U-ABORT ind P-U-ABORT req

Event source	*State →* *Event*	*STA0* *Null*	*STA1* *Assoc. Pending*	*STA2* *Data Transfer*	*STA3* *Release Pending*	*STA4* *Release Collision*
	P-DATA ind (user)	p3: STA0		p4 | p5: STA2 SASO-deliver ~(p4 | p5): STA2 D-DATA ind	p2 & (p4 | p5): STA3 SASO-deliver p2 & ~(p4 | p5): STA3 D-DATA ind	
	P-U-ABORT ind	STA0	STA1 P-U-ABORT ind	STA2 P-U-ABORT ind	STA3 P-U-ABORT ind	STA4 P-U-ABORT ind
	P-P-ABORT ind	STA0	STA1 P-P-ABORT ind	STA2 P-P-ABORT ind	STA3 P-P-ABORT ind	STA4 P-P-ABORT ind

Table 2-12. Predicates used in Table 2-11

Predicate	*Meaning*
p0	This is a new instance of communication, i.e. no previous association exists (effectively, a new AE invocation is created).
p1	This CF is the initiator CF, i.e. the local DS-user issued a D-START request primitive.
~p1	This CF is the responder CF, i.e. the supporting service issued a P-CONNECT indication primitive.
p2	This CF is the release initiator, i.e. the local DS-user issued a D-END request primitive.
~p2	This CF is the release responder, i.e. the supporting service issued a P-DATA indication containing an RLRQ APDU.
p3	This CF is the “Abort+Data” initiator, i.e. the CF issued a P-DATA request containing an ABRT APDU, and it is awaiting disconnection by the peer.
~p3	This CF has not initiated an Abort containing user data.

Table 2-13. Incoming event list

Abbreviated name	*Source*	*Description*
ATN-APP function req	Upper AE service boundary	Application-specific request primitive issued by the application-user
ATN-APP function rsp		Application-specific response primitive issued by the application-user
ATN-APP function ind	ATN-App ASE (upper service boundary)	Application-specific indication primitive issued by the Application ASE
ATN-APP function cnf		Application-specific confirmation primitive issued by the application ASE
D-START req	ATN-App ASE (lower service boundary)	D-START request primitive issued by DS-user
D-START rsp+		D-START response primitive issued by DS-user, with Result = accepted
D-START rsp-		D-START response primitive issued by DS-user, with Result = rejected (transient) or rejected (permanent)
D-DATA req		D-DATA request primitive issued by DS-user
D-END req		D-END request primitive issued by DS-user
D-END rsp+		D-END response primitive issued by DS-user, with Result = accepted
D-END rsp-		D-END response primitive issued by DS-user, with Result = rejected
D-ABORT req		D-ABORT request primitive issued by DS-user
A-ASSOCIATE ind	ACSE (upper service boundary)	A-ASSOCIATE indication primitive issued by ACSE service
A-ASSOCIATE cnf+		A-ASSOCIATE confirmation primitive issued by ACSE service, with Result = accepted
A-ASSOCIATE cnf-		A-ASSOCIATE confirmation primitive issued by ACSE service, with Result = rejected (transient) or rejected (permanent)
A-RELEASE ind		A-RELEASE indication primitive issued by ACSE service
A-RELEASE cnf+		A-RELEASE confirmation primitive issued by ACSE service, with Result = affirmative
A-RELEASE cnf-		A-RELEASE confirmation primitive issued by ACSE service, with Result = negative
A-ABORT ind		A-ABORT indication primitive issued by ACSE service
A-P-ABORT ind		A-P-ABORT indication primitive issued by ACSE service
P-CONNECT req	ACSE (lower service boundary)	P-CONNECT request primitive issued by ACSE
P-CONNECT rsp+		P-CONNECT response primitive issued by ACSE, with Result = acceptance
P-CONNECT rsp-		P-CONNECT response primitive issued by ACSE, with Result = user-rejection or provider-rejection

Abbreviated name	*Source*	*Description*
P-RELEASE req		P-RELEASE request primitive issued by ACSE
P-RELEASE rsp+		P-RELEASE response primitive issued by ACSE, with Result = affirmative
P-RELEASE rsp-		P-RELEASE response primitive issued by ACSE, with Result = negative
P-U-ABORT req (data)		P-U-ABORT request primitive issued by ACSE, with the user data parameter present
P-U-ABORT req (no data)		P-U-ABORT request primitive issued by ACSE, with the user data parameter empty or absent
P-CONNECT ind	Supporting service	P-CONNECT indication primitive issued by presentation service provider
P-CONNECT cnf+		P-CONNECT confirmation primitive issued by presentation service provider, with Result = acceptance
P-CONNECT cnf-		P-CONNECT confirmation primitive issued by presentation service provider, with Result = user-rejection or provider-rejection
P-DATA ind (RLRQ)		P-DATA indication primitive issued by presentation service provider, with an RLRQ APDU as user data
P-DATA ind (RLRE+)		P-DATA indication primitive issued by presentation service provider, with an RLRE APDU as user data, with the reason field set to “normal”
P-DATA ind (RLRE-)		P-DATA indication primitive issued by presentation service provider, with an RLRE APDU as user data, with the reason field set to “not-finished”
P-DATA ind (ABRT)		P-DATA indication primitive issued by presentation service provider, with an ABRT APDU as user data
P-DATA ind (user)		P-DATA indication primitive issued by presentation service provider, with an ATN-APP APDU (e.g. an ADS-C-ASE protocol data unit) as user data
P-U-ABORT ind		P-U-ABORT indication primitive issued by presentation service provider
P-P-ABORT ind		P-P-ABORT indication primitive issued by presentation service provider

Table 2-14. Outgoing event list

Abbreviated name	*Target*	*Description*
ATN-App ind	Upper AE service boundary	Application-specific indication primitive mapped transparently from the upper service boundary of the ATN-App ASE
ATN-App cnf		Application-specific confirmation primitive mapped transparently from the upper service boundary of the ATN-App ASE
ATN-App ASE req	Upper ATN-App ASE service boundary	Application-specific request primitive mapped transparently from the upper AE service boundary
ATN-App ASE rsp		Application-specific response primitive mapped transparently from the upper AE service boundary
D-START ind	DS-user	D-START indication primitive issued
D-START cnf+		D-START confirmation primitive issued, with the Result parameter set to the abstract value “accepted”
D-START cnf-		D-START confirmation primitive issued, with the Result parameter set to the abstract value “rejected (transient)” or “rejected (permanent)”, according to the A-ASSOCIATE confirmation primitive that was received
D-DATA ind		D-DATA indication primitive issued
D-END ind		D-END indication primitive issued
D-END cnf+		D-END confirmation primitive issued, with the Result parameter set to the abstract value “accepted”
D-END cnf-		D-END confirmation primitive issued, with the Result parameter set to the abstract value “rejected”
D-ABORT ind		D-ABORT indication primitive issued
D-P-ABORT ind		D-P-ABORT indication primitive issued
A-ASSOC req	ACSE service provider	A-ASSOCIATE request primitive issued
A-ASSOC rsp+		A-ASSOCIATE response primitive issued, with Result = “accepted”
A-ASSOC rsp-		A-ASSOCIATE response primitive issued, with Result = “rejected (transient)” or “rejected (permanent)”, according to the D-START response primitive that was received
A-RELEASE req		A-RELEASE request primitive issued
A-RELEASE rsp+		A-RELEASE response primitive issued, with Result = “affirmative” and Reason = “normal”
A-RELEASE rsp-		A-RELEASE response primitive issued, with Result = “negative” and Reason = “not-finished”
A-ABORT req		A-ABORT request primitive issued
P-CONN ind	Lower ACSE service boundary	P-CONNECT indication primitive invoked

Abbreviated name	*Target*	*Description*
P-CONN cnf+		P-CONNECT confirmation primitive invoked, with the Result parameter set to “acceptance”
P-CONN cnf-		P-CONNECT confirmation primitive invoked, with the Result parameter set to “user-rejection”
P-RELEASE ind		P-RELEASE indication primitive invoked
P-RELEASE cnf+		P-RELEASE confirmation primitive invoked, with the Result parameter set to “affirmative”
P-RELEASE cnf-		P-RELEASE confirmation primitive invoked, with the Result parameter set to “negative”
P-U-ABORT ind		P-U-ABORT indication primitive invoked
P-P-ABORT ind		P-P-ABORT indication primitive invoked
P-CONN req	Supporting service	P-CONNECT request primitive issued
P-CONN rsp+		P-CONNECT response primitive issued, with the Result parameter set to “acceptance”
P-CONN rsp-		P-CONNECT response primitive issued, with the Result parameter set to “user-rejection”
P-DATA req (RLRQ)		P-DATA request primitive issued. The User Data parameter contains an RLRQ APDU.
P-DATA req (RLRE+)		P-DATA request primitive issued. The User Data parameter contains an RLRE APDU, with the reason field set to “normal”.
P-DATA req (RLRE-)		P-DATA request primitive issued. The User Data parameter contains an RLRE APDU, with the reason field set to “not-finished”.
P-DATA req (ABRT)		P-DATA request primitive issued. The User Data parameter contains an ABRT APDU.
P-DATA req (user)		P-DATA request primitive issued. The User Data parameter contains an ATN-App ASE APDU (e.g. an ADS-C-ASE protocol data unit).
P-U-ABORT req		P-U-ABORT request primitive issued

2.3.3.3 Services invoked by the application-user

2.3.3.3.1 Introduction

The actions that result from inputs generated by the user of this ATN-App AE are defined in 2.3.3.3.2.1 to 2.3.3.3.2.2. The service primitives available to the application-user are specific to the ATN application. This service is detailed in the individual application specifications.

2.3.3.3.2 Application-user request and response primitives

When invoked

2.3.3.3.2.1 Invocations of application-user request and response primitives by the application-user shall be allowed when the CF is in any valid state.

Action upon invocation

2.3.3.3.2.2 When the application-user request or response primitive is issued, the CF shall:

a) invoke the equivalent primitive of the ATN-App ASE service, with a one-to-one mapping of parameters; and

b) remain in its current state.

2.3.3.4 Services invoked by ATN-App ASE

2.3.3.4.1 ATN-App ASE indication and confirmation primitives

When invoked

2.3.3.4.1.1 Invocations of ATN-App ASE indication and confirmation primitives by the ATN-App ASE shall be allowed when the CF is in any valid state.

Action upon invocation

2.3.3.4.1.2 When the ATN-App ASE indication or confirmation primitive is issued, the CF shall:

a) invoke the equivalent primitive of the application-user service, with a one-to-one mapping of parameters; and

b) remain in its current state.

2.3.3.4.2 D-START request primitive

When invoked

2.3.3.4.2.1 When the D-START request primitive is invoked by the ATN-App ASE, a new instance of communication shall be created, with its CF initially in the NULL state.

Action upon invocation

2.3.3.4.2.2 When the D-START request is validly invoked with the *Security Requirements* parameter absent or set to the abstract value “no security”, the CF shall:

a) determine the app-type as defined for the ATN-App AE;

b) construct the application context name, with the value of the “version” arc set equal to the *DS-user Version Number* parameter if provided, and set to zero otherwise;

c) if not specified in the request primitive, retrieve the local Calling Presentation Address;

d) determine the Called Presentation Address via look-up from the *Called Peer ID* parameter;

e) if the *Calling Peer ID* parameter is present, then retrieve the corresponding Calling AP-title and Calling AE-Qualifier. If the *Calling Peer ID* is not present, then the Calling AP-title and the Calling AE-Qualifier are not used in the A-ASSOCIATE request (and they will not then be included in the resulting A-ASSOCIATE-REQUEST (AARQ) APDU). The way the Calling AP-title and the Calling AE-Qualifier are retrieved is a local implementation matter;

f) make no use of the A-ASSOCIATE parameter *ACSE Requirements*;

g) construct an A-ASSOCIATE request primitive with the parameter values as in Table 2-15;

h) invoke the A-ASSOCIATE request primitive; and

i) enter the ASSOCIATION PENDING state as an initiator CF.

Table 2-15. A-ASSOCIATE request parameter values

A-ASSOCIATE request parameter	*ISO status*	*ATN value*
Mode	U	Not used (default value)
Application Context Name	M	Derived as in 2.3.3.4.2.2 b)
Application Context Name List	C	Not used
Calling AP-title	U	Derived as in 2.3.3.4.2.2 e)
Calling AE-Qualifier	U	Derived as in 2.3.3.4.2.2 e)
Calling AP Invocation-identifier	U	Not used
Calling AE Invocation-identifier	U	Not used
Called AP-title	U	Not used
Called AE-Qualifier	U	Not used
Called AP Invocation-identifier	U	Not used
Called AE Invocation-identifier	U	Not used
ACSE Requirements	U	Make no use of the A-ASSOCIATE parameter *ACSE Requirements*
Authentication-mechanism-name	U	Not used
Authentication-value	U	Not used
User Information	U	D-START *User Data* parameter
Calling Presentation Address	M	Derived as in 2.3.3.4.2.2 c)
Called Presentation Address	M	Derived as in 2.3.3.4.2.2 d)
Presentation Context Definition List	U	Not used
Default Presentation Context Name	U	Not used

A-ASSOCIATE request parameter	*ISO status*	*ATN value*
Quality of Service	M	See 2.3.3.4.2.5 to 2.3.3.4.2.18
Presentation Requirements	U	Not used (default value)
Session Requirements	M	No orderly release (NOR), duplex
Initial Synchronization Point Serial No.	C	Not used
Initial Assignment of Tokens	C	Not used
Session-connection Identifier	U	Not used

QOS parameter mappings

2.3.3.4.2.3 Paragraphs 2.3.3.4.2.4 to 2.3.3.4.2.16 specify how the QOS parameters in the D-START request and response primitives are conveyed to the ATN Internet.

2.3.3.4.2.4 The Routing Class component of the *QOS* parameter in the D-START request and response primitives shall be conveyed to the ATN Internet and mapped to the ATN security label by local means, using the values for Security Tag Value as specified in the ATN ICS technical provisions.

2.3.3.4.2.5 The mechanism by which the connection initiator provides the appropriate ATN security label is a local matter. For example, it may be identified by an extension to the transport service interface, be implicit in the choice of a given TSAP, or be identified using a systems management function.

2.3.3.4.2.6 If no value for *Routing Class* is specified in the D-START request primitive, then a default value shall be assigned as follows:

a) If the ATN-App AE is one of the ATS applications specified in Parts I or II of this manual, the value corresponding to “ATSC: no traffic type policy preference” is assigned.

b) If the ATN-App AE is not one of the ATS applications specified in Parts I or II of this manual, the traffic type defaults to “general communications”, and no security tag value is conveyed.

2.3.3.4.2.7 The Routing Class value conveyed to the ATN ICS when the D-START response primitive is invoked shall be the same as that which was passed to the DS-user in the D-START indication primitive.

2.3.3.4.2.8 The Priority component of the *QOS* parameter in the D-START request and response primitives shall be provided to the TS-provider, by implementation-specific means, using the values for “Transport Layer Priority” specified in the ATN Priority Table.

2.3.3.4.2.9 Although transport priority and network priority are semantically independent of each other, the ATN ICS requires that the TS-user specify the application service priority, which in turn is mapped into the resulting connectionless network protocol (CLNP) PDUs according to the ATN Priority Table, which defines the fixed relationship between transport priority and the network priority.

2.3.3.4.2.10 If no value for Priority is specified in the D-START request primitive, then the value corresponding to “network/systems administration” shall be used.

2.3.3.4.2.11 The Priority value conveyed when the D-START response primitive is invoked shall be the same as that which was passed to the DS-user in the D-START indication primitive.

2.3.3.4.2.12 If the Routing Class parameter has an ATSC value, then the RER component of the A-ASSOCIATE *QOS* parameter shall be set to the logical value that maps to the lowest RER (highest integrity) supported by the transport service.

2.3.3.4.2.13 The A-ASSOCIATE RER is mapped to the T-CONNECT RER parameter, the use of which is specified in the ATN ICS technical provisions.

2.3.3.4.2.14 If the Routing Class parameter has a non-ATSC value, then the RER component of the *QOS* parameter in the D-START request primitive shall map to the RER component of the A-ASSOCIATE *QOS* parameter.

2.3.3.4.2.15 The RER value in the D-START response primitive shall be taken to be the same as that which was passed to the DS-user in the D-START indication primitive.

2.3.3.4.2.16 The RER is present in the D-START response for backward compatibility with the previous version of the DS. It is not used in the current version.

2.3.3.4.3 D-START response primitive

When invoked

2.3.3.4.3.1 The D-START response primitive may be validly invoked by the ATN-App ASE when the CF is the responder CF (see 2.3.3.6.2.2) and is in the ASSOCIATION PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.4.3.2 When a D-START response primitive is validly invoked, the CF shall:

a) construct the application context name, with the value of the “version” arc set equal to the *DS-User Version Number* parameter if provided, and set to zero otherwise;

b) retrieve the responding Presentation Address;

c) make no use of the A-ASSOCIATE parameter “ACSE Requirements”;

d) construct an A-ASSOCIATE response primitive with the parameter values as in Table 2-16;

e) invoke the A-ASSOCIATE response; and

f) remain in the same state.

Table 2-16

A-ASSOCIATE response parameter	*ISO status*	*ATN value*
Application Context Name	M	Derived as in 2.3.3.4.3.2 a)
Application Context Name List	C	Not used

A-ASSOCIATE response parameter	*ISO status*	*ATN value*
Responding AP-title	U	Not used
Responding AE-Qualifier	U	Not used
Responding AP Invocation-identifier	U	Not used
Responding AE Invocation-identifier	U	Not used
ACSE Requirements	C	Derived as in 2.3.3.4.3.2 c)
Authentication-mechanism-name	U	Not used
Authentication-value	U	Not used
User Information	U	D-START User Data parameter
Result	M	D-START Result parameter
Diagnostic	U	Not used
Responding Presentation Address	M	Derived as in 2.3.3.4.3.2 b)
Presentation Context Definition Result List	C	Not used
Default Presentation Context Result	C	Not used
Quality of Service	M	As for D-START request (see 2.3.3.4.2.3 to 2.3.3.4.2.16)
Presentation Requirements	U	Not used (default value)
Session Requirements	M	No orderly release (NOR), duplex
Initial Synchronization Point Serial No.	C	Not used
Initial Assignment of Tokens	C	Not used
Session-connection Identifier	U	Not used

2.3.3.4.4 D-END request primitive

When invoked

2.3.3.4.4.1 The D-END request primitive may be validly invoked by the ATN-App ASE when the CF is in the DATA TRANSFER state; if it is in any other state, then appropriate error-recovery action shall be taken. For example, if the CF is in the RELEASE PENDING state, then the D-END request is rejected locally, with an appropriate result code.

Action upon invocation

2.3.3.4.4.2 When a D-END request primitive is validly invoked, the CF shall:

a) construct an A-RELEASE request primitive with the parameter values as in Table 2-17;

b) invoke the A-RELEASE request primitive; and

c) enter the RELEASE PENDING state as the release initiator CF.

Table 2-17

A-RELEASE request parameter	*ISO status*	*ATN value*
Reason	U	“Normal”
User Information	U	D-END *User Data* parameter

2.3.3.4.5 D-END response primitive

When invoked

2.3.3.4.5.1 The D-END response primitive may be validly invoked by the ATN-App ASE when the CF is the release responder CF and is in the RELEASE PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.4.5.2 When a D-END response primitive is validly invoked and the *Result* parameter has the value “accepted”, the CF shall:

a) construct an A-RELEASE response primitive with the parameter values as in Table 2-18;

b) invoke the A-RELEASE response primitive; and

c) remain in the RELEASE PENDING state.

Table 2-18

A-RELEASE response parameter	*ISO status*	*ATN value*
Reason	U	“Normal”
User Information	U	D-END *User Data* parameter
Result	M	“Affirmative”

2.3.3.4.5.3 When a D-END response primitive is validly invoked on a dialogue and the *Result* parameter has the abstract value “rejected”, the CF shall:

a) construct an A-RELEASE response primitive with the parameter values as in Table 2-19;

b) invoke the A-RELEASE response primitive; and

c) remain in the RELEASE PENDING state.

Table 2-19

A-RELEASE response parameter	*ISO status*	*ATN value*
Reason	U	“Not finished”
User Information	U	D-END *User Data* parameter
Result	M	“Negative”

2.3.3.4.6 D-DATA request primitive

When invoked

2.3.3.4.6.1 The D-DATA request primitive may be validly invoked by the ATN-App ASE when the CF is in the DATA TRANSFER state, or (if it is the release responder) in the RELEASE PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.4.6.2 When a D-DATA request primitive is validly invoked, the CF shall:

a) using the definition of presentation user data in 2.3.2.6, encode the D-DATA request *User Data* parameter with the presentation-context-identifier value corresponding to “user-ase-apdu”;

b) invoke a P-DATA request primitive with the resulting encoding as User Data; and

c) remain in the same state.

2.3.3.4.7 D-ABORT request primitive

When invoked

2.3.3.4.7.1 Invocations of the D-ABORT request primitive by the ATN-App ASE shall be allowed when the CF is in any valid state except the NULL state; if an invocation occurs when the CF is in the NULL state, then an error has occurred (see 2.3.3.2.6).

Action upon invocation

2.3.3.4.7.2 When a D-ABORT request primitive is validly invoked, and the CF is in DATA TRANSFER state, the CF shall:

a) if the *Originator* parameter of the D-ABORT has the symbolic value “user”, then set Diagnostic to “no reason given”. If the *Originator* parameter is absent or has any symbolic value other than “user”, then set Diagnostic to “protocol error”;

b) construct an A-ABORT request primitive with the parameter values as in Table 2-20;

c) invoke the A-ABORT request primitive; and

d) remain in the same state.

Table 2-20

A-ABORT request parameter	*ISO status*	*ATN value*
Diagnostic	U	Derived as in 2.3.3.4.7.2 a)
User Information	U	D-ABORT User Data parameter, if present and not empty.

2.3.3.4.7.3 When a D-ABORT request primitive is validly invoked and the CF is in the ASSOCIATION PENDING, RELEASE PENDING, or RELEASE COLLISION state, the CF shall invoke an A-ABORT request primitive with no parameters and remain in the same state.

2.3.3.5 ACSE services delivered to the CF

2.3.3.5.1 Introduction

Events that occur at the upper service boundary of ACSE, i.e. indication and confirmation primitives which are generated by ACSE and which require handling by the CF, are defined in the following paragraphs of section 2.3.3.5.

2.3.3.5.2 A-ASSOCIATE indication primitive

When invoked

2.3.3.5.2.1 The A-ASSOCIATE indication primitive may be validly invoked by ACSE when the CF is in the ASSOCIATION PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.2.2 When an A-ASSOCIATE indication primitive is validly invoked with the *ACSE Requirements* parameter not present, the CF shall:

a) if the “version” component of the *Application Context Name* parameter is non-zero, then use it as the *DS-user Version Number* in the D-START indication primitive. If it has the value zero, then omit the *DS-user Version Number* parameter in the D-START indication;

b) if the *Calling AP-title* parameter is present, extract the Calling Peer ID from it;

c) construct a D-START indication primitive with the parameter values as in Table 2-21;

d) invoke the D-START indication primitive; and

e) remain in the ASSOCIATION PENDING state.

Table 2-21

D-START indication parameter	*Value*
Calling Peer ID	Derived as in 2.3.3.5.2.2 b)
DS-user Version Number	Derived as in 2.3.3.5.2.2 a)
Security Requirements	"No security"
Quality of Service	See 2.3.3.5.2.3 to 2.3.3.5.2.6
User Data	A-ASSOCIATE *User Information* parameter

QOS parameter mappings

2.3.3.5.2.3 Paragraphs 2.3.3.5.2.4 to 2.3.3.5.2.6 specify how the *QOS* parameters in the A-ASSOCIATE indication and confirmation primitives are conveyed to the DS-user as parameters of the D-START indication and confirmation primitives.

2.3.3.5.2.4 The Routing Class component of the *QOS* parameter in the D-START indication and confirmation primitives shall be obtained from the ATN Internet by local means, using the abstract values for Security Tag Values as specified in the ATN ICS technical provisions.

2.3.3.5.2.5 The Priority component of the *QOS* parameter in the D-START indication and confirmation primitives shall be taken from information provided by the TS-provider, by implementation-specific means, using the abstract values for "Transport Layer Priority" specified in the ATN Priority Table.

2.3.3.5.2.6 The RER component of the *QOS* parameter in the D-START indication and confirmation primitives shall be derived from the RER component of the A-ASSOCIATE *QOS* parameter as follows:

a) For ATSC applications: if the A-ASSOCIATE value equates to the highest available integrity level (as a minimum, the standard 16-bit transport checksum is required to be used), then set the RER to logical value "low"; otherwise set it to "high".

b) For non-ATSC applications: the RER is mapped directly from the A-ASSOCIATE value.

2.3.3.5.3 A-ASSOCIATE confirmation primitive

When invoked

2.3.3.5.3.1 The A-ASSOCIATE confirmation primitive may be validly invoked by ACSE when the CF is in the ASSOCIATION PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.3.2 When an A-ASSOCIATE confirmation primitive is validly invoked, and the *ACSE Requirements* parameter is absent, and the *Result* parameter has the abstract value "accepted", the CF shall:

a) if the "version" component of the *Application Context Name* parameter is non-zero, then use it as the *DS-user Version Number* in the D-START confirmation primitive. If it has the value zero, then omit the

DS-user Version Number parameter in the D-START confirmation;

b) construct a D-START confirmation primitive with the parameter values as in Table 2-22;

c) invoke the D-START confirmation primitive; and

d) enter the DATA TRANSFER state as the initiator CF.

Table 2-22

D-START confirmation parameter	*Value*
DS-user Version Number	Derived as in 2.3.3.5.3.2 a)
Security Requirements	"No security"
Quality of Service	As for A-ASSOCIATE indication (see 2.3.3.5.2.3 to 2.3.3.5.2.6)
Result	"Accepted"
Reject Source	Not used
User Data	A-ASSOCIATE *User Information* parameter

2.3.3.5.3.3 When an A-ASSOCIATE confirmation primitive is validly invoked and the *ACSE Requirements* parameter is absent, and the *Result* parameter has the abstract value "rejected (permanent)" or "rejected (transient)", and the *Application Context Name* parameter conforms to the specification in 2.3.2.5, and the *Responding Presentation Address* parameter is consistent with the *Called Presentation Address* that was used in the A-ASSOCIATE request primitive, the CF shall:

a) if the "version" component of the *Application Context Name* parameter is non-zero, then use it as the *DS-user Version Number* in the D-START confirmation primitive. If it has the value zero, then omit the *DS-user Version Number* parameter in the D-START confirmation primitive;

b) if the A-ASSOCIATE confirmation *Result Source* parameter has the abstract value "ACSE service-user", form a *Reject Source* parameter with the value "DS-user". If the A-ASSOCIATE confirmation *Result Source* parameter has the abstract value "ACSE service provider" or "presentation service provider", form a *Reject Source* parameter with the value "DS-provider";

c) construct a D-START confirmation primitive with the parameter values as in Table 2-23;

d) invoke the D-START confirmation primitive;

e) enter the NULL state.

Table 2-23

D-START confirmation parameter	*Value*
DS-user Version Number	Derived as in 2.3.3.5.3.3 a)

D-START confirmation parameter	*Value*
Security Requirements	"No security"
Quality of Service	As for A-ASSOCIATE indication (see 2.3.3.5.2.3 to 2.3.3.5.2.6)
Result	"Rejected (permanent)" or "rejected (transient)", from the A-ASSOCIATE *Result* parameter
Reject Source	Derived as in 2.3.3.5.3.3 b)
User Data	A-ASSOCIATE *User Information* parameter

QOS parameter mappings

2.3.3.5.3.4 Paragraphs 2.3.3.5.2.4 to 2.3.3.5.2.6 specify how the QOS parameters in A-ASSOCIATE indication and confirmation primitives are conveyed to the DS-user as parameters of the D-START indication and confirmation primitives.

2.3.3.5.4 A-RELEASE indication primitive

When invoked

2.3.3.5.4.1 The A-RELEASE indication primitive may be validly invoked by ACSE when the CF is in the RELEASE PENDING or the RELEASE COLLISION state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.4.2 When an A-RELEASE indication primitive is validly invoked, and the CF is in the RELEASE PENDING state, the CF shall:

a) construct a D-END indication primitive, with the *User Data* parameter set equal to the value of the *User Information* parameter of the A-RELEASE indication primitive;

b) invoke the D-END indication; and

c) remain in the RELEASE PENDING state.

2.3.3.5.4.3 When an A-RELEASE indication primitive is validly invoked, and the CF is the initiator CF and is in the RELEASE COLLISION state, the CF shall:

a) construct a D-END confirmation primitive, with the *User Data* parameter set equal to the value of the *User Information* parameter of the A-RELEASE indication primitive, if present. The D-END confirmation is not issued to the DS-user until the orderly release procedure is complete and an A-RELEASE confirmation is received;

b) construct an A-RELEASE response primitive with the parameter values as in Table 2-24;

c) invoke the A-RELEASE response primitive; and

d) remain in the RELEASE COLLISION state.

Table 2-24

A-RELEASE response parameter	*ISO status*	*ATN value*
Reason	U	“Normal”
User Information	U	Not present
Result	M	“Affirmative”

2.3.3.5.4.4 When an A-RELEASE indication primitive is validly invoked, and the CF is in the RELEASE COLLISION state, and it is the responder CF, the CF shall:

a) construct a D-END confirmation primitive, with the *User Data* parameter set equal to the value of the *User Information* parameter of the A-RELEASE indication primitive, if present. The D-END confirmation is not issued to the DS-user until the orderly release procedure is complete and an A-RELEASE confirmation is received; and

b) remain in the RELEASE COLLISION state.

2.3.3.5.5 A-RELEASE confirmation primitive

When invoked

2.3.3.5.5.1 The A-RELEASE confirmation primitive may be invoked by ACSE when the CF is in the RELEASE PENDING or RELEASE COLLISION state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.5.2 When an A-RELEASE confirmation primitive is validly invoked, and the CF is in the RELEASE PENDING state, and the *Result* parameter has the abstract value “affirmative”, the CF shall:

a) construct a D-END confirmation primitive with the parameter values as in Table 2-25;

b) invoke the D-END confirmation primitive;

c) issue a P-U-ABORT request primitive with no parameters (this will cause the release of the underlying transport connection); and

d) enter the NULL state.

Table 3-25

D-END confirmation parameter	*Value*
Result	"Affirmative"
User Data	*User Information* parameter from the A-RELEASE confirmation, if present

2.3.3.5.5.3 When an A-RELEASE confirmation primitive is validly invoked, and the CF is in the RELEASE PENDING state, and the *Result* parameter has the abstract value "negative", the CF shall:

a) construct a D-END confirmation primitive with the parameter values as in Table 2-26;

b) invoke the D-END confirmation primitive; and

c) enter the DATA TRANSFER state.

Table 2-26

D-END confirmation parameter	*Value*
Result	"Rejected"
User Data	*User Information* parameter from the A-RELEASE confirmation, if present

2.3.3.5.5.4 When an A-RELEASE confirmation primitive is validly invoked on a dialogue, and the *Result* parameter has the abstract value "affirmative", and the CF is the initiator CF and is in the RELEASE COLLISION state, the CF shall:

a) issue the D-END confirmation primitive, which was previously formed in response to the reception of an A-RELEASE indication primitive, to the DS-user;

b) issue a P-U-ABORT request primitive with no parameters (this will cause the release of the underlying transport connection); and

c) enter the NULL state.

2.3.3.5.5.5 When an A-RELEASE confirmation primitive is validly invoked, and the *Result* parameter has the abstract value "affirmative", and the CF is the responder CF and is in the RELEASE COLLISION state, the CF shall:

a) issue the D-END confirmation primitive, which was previously formed in response to the reception of an A-RELEASE indication primitive, to the DS-user;

b) construct an A-RELEASE response primitive, with the *Result* parameter set to “affirmative”;

c) invoke the A-RELEASE response; and

d) remain in the RELEASE COLLISION state.

2.3.3.5.6 A-ABORT indication primitive

When invoked

2.3.3.5.6.1 Invocations of the A-ABORT indication primitive by ACSE shall be allowed when the CF is in any valid state except the NULL state; if an invocation occurs when the CF is in the NULL state, then an error has occurred (see 2.3.3.2.6).

Action upon invocation

2.3.3.5.6.2 When an A-ABORT indication primitive is validly invoked, the CF shall:

a) if the *Abort Source* parameter of the A-ABORT indication is set to “ACSE service-user”, and the *Diagnostic* parameter is set to “no reason given”, issue a D-ABORT indication primitive to the DS-user, with the *Originator* parameter set to “user”, and the *User Data* parameter set equal to the *User Information* parameter in the A-ABORT indication, if present;

b) if the *Abort Source* parameter of the A-ABORT indication is set to “ACSE service-user”, and the *Diagnostic* parameter is absent or is set to any value other than “no reason given”, then issue a D-ABORT indication primitive to the DS-user, with the *Originator* parameter set to “provider”, and the *User Data* parameter set equal to the *User Information* parameter in the A-ABORT indication, if present;

c) if the *Abort Source* parameter of the A-ABORT indication has the abstract value “ACSE service provider”, then issue a D-ABORT indication primitive to the DS-user, with the *Originator* parameter set to the abstract value “provider”, and the *User Data* parameter set equal to the *User Information* parameter in the A-ABORT indication, if present; and

d) enter the NULL state.

2.3.3.5.7 A-P-ABORT indication primitive

When invoked

2.3.3.5.7.1 Invocations of the A-P-ABORT indication primitive by ACSE shall be allowed when the CF is in any valid state, except the NULL state; if an invocation occurs when the CF is in the NULL state, then an error has occurred (see 2.3.3.2.6).

Action upon invocation

2.3.3.5.7.2 When an A-P-ABORT indication primitive is validly invoked, the CF shall:

a) issue a D-P-ABORT indication primitive to the DS-user, and discard any *Provider Reason* parameter in the A-P-ABORT indication; and

b) enter the NULL state.

Services used by ACSE

2.3.3.5.7.3 ACSE, edition 2 (contained in ITU-T Rec. X.227), mandates the mapping of ACSE APDUs to the underlying presentation service provider. However, when the efficient encoding options of session and presentation protocols are used, the full presentation service is no longer available. Therefore, invocations of presentation service primitives by ACSE are “intercepted” by the CF and re-mapped to the “actual” presentation service as appropriate.

2.3.3.5.8 P-CONNECT request primitive

When invoked

2.3.3.5.8.1 The P-CONNECT request primitive may be validly invoked by ACSE when the CF is in the ASSOCIATION PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.8.2 When a P-CONNECT request primitive is validly invoked, the CF shall transparently invoke the equivalent presentation service primitive and remain in the same state.

2.3.3.5.9 P-CONNECT response primitive

When invoked

2.3.3.5.9.1 The P-CONNECT response primitive may be validly invoked by ACSE when the CF is in the ASSOCIATION PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.9.2 When the P-CONNECT response primitive is validly invoked, the CF shall:

a) transparently invoke the equivalent presentation service primitive; and

b) if the P-CONNECT response *Result* parameter has the abstract value “acceptance”, then enter the DATA TRANSFER state, otherwise enter the NULL state.

2.3.3.5.10 P-U-ABORT request primitive

When invoked

2.3.3.5.10.1 Invocations of the P-U-ABORT request primitive by ACSE shall be allowed when the CF is in any valid state.

Action upon invocation

2.3.3.5.10.2 When a P-U-ABORT request primitive is validly invoked, the CF shall:

a) if the P-U-ABORT request *User Data* parameter is present, and the CF is in the DATA TRANSFER state:

1) encode the presentation user data as indicated in 2.3.2.6 with the P-U-ABORT *User Data* parameter (an ABRT APDU) as the presentation data value, and presentation context identifier value corresponding to “acse-apdu”; and

2) invoke a P-DATA request primitive with the resulting encoding as *User Data*.

Otherwise, invoke a P-U-ABORT request primitive with no parameters (this will cause the underlying transport connection to be disconnected); and

b) enter the NULL state.

2.3.3.5.11 P-RELEASE request primitive

Introduction

2.3.3.5.11.1 ACSE, edition 2 (contained in ITU-T Rec. X.227), mandates the mapping of A-RELEASE APDUs (RLRQ and RLRE) to the P-RELEASE service. However, when the efficient encoding options of session and presentation protocols are used, the session no orderly release (NOR) functional unit is selected and no mapping for the P-RELEASE service is available. In order to provide an orderly release service, the CF re-maps invocations of the P-RELEASE service at the lower service boundary of ACSE to invocations of the P-DATA service, with the release APDUs transferred as user information.

When invoked

2.3.3.5.11.2 The P-RELEASE request primitive may be validly invoked by ACSE when the CF is in the RELEASE PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.11.3 When a P-RELEASE request primitive is validly invoked, the CF shall:

a) encode the presentation user data as indicated in 2.3.2.6 with the P-RELEASE *User Data* parameter (an RLRQ APDU) as the presentation data value, and presentation context identifier corresponding to “acse-apdu”;

b) invoke a P-DATA request primitive with the resulting encoding as *User Data*; and

c) remain in the RELEASE PENDING state.

2.3.3.5.12 P-RELEASE response primitive

When invoked

2.3.3.5.12.1 The P-RELEASE response primitive may be validly invoked by ACSE when the CF is in the RELEASE PENDING or RELEASE COLLISION state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.5.12.2 When a P-RELEASE response primitive is validly invoked, and the CF is in the RELEASE PENDING state, and the *Result* parameter has the abstract value “affirmative”, the CF shall:

a) encode the presentation user data as indicated in 2.3.2 with the P-RELEASE *User Data* parameter (an RLRE APDU) as the presentation data value, and presentation context identifier corresponding to “acse-apdu”;

b) invoke a P-DATA request primitive with the resulting encoding as *User Data*; and

c) enter the NULL state.

The peer AEI is now expected to issue a P-U-ABORT request, which will cause the release of the underlying connection.

2.3.3.5.12.3 When a P-RELEASE response primitive is validly invoked, and the CF is in the RELEASE PENDING state, and the *Result* parameter has the abstract value “negative”, the CF shall:

a) encode the presentation user data as indicated in 2.3.2 with the P-RELEASE *User Data* parameter (an RLRE APDU) as the presentation data value, and presentation context identifier corresponding to “acse-apdu”;

b) invoke a P-DATA request primitive with the resulting encoding as *User Data*; and

c) enter the DATA TRANSFER state.

2.3.3.5.12.4 When a P-RELEASE response primitive is validly invoked, and the CF is the initiator CF and is in the RELEASE COLLISION state, the CF shall:

a) encode the presentation user data as indicated in 2.3.2 with the P-RELEASE *User Data* parameter (an RLRE APDU) as the presentation data value, and presentation context identifier corresponding to “acse-apdu”;

b) invoke a P-DATA request primitive with the resulting encoding as *User Data*; and

c) remain in the RELEASE COLLISION state.

2.3.3.5.12.5 When a P-RELEASE response primitive is validly invoked, and the CF is the responder CF and is in the RELEASE COLLISION state, the CF shall:

a) encode the presentation user data as indicated in 2.3.2 with the P-RELEASE *User Data* parameter (an RLRE APDU) as the presentation data value, and presentation context identifier corresponding to “acse-apdu”;

b) invoke a P-DATA request primitive with the resulting encoding as *User Data*; and

c) enter the NULL state.

The peer AEI is now expected to issue a P-U-ABORT request, which will cause the release of the underlying connection.

2.3.3.5.12.6 After entering the NULL state, implementations should release the underlying connection (e.g. by issuing the P-U-ABORT request) if the communication peer does not cause the connection to be released as expected (i.e. after a period of time not less than twice the anticipated end-to-end transit time).

2.3.3.6 Supporting services delivered to the CF

2.3.3.6.1 Introduction

2.3.3.6.1.1 The mapping by the CF of presentation service indication and confirmation primitives, which are invoked by the presentation service provider, is defined in 2.3.3.6.

2.3.3.6.1.2 The provisions in 2.3.3.6 describe the behaviour to be exhibited by the ATN-App AE when the supporting communications service exhibits behaviour modelled by the passing of indication or confirmation primitives to the application layer.

2.3.3.6.2 P-CONNECT indication primitive

When invoked

2.3.3.6.2.1 When the P-CONNECT indication primitive is invoked by the supporting service, a new instance of communication shall be created, with its CF initially in the NULL state.

Action upon invocation

2.3.3.6.2.2 When a P-CONNECT indication primitive is validly invoked, the CF shall:

a) transparently invoke the equivalent presentation service primitive at the lower ACSE service boundary; and

b) enter the ASSOCIATION PENDING state as the responder CF.

2.3.3.6.3 P-CONNECT confirmation primitive

When invoked

2.3.3.6.3.1 The P-CONNECT confirmation primitive may be validly invoked by the supporting service when the CF is in the ASSOCIATION PENDING state; if it is in any other state, then appropriate error-recovery action shall be taken.

Action upon invocation

2.3.3.6.3.2 When a P-CONNECT confirmation primitive is validly invoked, the CF shall:

a) transparently invoke the equivalent presentation service primitive at the lower ACSE service boundary; and

b) remain in the ASSOCIATION PENDING state.

2.3.3.6.4 P-U-ABORT indication primitive

When invoked

2.3.3.6.4.1 Invocations of the P-U-ABORT indication primitive by the supporting service shall be allowed when the CF is in any valid state.

Action upon invocation

2.3.3.6.4.2 When a P-U-ABORT indication primitive is validly invoked, the CF shall:

a) if the CF is in the NULL state, take no action; or
b) if the CF is not in the NULL state, transparently invoke the equivalent presentation service primitive at the lower ACSE service boundary, and remain in the same state.

2.3.3.6.5 P-P-ABORT indication primitive
When invoked

2.3.3.6.5.1 Invocations of the P-P-ABORT indication primitive by the supporting service shall be allowed when the CF is in any valid state.
Action upon invocation

2.3.3.6.5.2 When a P-P-ABORT indication primitive is validly invoked, the CF shall:

a) if the CF is in the NULL state, take no action; or

b) if the CF is not in the NULL state, transparently invoke the corresponding presentation service primitive at the lower ACSE service boundary, and remain in the same state.

2.3.3.6.6 P-DATA indication primitive
When invoked

2.3.3.6.6.1 Invocations of the P-DATA indication primitive by the supporting service shall be allowed when the CF is in a valid state to receive the decoded APDU, as listed in 2.3.3.6.6.2 to 2.3.3.6.6.3; if an invocation occurs when the CF is not in a valid state, then an error has occurred (see 2.3.3.2.6).
Action upon invocation

2.3.3.6.6.2 When a P-DATA indication primitive is validly invoked, the CF shall decode the presentation user data as indicated in 2.3.2.6 to determine the destination ASE of the APDU, and extract the presentation data value.

2.3.3.6.6.3 The destination ASE is determined from the value of the presentation-context-identifier in the received user-data. Valid values are acse-apdu and user-ase-apdu, which correspond to destination ASEs of ACSE and ATN-App ASE, respectively.

ACSE APDU received

2.3.3.6.6.4 If the destination ASE is ACSE, then the CF shall determine the type of ACSE APDU present in the extracted presentation data value. ACSE APDUs that may validly be received in a P-DATA indication are A-Release-

Request (RLRQ), A-Release-Response (RLRE), and A-Abort (ABRT) APDUs.

2.3.3.6.6.5 If the received APDU is RLRQ, the CF shall:

a) if in the DATA TRANSFER state, then invoke a P-RELEASE indication primitive at the ACSE lower service boundary, with the RLRQ as *User Data*, and enter the RELEASE PENDING state as the release responder CF;
b) if in the RELEASE PENDING state, and the CF is the release initiator, then invoke a P-RELEASE indication primitive at the ACSE lower service boundary, with the RLRQ as *User Data*, and enter the RELEASE COLLISION state;

c) if in the NULL state, and this CF has previously issued an ABRT APDU and is awaiting disconnection by the peer, then take no action and remain in the NULL state; and

d) if none of the conditions a) to c) is satisfied, then take error-handling action as described in 2.3.3.6.6.9.

2.3.3.6.6.6 If the received APDU is RLRE, the CF shall:

a) if the Reason field in the RLRE has the value “not-finished”, and the CF is in the RELEASE PENDING state, then invoke a P-RELEASE confirmation primitive at the ACSE lower service boundary, with the *result* parameter set to “negative”, and the RLRE as *User Data*; and remain in the RELEASE PENDING state;

b) if the Reason field in the RLRE has the value “normal”, and the CF is in the RELEASE PENDING or RELEASE COLLISION state, then invoke a P-RELEASE confirmation primitive at the ACSE lower service boundary, with the *result* parameter set to “affirmative”, and the RLRE as *User Data*; and remain in the same state;

c) if the CF is in the NULL state, and this CF has previously issued an ABRT APDU and is awaiting disconnection by the peer, then take no action and remain in the NULL state; and

d) if none of the conditions a) to c) is satisfied, then take error-handling action in 2.3.3.6.6.9.

2.3.3.6.6.7 If the received APDU is ABRT, the CF shall:

a) if the CF is in the state DATA TRANSFER, or RELEASE PENDING, or RELEASE COLLISION, then invoke a P-U-ABORT indication primitive at the ACSE lower service boundary, with the ABRT as *User Data*, and issue a P-U-ABORT request with no parameters to the underlying service; and remain in the same state;

b) if the CF is in the NULL state, then take no action unless this CF has previously issued an ABRT APDU and is awaiting disconnection by the peer, in which case issue a P-U-ABORT request to the underlying service; and remain in the same state; and

c) if neither of the conditions a) nor b) is satisfied, then take error-handling action as described in 2.3.3.6.6.9.

ATN-App APDU received

2.3.3.6.6.8 If the destination ASE is ATN-App ASE, then the CF shall:

a) if the CF is in the DATA TRANSFER state, or the CF is in the RELEASE PENDING state and is the

release initiator CF, then issue a D-DATA indication primitive to the DS-user, with the received presentation data value as the *User Data* parameter, and remain in the same state;

b) if the CF is in the NULL state, and this CF has previously issued an ABRT APDU and is awaiting disconnection by the peer, then take no action and remain in the same state; and

c) if neither of the conditions a) nor b) is satisfied, then take error-handling action as described in 2.3.3.6.6.9.

Error conditions

2.3.3.6.6.9 If the destination ASE is invalid (i.e. neither ACSE nor ATN-App ASE), or an unrecognized APDU is received, or a valid APDU is received when the CF is not in the correct state (as defined in 2.3.3.6.6.4 to 2.3.3.6.6.8), then the CF shall:

a) if not in the NULL state, then issue a P-U-ABORT request with no parameters to the supporting service; and

b) regardless of the CF state, behave as if a P-U-ABORT indication had been received.

2.4 SESSION LAYER REQUIREMENTS

Note.— The session layer requirements are described in many cases by means of completed protocol implementation conformance statement (PICS) pro forma tables. In such tables, the "Ref." column contains a reference to the relevant section in the session layer PICS pro forma, ISO/IEC 8327-2 | ITU-T Rec. X.245 (1995).

2.4.1 Protocol versions implemented

Session protocol versions shall be supported as specified in Table 2-27.

Table 2-27. Session protocol versions supported

Ref.	*Version*	*ISO status*	*ATN support*
S.A.3/1	Version 1	O.1	-
S.A.3/2	Version 2	O.1	M

O.1: The ISO PICS requires that the implementation of one, and only one, version of the protocol is described.

2.4.2 Session functional units

2.4.2.1 Session functional units (S-FUs) shall be selected as specified in Table 2-28.

Table 2-28. Selection of session functional units

Ref.	*Functional unit*	*ISO status*	*ATN support*
S.A.6.1/1	Kernel	M	M
S.A.6.1/2	Negotiated release	O	X
S.A.6.1/3	Half duplex (HD)	O.2	X
S.A.6.1/4	Duplex	O.2	M
S.A.6.1/5	Expedited data (EX)	O	X
S.A.6.1/6	Typed data	O	X
S.A.6.1/7	Capability data exchange	C1	X
S.A.6.1/8	Minor synchronize (SY)	O	X
S.A.6.1/9	Symmetric synchronize (SS)	O	X
S.A.6.1/10	Data separation	C2	X
S.A.6.1/11	Major synchronize	O	X
S.A.6.1/12	Resynchronize	O	X
S.A.6.1/13	Exceptions	C3	X
S.A.6.1/14	Activity management (ACT)	O	X
2.4.2.1.1	No orderly release (NOR)	O	M
2.4.2.1.1	Special user-data	O	X

O.2: The ISO standard requires at least one of the functional units duplex and half duplex to be implemented.
C1: If [S-FU(ACT)], then O else N/A.
C2: If [S-FU(SY) or S-FU(SS)], then O else N/A.
C3: If [S-FU(HD)], then O else N/A.

2.4.2.1.1 The no orderly release (NOR) and special user-data S-FUs were added by amendment to the base standard to enable efficiency enhancements to the session protocol; they were not included in the earlier standard PICS.

2.4.3 Protocol mechanisms

2.4.3.1 Session protocol mechanisms shall be supported as specified in Table 2-29.

Table 2-29. Session protocol mechanisms supported

Ref.	*Mechanism*	*ISO status*	*ATN support*	*Associated mnemonic*
S.A.6.2/1	Use of transport expedited data (extended control QOS)	C4	X	S-EXP_T
S.A.6.2/2	Reuse of transport connection	O	O	S-REUSE_T

Ref.	*Mechanism*	*ISO status*	*ATN support*	*Associated mnemonic*
S.A.6.2/3	Basic concatenation	M	M (see 2.4.3.1.2)	
S.A.6.2/4	Extended concatenation (sending)	O	X	
S.A.6.2/5	Extended concatenation (receiving)	O	X	S-XCONC_RCV
S.A.6.2/6	Segmenting (sending)	O	X	S-SEG_SDR
S.A.6.2/7	Segmenting (receiving)	O	X	S-SEG_RCV
S.A.6.2/8	Maximum size of SS-user-data (S-CONNECT) > 512	O	O	S-MAXSIZE_512
S.A.6.2/9	Maximum size of SS-user-data (S-CONNECT) > 10240	O	O	S-MAXSIZE_10240
S.A.6.2/10	Maximum size of SS-user-data (S-ABORT) > 9	O	X	S-MAXSIZE_9
2.4.3.1.1	Null-encoding protocol option	-	M	
2.4.3.1.1	Short-connect protocol option	-	M	
2.4.3.1.1	Short-encoding protocol option	-	X	

C4: If [S-FU(EX)], then M else O.

2.4.3.1.1 The null-encoding, short-connect and short-encoding protocol options were added by amendment to the base standard to enable efficiency enhancements to the session protocol; they were not included in the earlier standard PICS.

2.4.3.1.2 Only Category 1 session protocol data units (SPDUs) are used for this ATN profile. By definition, these are never concatenated. Therefore, basic concatenation is not applicable to this specification, but it is supported to the extent necessary for compliance with the ISO PICS.

2.4.3.2 The session protocol shall implement the efficiency enhancements in ISO/IEC 8327-1:1996/Amdt 1:1997 | ITU-T Rec. X.225 (1995)/Amdt 1 (1997) as specified, together with all approved amendments and defect report resolutions.

2.4.3.3 If the null-encoding protocol option is offered by the initiating session protocol machine (SPM), the responding SPM shall select only the kernel, full-duplex and no orderly release functional units for use on this connection.

2.4.3.4 The SPDUs associated with the short-connect protocol option (i.e. short connect (SCN), short accept (SAC), short accept continue (SACC), short refuse (SRF) and short refuse continue (SRFC)) shall be transferred as user data on the transport layer T-CONNECT primitives, where possible. (This is only possible if the complete SPDUs, including any user data, meet any size restrictions of the T-CONNECT user-data.)

2.4.4 Supported roles

2.4.4.1 Session connection

2.4.4.1.1 The roles for session connection shall be supported as specified in Table 2-30.

Table 2-30. Session connection roles supported

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
S.A.7.1.1.1/1	Connection initiator	O.3	M	S-CON_initiator
S.A.7.1.1.1/2	Connection responder	O.3	M	S-CON_responder

O.3: The ISO standard requires a conforming implementation to support at least one of these roles as required by the implementation.

2.4.4.1.2 When a connection establishment request is accepted, the SHORT-CPA presentation protocol data unit (PPDU) in the SS-User-data of the positive S-CONNECT response/confirmation primitive shall map to the *User Data* parameter of an SAC SPDU.

2.4.4.1.3 When a connection establishment request is refused, the SHORT-CPR PPDU in the SS-User-data of the negative S-CONNECT response/confirmation primitive shall map to the *UserData* parameter of an SRF SPDU.

2.4.4.2 Orderly release

The roles for session orderly release shall be supported as specified in Table 2-31.

Table 2-31. Session orderly release roles supported

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
S.A.7.1.1.2/1	Requestor	O.4	N/A (See Note)	S-REL_requestor
S.A.7.1.1.2/2	Acceptor	O.4	N/A (See Note)	S-REL_acceptor

O.4: The ISO standard requires a conforming implementation to support at least one of these roles as part of the kernel functional unit. However, selection of the no orderly release functional unit removes this requirement.

Note.— Not applicable, as the no orderly release functional unit is selected. For ATN applications, orderly release is provided by the CF as described in 2.3.

2.4.4.3 Normal data transfer

The roles for session normal data transfer shall be supported as specified in Table 2-32.

Table 2-32. Session normal data transfer roles supported

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
S.A.7.1.1.3/1	Requestor	O.5	M	S-DATA_requestor
S.A.7.1.1.3/2	Acceptor	O.5	M	S-DATA_acceptor

O.5: The ISO standard requires a conforming implementation to support at least one of these roles.

2.4.5 Supported SPDUs

2.4.5.1 Introduction

This section specifies the SPDUs associated with the supported session functional units. There are no additional SPDUs associated with the duplex functional unit or with the no orderly release functional unit.

2.4.5.2 Support for the SPDUs associated with the kernel functional unit

2.4.5.2.1 Support for SPDUs shall be as specified in Table 2-33.

Table 2-33. Supported SPDUs

Ref.	*SPDU*	*Sender*		*Receiver*		*Mnemonics*
		ISO status	*ATN support*	*ISO status*	*ATN support*	
S.A.7.1.2/1	Connect (CN)	C5	N/A (Note 2)	C6	N/A (Note 2)	
S.A.7.1.2/2	Overflow Accept (OA)	C7	N/A (Note 2)	C8	N/A (Note 2)	S-OA_SDR / S-OA_RCV
S.A.7.1.2/3	Connect Data Overflow (CDO)	C9	N/A (Note 2)	C10	N/A (Note 2)	S-CDO_SDR / S-CDO_RCV
S.A.7.1.2/4	Accept (AC)	C6	N/A (Note 2)	C5	N/A (Note 2)	
S.A.7.1.2/5	Refuse (RF)	C6	N/A (Note 2)	C5	N/A (Note 2)	
S.A.7.1.2/6	Finish (FN)	C11	N/A (Note 3)	C12	N/A (Note 3)	
S.A.7.1.2/7	Disconnect (DN)	C12	N/A (Note 3)	C11	N/A (Note 3)	
S.A.7.1.2/8	Abort	M	N/A (Note 4)	M	N/A (Note 4)	
S.A.7.1.2/9	Abort Accept (AA)	O	N/A (Note 4)	M	N/A (Note 4)	
S.A.7.1.2/10	Data Transfer (DT)	C13	N/A (Note 4)	C14	N/A (Note 4)	
S.A.7.1.2/11	Prepare (PR)	C15	X	C15	X	S-PR_SDR / S-PR_RCV
Note 1	Short Connect (SCN)	C17	M	C17	M	
Note 1	Short Accept (SAC)	C17	M	C17	M	
Note 1	Short Refuse (SRF)	C17	M	C17	M	
Note 1	Null (NL)	C18	M	C18	M	
Note 1	Short Connect Continue (SCNC)	C16	N/A	C16	N/A	
Note 1	Short Accept Continue (SACC)	C17	M	C17	M	
Note 1	Short Refuse Continue (SRFC)	C17	M	C17	M	
Note 1	Short Finish (SFN)	C16	N/A	C16	N/A	
Note 1	Short Disconnect (SDN)	C16	N/A	C16	N/A	

Ref.	*SPDU*	*Sender*		*Receiver*		*Mnemonics*
		ISO status	*ATN support*	*ISO status*	*ATN support*	
Note 1	Short Data Transfer (SDT)	C16	N/A	C16	N/A	
Note 1	Short Abort (SAB)	C16	N/A	C16	N/A	

C5: If [S-CON_initiator], then M else N/A.

C6: If [S-CON_responder], then M else N/A.

C7: If [S-V1 or (NOT S-CON_responder)], then N/A else if [S-MAXSIZE_10240], then M else O.

C8: If [NOT S-V1 and S-CON_responder and S-MAXSIZE_10240], then M else N/A.

C9: If [S-V1 or (NOT S-CON_initiator)], then N/A else if [S-MAXSIZE_10240] ,then M else O.

C10: If [NOT S-V1 and S-CON_initiator and S-MAXSIZE_10240], then M else N/A.

C11: If [S-REL_requestor], then M else N/A.

C12: If [S-REL_acceptor], then M else N/A.

C13: If [S-DATA_requestor], then M else N/A.

C14: If [S-DATA_acceptor], then M else N/A.

C15: If [NOT S-V1 and S-MAXSIZE_9 and S-EXP_T], then M else N/A.

C16: Used only if the short-encoding protocol option is selected.

C17: Used if short-encoding or null-encoding is used.

C18: Used only if the null-encoding protocol option is supported.

Notes:

1.— These PDUs were added by amendment to the base standard to enable efficiency enhancements to the session protocol; they were not included in the earlier standard PICS.

2.— Not applicable, as the short-connect protocol option is selected.

3.— Not applicable, as the no orderly release functional unit is selected.

4.— Not applicable, as the null-encoding protocol option is selected.

2.4.5.2.2 The SCN, SAC, SRF, SACC and SRFC SPDUs shall be encoded such that the parameter bit of the “SI&P” octet is set to the value 0, indicating that all following octets are User Information (i.e. no SPDU parameters are present). (This is a requirement of the null-encoding protocol option.)

2.4.5.3 Support for the SPDUs associated with token exchange

2.4.5.3.1 Support for SPDUs associated with token exchange shall be as specified in Table 2-34.

Table 2-34. SPDUs associated with token exchange

		Sender		*Receiver*	
Ref.	*SPDU*	*ISO status*	*ATN support*	*ISO status*	*ATN support*
S.A.7.1.3/1	Give tokens (GT)	M	(See Note)	M	(See Note)
S.A.7.1.3/2	Please tokens (PT)	M	(See Note)	M	(See Note)

Note.— Not applicable, as the null-encoding protocol option is selected.

2.4.5.3.2 The ISO PICS states that the two SPDUs “give tokens” and “please tokens” are used for token exchange, but they are also used as category 0 SPDUs in basic concatenation. Therefore, their implementation is mandatory even if no token is supported (reference ISO/IEC 8327-1 | ITU-T Rec. X.225, Clauses 7.16 and 7.17). However, if the null-encoding protocol option is selected, their encoding will be null, i.e. not present.

2.4.6 Use of null-encoding and short-connect session protocol options

The null-encoding and short-connect session protocol options shall be selected for use, with the requirements as specified in Table 2-35.

Table 2-35. Use of the null-encoding and short-connect session protocol options

Ref.	*Requirement*	*Base status*	*ATN requirement*
a	The calling and called session selectors are null.	C1	M
b	The session requirements parameter in the S-CONNECT service includes the kernel, full-duplex and no orderly release functional units only.	C1	M

C1: The SPMs may use the short-connect protocol option to establish a session connection using the null-encoding option. The null-encoding protocol option is available for use on an established connection only if the conditions a and b in Table 2-35 are both true.

2.4.7 Mapping to the ATN Internet transport service

2.4.7.1 The use of the connection-oriented transport service provided by the ATN Internet shall be as specified in Clause 6 of ISO/IEC 8327-1 | ITU-T Rec. X.225 (1995), except as stated in this section.

2.4.7.2 The called and calling TSAP address shall be provided to the TS-provider on a per transport connection basis, using the called and calling PSAP addresses as provided to ACSE in the A-ASSOCIATE request, with null presentation and session selectors.

2.4.7.3 The TS-user shall indicate in all T-CONNECT requests that the transport expedited flow is not required.

2.4.7.4 Information on the use of the transport checksum shall be conveyed between the TS-user and TS-provider via the RER component of the T-CONNECT QOS parameter.

2.4.7.4.1 The ATN ICS technical provisions specify the use by the TS-user of the required RER parameter. This affects the degree of integrity checking of all data sent over the underlying transport connection.

2.4.7.4.2 In the ATN, the QOS provided to applications is otherwise maintained using capacity-planning techniques that are outside of the scope of this specification. Network administrators are responsible for designing and implementing a network that will meet the QOS requirements of the CNS/ATM applications that use it.

2.4.7.5 The use of the transport checksum shall be specified on a per transport connection basis, based on TS-user requests in the T-CONNECT request primitive.

2.4.7.6 The application service priority shall be provided to the TS-provider on a per transport connection basis, by implementation-specific means, and using the values for “transport layer priority” specified in the ATN Priority Table.

2.4.7.6.1 Although transport priority and network priority are semantically independent of each other, it is required (in the ATN ICS technical provisions) that the TS-user specify the application service priority, which in turn is mapped into the resulting CLNP PDUs according to the ATN Priority Table, which defines the fixed relationship between transport priority and the network priority.

2.4.7.7 The ATN security label shall be provided to the TS-provider on a per transport connection basis.

2.4.7.8 The ATN security label value shall be encoded according to the ATN ICS technical provisions, and passed between TS-user and TS-provider by implementation-specific means.

2.4.7.9 The QOS parameter “Routing Class” shall be conveyed as the security tag field of the security tag set for Traffic Type and Associated Routing Policies within the ATN security label.

2.4.7.9.1 According to the ICS technical provisions, the mechanism by which the [transport] connection initiator provides the appropriate ATN security label is a local matter. For example, it may be identified by an extension to the transport service interface, be implicit in the choice of a given TSAP, or be identified using a systems management function.

2.4.7.9.2 The ATN ICS technical provisions specify the syntax of the ATN security label field that must be used by the TS-user. The encoding of the ATN security label field is summarized in Table 2-36. The D-START QOS parameter “Routing Class” maps to the field labelled “Traffic type & category”.

2.4.7.10 No transport service QOS parameters other than those specified in the preceding subsections shall be specified when establishing a transport connection.

Table 2-36. Encoding of the ATN security label field

ATN security label field	*Value (Hex)*	*Length (Octets)*
Security registration ID length	6	1
Security registration ID = OID {1.3.27.0.0}	06, 04, 2B, 1B, 00, 00	6
Security information length	4	1
Security information:		
Tag set name length	1	1
Tag set name = “Traffic type & associated routing policies”	0F	1
Tag Set Length	1	1
Security tag value = Traffic type & category (from ATN ICS technical provisions)	01 (for example)	1
		Total: 12 Octets

2.5 PRESENTATION LAYER REQUIREMENTS

Note.— The presentation layer requirements are described in many cases by means of completed PICS pro forma tables. In such tables, the “Ref.” column contains a reference to the relevant section in the presentation layer PICS pro forma ISO/IEC 8823-2 | ITU-T Rec. X.246 (1996).

2.5.1 Protocol mechanisms

2.5.1.1 The presentation protocol mechanisms supported shall be as specified in Table 2-37.

Table 2-37. Presentation protocol mechanisms supported

Ref.	*Protocol mechanism*	*ISO status*	*ATN support*	*Mnemonic*
P.A.6.1/2	Normal mode	O.1	M	
P.A.6.1/1	X.410-1984 mode	O.1	X	
See Note	Nominated context	O	N/A	
See Note	Short encoding	O	N/A	
See Note	Packed Encoding Rules	O	N/A	
2.5.1.1.1	Short-connect	O	M	
2.5.1.1.1	Null-encoding	O	M	

O.1: The ISO standard requires that either normal mode or X.410 (1984) mode or both be supported.

Note.— Optional protocol mechanisms defined in efficiency enhancement amendment.

2.5.1.1.1 The short-connect and null-encoding optional protocol mechanisms were added by amendment to the

base standard to enable efficiency enhancements to the presentation protocol; they were not included in the earlier standard PICS.

2.5.1.1.2 The presentation protocol shall implement the efficiency enhancements in ISO/IEC 8823-1: 1994/Amdt 1: 1997 | ITU-T Rec. X.226 (1994)/Amdt 1 (1997) as specified, together with all approved amendments and defect report resolutions.

2.5.2 Use of null-encoding and short-connect presentation protocol options

The null-encoding and short-connect presentation protocol options shall be selected for use, with the requirements as specified in Table 2-38.

Table 2-38. Use of the null-encoding and short-connect presentation protocol options

Ref.	*Requirement*	*Base status*	*ATN requirement*
a	The presentation context definition list contains precisely one item in which the abstract syntax is known to the responding presentation protocol machine (PPM) by bilateral agreement.	C1	N/A
b	The presentation context definition list is empty, and the default context is known by bilateral agreement.	C1	M
c	The presentation context definition list is empty, and the abstract syntax of the default context is known to the responding PPM by bilateral agreement and is specified in ASN.1.	C1	M
d	The calling and called presentation selectors are null.	C2	M
e	The presentation-requirements parameter in the P-CONNECT service includes the kernel functional unit only.	C2	M

C1: The null-encoding protocol option is available for use on an established connection only if at least one of the conditions a, b and c in Table 2-38 is true.

C2: The short-connect protocol option is used only in connection establishment to establish a connection on which the null-encoding option will be used; it can only be used if both of the conditions d and e in Table 2-38 are true.

2.5.3 Mapping of presentation primitives to the null-encoding option

2.5.3.1 When the null-encoding presentation protocol option is selected, no presentation protocol control information is present once the connection has been established. Thus, no presentation PDUs are supported. The presentation connection is only terminated by the termination of the supporting session and transport connections.

2.5.3.2 The user of the presentation service shall not issue any presentation primitives other than P-CONNECT request, P-CONNECT response, P-DATA request and P-U-ABORT request.

2.5.3.3 When it is required to release the presentation connection, the presentation service user shall issue a

P-U-ABORT request.

2.5.3.4 Any user data in a P-U-ABORT request shall be ignored by the presentation service provider.

2.5.4 Presentation functional units

2.5.4.1 The presentation functional units selected shall be as specified in Table 2-39.

Table 2-39. Selection of presentation functional units

Ref.	*Presentation functional unit*	*ISO status*	*ATN support*	*Mnemonic*
P.A.6.2/1	Kernel	M	M	
P.A.6.2/2	Presentation context management	O	X	P-FU(CM)
P.A.6.2/3	Presentation context restoration	C1	X	P-FU(CR)

C1: If presentation context management (2) is supported, then O else N/A.

2.5.4.2 The presentation pass-through functional units selected shall be as specified in Table 2-40.

Table 2-40. Selection of presentation pass-through functional units

Ref.	*Pass-through to session functional units*	*ISO status*	*ATN support*	*Mnemonic*
P.A.6.2/4	Negotiated release	O	X	S-FU(NR)
P.A.6.2/5	Half duplex	O.2	X	S-FU(HD)
P.A.6.2/6	Duplex	O.2	M	S-FU(FD)
P.A.6.2/7	Expedited data	O	X	S-FU(EX)
P.A.6.2/8	Typed data	O	X	S-FU(TD)
P.A.6.2/9	Capability data exchange	C1	X	S-FU(CD)
P.A.6.2/10	Minor synchronize	O	X	S-FU(SY)
P.A.6.2/11	Symmetric synchronize	O	X	S-FU(SS)
P.A.6.2/12	Data separation	O	X	S-FU(DS)
P.A.6.2/13	Major synchronize	O	X	S-FU(MA)
P.A.6.2/14	Resynchronize	O	X	S-FU(RESYNC)
P.A.6.2/15	Exceptions	C2	X	S-FU(EXCEP)
P.A.6.2/16	Activity management	O	X	S-FU(ACT)
2.5.4.2.1	No orderly release (NOR)	-	M	S-FU(NOR)

O.2: The ISO standard requires that pass-through for at least one of the session functional units duplex and half

duplex be supported.

C1: If [S-FU(ACT), then O else N/A.

C2: If [S-FU(HD), then O else N/A.

2.5.4.2.1 The NOR session functional unit is defined in the ISO session service efficiency enhancement amendment.

2.5.5 Elements of procedure

2.5.5.1 Supported roles

2.5.5.1.1 Presentation connection

2.5.5.1.1.1 The supported roles for establishing presentation connections shall be as specified in Table 2-41.

Table 2-41. Presentation connection roles

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
P.A.7.1.1.1/1	Initiator	O.3	M	P-CON_initiator
P.A.7.1.1.1/2	Responder	O.3	M	P-CON_responder

O.3: The ISO standard requires a conforming implementation to support at least one of these roles.

2.5.5.1.1.2 When a connection establishment request is accepted, the AARE (accepted) in the user data of the positive P-CONNECT response/confirmation primitive shall map to the User Data parameter of a SHORT-CPA PPDU.

2.5.5.1.1.3 When a connection establishment request is refused, the AARE (rejected) in the user data of the negative P-CONNECT response/confirmation primitive shall map to the User Data parameter of a SHORT-CPR PPDU.

2.5.5.1.2 Orderly release

The supported roles for the orderly release of presentation connections shall be as specified in Table 2-42.

Table 2-42. Presentation connection orderly release roles

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
P.A.7.1.1.3/1	Requestor	O	N/A	P-REL_requestor
P.A.7.1.1.3/2	Acceptor	O	N/A	P-REL_acceptor

2.5.5.1.3 Normal data

The supported roles for normal data shall be as specified in Table 2-43.

Table 2-43. Presentation normal data roles

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
P.A.7.1.1.2/1	Requestor	O	M	P-DATA_requestor
P.A.7.1.1.2/2	Acceptor	O	M	P-DATA_acceptor

2.5.6 Supported presentation protocol data units (PPDUs)

2.5.6.1 Introduction

This section specifies the PPDUs associated with the supported presentation functional units. There are no additional PPDUs nor is there any additional pass-through functionality associated with the supported session functional units.

2.5.6.2 Supported PPDUs associated with the kernel services

2.5.6.2.1 The PPDUs supported shall be as specified in Table 2-44.

Table 2-44. Supported PPDUs

		Sender		*Receiver*		
Ref.	*PPDU*	*ISO status*	*ATN support*	*ISO status*	*ATN support*	*Mnemonics*
P.A.7.1.2/1	Connect presentation (CP)	C3	N/A (2.5.6.2.1.2)	C4	N/A (2.5.6.2.1.2)	
P.A.7.1.2/2	Connect presentation accept (CPA)	C4	N/A (2.5.6.2.1.2)	C3	N/A (2.5.6.2.1.2)	S-OA_SDR / S-OA_RCV
P.A.7.1.2/3	Connect presentation reject (CPR)	C4	N/A (2.5.6.2.1.2)	C3	N/A (2.5.6.2.1.2)	S-CDO_SDR / S-CDO_RCV
P.A.7.1.2/4	Abnormal release provider (ARP)	M	N/A (2.5.6.2.1.2)	M	N/A (2.5.6.2.1.2)	
P.A.7.1.2/5	Abnormal release user (ARU)	O	N/A (2.5.6.2.1.2)	M	N/A (2.5.6.2.1.2)	
P.A.7.1.2/6	Presentation Data (TD)	C5	N/A (2.5.6.2.1.2)	C6	N/A (2.5.6.2.1.2)	
2.5.6.2.1.1	Short Connect (SHORT-CP)	O	M	O	M	

Ref.	*PPDU*	*Sender*		*Receiver*		*Mnemonics*
		ISO status	*ATN support*	*ISO status*	*ATN support*	
2.5.6.2.1.1	Short Connect Accept (SHORT-CPA)	O	M	O	M	
2.5.6.2.1.1	Short Connect Reject (SHORT-CPR)	O	M	O	M	

C3: If [P-CON_initiator], then M else N/A.

C4: If [P-CON_responder], then M else N/A.

C5: If [P-DATA_requestor], then M else N/A.

C6: If [P-DATA_acceptor], then M else N/A.

2.5.6.2.1.1 The SHORT-CP, SHORT-CPA and SHORT-CPR PDUs were defined in the efficiency enhancement amendment and were not in the original standard PICS.

2.5.6.2.1.2 PPDUs marked “N/A” in Table 2-44 are not applicable, as the short-connect and null-encoding protocol options are selected.

2.5.6.3 Structure and encoding of PPDUs

The SHORT-CP, SHORT-CPA and SHORT-CPR PPDUs shall have the encoding-choice bit-field set to “unaligned PER”.

2.6 ACSE SPECIFICATION

Note.— The ACSE requirements are described in many cases by means of completed PICS pro forma tables. In such tables, the “Ref.” column contains a reference to the relevant section in the ACSE PICS pro forma ISO/IEC 8650-2 | ITU-T Rec. X.247 (1996). In the tables, “M” indicates a feature that must be implemented, “O” indicates an optional feature, and “X” indicates a feature that must not be implemented.

2.6.1 Protocol details

The specification of the ACSE protocol supported shall be as defined in Table 2-45.

Table 2-45. Identification of ACSE protocol specification

Identification of protocol specification	*ATN support*	*Comments*
ISO/IEC 8650-1: 1996/Amdt 1:1997	ITU-T Rec. X.227 (1995)/Amdt 1 (1996)	M	See Note.

Note.— This is the second edition of the ACSE protocol specification.

2.6.2 Protocol versions

The version of the ACSE protocol supported shall be as specified in Table 2-46.

Table 2-46. Identification of ACSE protocol version

Ref.	*Version*	*ISO status*	*ATN support*	*Mnemonic*
A.A.4.2/1	Version 1	O.1	M	A-V1
A.A.4.2/2	Version 2	O.1		

O.1: The ISO PICS requires support of the implementation of only one version of the protocol to be described.

2.6.3 Supported roles

2.6.3.1 Association establishment

2.6.3.1.1 The supported roles for association establishment shall be as specified in Table 2-47.

Table 2-47. ACSE roles for association establishment

Ref.	*Capability*	*ISO status*	*ATN support*	*Mnemonic*
A.A.6.1/1	Association initiator	O.2	See 2.6.3.1.2	A-CON_initiator
A.A.6.1/2	Association responder	O.2	See 2.6.3.1.2	A-CON_responder

O.2: The ISO standard requires a conforming implementation to support at least one of the roles.

2.6.3.1.2 Either one or both of the ACSE roles “association initiator” or “association responder” shall be supported.

2.6.3.2 Normal release procedure

2.6.3.2.1 The supported roles for the normal release procedure shall be as specified in Table 2-48.

Table 2-48. ACSE roles for normal release

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
A.A.6.2/1	Initiator	O	See 2.6.3.2.2	A-REL_requestor
A.A.6.2/2	Responder	O	See 2.6.3.2.2	A-REL_acceptor

2.6.3.2.2 Either one or both of the ACSE normal release roles “initiator” or “responder” shall be supported.

2.6.3.2.3 The ACSE release responder shall be allowed to give a negative response, despite the fact that the session negotiated release functional unit is not selected for the association.

2.6.3.2.3.1 Provision 2.6.3.2.3 waives the ISO/IEC 8649 Ed. 2 (1996) | ITU-T Rec. X.217 (1995) requirement that the responder may give a negative response only if session negotiated release is selected. This is possible because, for ATN, the ACSE release PDUs do not map directly to the presentation release service; they are re-mapped by the CF to P-DATA.

2.6.3.3 Abnormal release procedure

The supported roles for the abnormal release procedure shall be as specified in Table 2-49.

Table 2-49. ACSE roles for abnormal release

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
A.A.6.3/1	Initiator	M	M	
A.A.6.3/2	Responder	M	M	

2.6.4 Protocol mechanisms

2.6.4.1 General

The ACSE protocol mechanisms supported shall be as specified in Table 2-50.

Table 2-50. ACSE protocol mechanisms supported

Ref.	*Protocol mechanism*	*ISO status*	*ATN support*	*Mnemonic*
A.A.7/1	Normal mode	O.4	M	
A.A.7/2	X.410-1984 mode	O.4	X	
A.A.7/2	Rules for extensibility	M	M	
A.A.7/4	Supports operation of session version 2	O	M	S-O-SESS-V2

O.4: The ISO standard requires that either normal mode or X.410-1984 mode, or both of these modes, be supported.

2.6.4.2 Extensibility and encoding

2.6.4.2.1 For the purposes of this specification, the abstract syntax module defined in Clause 9 of the ACSE protocol specification shall be augmented with the ASN.1 extensibility notation as specified in ISO/IEC 8650-1: 1996/Amdt 1: 1997 | ITU-T Rec. X.227 (1995)/Amdt 1 (1996).

2.6.4.2.2 The system shall support that encoding which results from applying the ASN.1 PER (basic, unaligned variant), as specified in ISO/IEC 8825-2 | ITU-T Rec. X.691 (1995), to the abstract syntax module specified in 2.6.4.2.1.

2.6.4.2.3 Packed encoding (basic, unaligned) shall be used for encoding all ACSE protocol control information for interchange.

2.6.4.2.4 When embedded in fully-encoded-data at the presentation service boundary, encoded ACSE APDUs are treated as bit-oriented values that are not padded to an integral number of octets; the length determinant includes only the significant bits of the encoding, corresponding to the ASN.1 type.

2.6.5 ACSE functional units

The ACSE functional units selected shall be as specified in Table 2-51.

Table 2-51. Selection of ACSE functional units

Ref.	*Role*	*ISO status*	*ATN support*	*Mnemonic*
A.A.8/1	Normal mode	M	M	
A.A.8/2	Authentication	O	C1	A-FU(AU)

C1: If the DS-user requires the use of the *Security Requirements* parameter of the D-START primitives, then M, else O.

2.6.6 Supported APDUs

2.6.6.1 General

The ACSE protocol data units supported shall be as specified in Table 2-52.

Table 2-52. Supported ACSE protocol data units

		Sender		*Receiver*		
Ref.	*APDU*	*ISO status*	*ATN support*	*ISO status*	*ATN support*	*Comment*
A.A.9/1	AARQ	C1	M	C2	M	
A.A.9/2	AARE	C2	M	C1	M	
A.A.9/3	RLRQ	C3	M	C4	M	
A.A.9/4	RLRE	C4	M	C3	M	
A.A.9/5	ABRT	C5	M	C5	M	

C1: If [A-CON_initiator], then M else N/A.
C2: If [A-CON_responder], then M else N/A.
C3: If [A-REL_requestor], then M else N/A.
C4: If [A-REL_acceptor], then M else N/A.
C5: If [S-O-SESS-V2], then M else N/A.

2.6.6.2 Supported APDU parameters

2.6.6.2.1 A-Associate-request (AARQ)

2.6.6.2.1.1 The parameters in the AARQ APDU shall be supported as specified in Table 2-53.

Table 2-53. Supported AARQ parameters

		Sender		*Receiver*	
Ref.	*Parameter*	*ISO status*	*ATN support*	*ISO status*	*ATN support*
A.A.10.1/1	Protocol Version	C6	X	C2	M
A.A.10.1/2	Application Context Name	C1	M	C2	M
A.A.10.1/3	Calling AP-title	C6	M	C2	M
A.A.10.1/4	Calling AE-Qualifier	C6	M	C2	M
A.A.10.1/5	Calling AP Invocation-identifier	C6	X	C2	M
A.A.10.1/6	Calling AE Invocation-identifier	C6	X	C2	M
A.A.10.1/7	Called AP-title	C6	X	C2	M
A.A.10.1/8	Called AE-Qualifier	C6	X	C2	M
A.A.10.1/9	Called AP Invocation-identifier	C6	X	C2	See 2.6.6.2.1.5
A.A.10.1/10	Called AE Invocation-identifier	C6	X	C2	See 2.6.6.2.1.5
A.A.10.1/11	ACSE-requirements	C8	See 2.6.6.2.1.2	C9	M
A.A.10.1/12	Authentication-mechanism-name	C8	See 2.6.6.2.1.2	C9	M
A.A.10.1/13	Authentication-value	C8	See 2.6.6.2.1.2	C9	M
A.A.10.1/14	Implementation Information	C6	X	C7	O
A.A.10.1/15	User Information	C6	M	C7	M

C1: If [A-CON_initiator], then M else N/A.
C2: If [A-CON_responder], then M else N/A.
C6: If [A-CON_initiator], then O else N/A.
C7: If [A-CON_responder], then O else N/A.
C8: If [A-CON_initiator and A-FU(AU)], then M else N/A.
C9: If [A-CON_responder and A-FU(AU)], then M else N/A.

2.6.6.2.1.2 The AARQ parameters “ACSE-requirements”, “authentication-mechanism-name” and “authentication-value” shall be supported for sending only if the connection initiator role (A-CON_initiator) and the authentication functional unit (A-FU(AU)) are supported.

2.6.6.2.1.3 The AARQ parameters “ACSE-requirements”, “authentication-mechanism-name” and “authentication-value” shall be supported for receiving if the connection responder role (A-CON_responder) is supported, but they are ignored if the authentication functional unit (A-FU(AU)) is not supported by the responder.

2.6.6.2.1.4 The ATN specification is non-conformant to the ISO PICS pro forma in that “ACSE-requirements”, “authentication-mechanism-name” and “authentication-value” are “M” for receiving, even if the authentication functional unit is not supported.

2.6.6.2.1.5 The AARQ parameters “Called AP invocation-identifier” and “Called AE invocation-identifier” shall be supported for receiving if the association responder role is supported.

2.6.6.2.2 A-Associate-response (AARE)

2.6.6.2.2.1 The parameters in the AARE APDU shall be supported as specified in Table 2-54.

Table 2-54. Supported AARE parameters

		Sender		*Receiver*	
Ref.	*Parameter*	*ISO status*	*ATN support*	*ISO status*	*ATN support*
A.A.10.2/1	Protocol Version	C7	X	C1	M
A.A.10.2/2	Application Context Name	C2	M	C1	M
A.A.10.2/3	Responding AP-title	C7	X	C1	M
A.A.10.2/4	Responding AE-Qualifier	C7	X	C1	M
A.A.10.2/5	Responding AP Invocation-identifier	C7	X	C1	M
A.A.10.2/6	Responding AE Invocation-identifier	C7	X	C1	M
A.A.10.2/7	Result	C2	M	C1	M
A.A.10.2/8	Result Source — diagnostic	C10	M	C11	M
A.A.10.2/9	ACSE-requirements	C9	See 2.6.6.2.2.2	C8	See 2.6.6.2.2.3
A.A.10.2/10	Authentication-mechanism-name	C9	See 2.6.6.2.2.2	C8	See 2.6.6.2.2.3
A.A.10.2/11	Authentication-value	C9	See 2.6.6.2.2.2	C8	See 2.6.6.2.2.3
A.A.10.2/12	Implementation Information	C7	X	C6	O
A.A.10.2/13	User Information	C7	M	C6	M

C1: If [A-CON_initiator], then M else N/A.
C2: If [A-CON_responder], then M else N/A.
C6: If [A-CON_initiator], then O else N/A.
C7: If [A-CON_responder], then O else N/A.
C8: If [A-CON_initiator and A-FU(AU)], then M else N/A.
C9: If [A-CON_responder and A-FU(AU)], then M else N/A.
C10: If [A-CON_responder], then (if [A-FU(AU)] then M (with a value range of 0 to 14) else M (with a value range of 0 to 10) else N/A.
C11: If [A-CON_initiator], then (if [A-FU(AU)] then M (with a value range of 0 to 14) else M (with a value range of 0 to 10) else N/A.

2.6.6.2.2.2 The AARE parameters “ACSE-requirements,” “authentication-mechanism-name” and “authentication-value” shall be supported for sending only if the connection responder role (A-CON_responder) and the authentication functional unit (A-FU(AU)) are supported.

2.6.6.2.2.3 The AARE parameters “ACSE-requirements”, “authentication-mechanism-name” and “authentication-value” shall be supported for receiving only if the connection initiator role (A-CON_initiator) and the authentication functional unit (A-FU(AU)) are supported.

2.6.6.2.3 A-Release-request (RLRQ)

The parameters in the RLRQ APDU shall be supported as specified in Table 2-55.

Table 2-55. Supported RLRQ parameters

Ref.	*Parameter*	*Sender*		*Receiver*	
		ISO status	*ATN support*	*ISO status*	*ATN support*
A.A.10.3/1	Reason	C12	M	C4	M
A.A.10.3/2	User Information	C12	M	C4	M

C4: If [A-REL_acceptor], then M else N/A.
C12: If [A-REL_requestor], then O else N/A.

2.6.6.2.4 A-Release-response (RLRE)

The parameters in the RLRE APDU shall be supported as specified in Table 2-56.

Table 2-56. Supported RLRE parameters

Ref.	*Parameter*	*Sender*		*Receiver*	
		ISO status	*ATN support*	*ISO status*	*ATN support*
A.A.10.4/1	Reason	C13	M	C3	M
A.A.10.4/2	User Information	C13	M	C3	M

C3: If [A-REL_requestor], then M else N/A.
C13: If [A-REL_acceptor], then O else N/A.

2.6.6.2.5 A-Abort (ABRT)

The parameters in the ABRT APDU shall be supported as specified in Table 2-57.

Table 2-57. Supported ABRT parameters

		Sender		*Receiver*	
Ref.	*Parameter*	*ISO status*	*ATN support*	*ISO status*	*ATN support*
A.A.10.5/1	Abort Source	M	M	M	M
A.A.10.5/2	Diagnostic	C14	M	C14	M
A.A.10.5/3	User Information	O	M	M	M

C14: If [A-FU(AU)], then M else N/A.

2.6.6.3 Supported parameter forms and values

2.6.6.3.1 AE-title name form

The AE-title parameter shall be supported in the forms specified in Table 2-58.

Table 2-58. AE-title name form

		Sender		*Receiver*	
Ref.	*Syntax form*	*ISO status*	*ATN support*	*ISO status*	*ATN support*
A.A.11.1/1	Form 1 (Directory name)	O.5	X	M	O
A.A.11.1/2	Form 2 (Object identifier and integer)	O.5	M	M	M

O.5: The ISO standard requires a conforming implementation to support at least one of the forms.

2.6.6.3.2 Authentication value form

2.6.6.3.2.1 The authentication-value parameter shall be supported in the forms specified in Table 2-59.

Table 2-59. Authentication-value form

Prerequisite: A-FU(AU)

Ref.	*Authentication-value form*	*Sender*		*Receiver*	
		ISO status	*ATN support*	*ISO status*	*ATN support*
A.A.11.2/1	GraphicString	O.6	X	C14	N/A
A.A.11.2/2	BIT STRING	O.6	M	C14	M
A.A.11.3/3	EXTERNAL	O.6	X	C14	N/A
A.A.11.4/4	Other	O.6	X	C14	N/A

O.6: The ISO standard requires a conforming implementation to support at least one of the forms.
C14: If [A-FU(AU)], then M else N/A.

2.6.6.3.2.2 If the authentication functional unit is supported, the BIT STRING form of encoding the ACSE authentication-value field shall be used with a bit-oriented encoding such that no additional padding bits are appended to the encoded value.

2.6.6.3.3 User Information form

User Information reference

2.6.6.3.3.1 The User Information parameter shall use the forms of reference specified in Table 2-60.

Table 2-60. User Information reference

Ref.	*Parameter*	*Sender*		*Receiver*	
		ISO status	*ATN support*	*ISO status*	*ATN support*
	Direct-reference	O	X	M	N/A
	Indirect-reference	O	O (See 2.6.6.3.3.2)	M	M
	Data-value-descriptor	O	X	M	N/A

2.6.6.3.3.2 The Indirect-reference parameter contains a presentation-context-id value as specified in Table 2-10 when the single-ASN-1-type encoding form is used. Otherwise, the presentation-context-id value is absent.
User Information encoding type

2.6.6.3.3.3 The User Information parameter encoding choice shall be as specified in Table 2-61.

Table 2-61. User Information encoding choice

Ref.	Parameter	Sender		Receiver	
		ISO status	*ATN support*	*ISO status*	*ATN support*
	Single-ASN1-type	O	O	M	M
	Octet-aligned	O	X	M	N/A
	Arbitrary	O	O	M	M

2.6.6.3.3.4 The arbitrary form of encoding ACSE user-information should be used.

2.6.6.3.3.4.1 If the recommendation in 2.6.6.3.3.4 is followed, a canonical encoding for a given user PDU is produced. This encoding is consistent with the fully-encoded-data wrapper used by the CF at the presentation service boundary and provides optimal bit-efficiency.

2.6.6.3.3.5 When the arbitrary (BIT STRING) form of encoding is used, a bit-oriented encoding shall be applied, such that no additional padding bits are appended to the encoded BIT STRING value in the EXTERNAL user information type or to the encoded EXTERNAL value itself.

2.6.6.3.3.5.1 The provision in 2.6.6.3.3.5 means that data encoded by ATN-App ASEs, when embedded as user-information in ACSE APDUs, are treated by the CF as normal BIT STRING values, not in general as an integral number of octets. Padding to an octet boundary only applies to the outermost fully-encoded-data value that is passed across the presentation service boundary.

2.6.6.3.3.6 If the single-ASN1-type (ABSTRACT-SYNTAX.&Type) form of encoding is used, the octet-oriented encoding of an open type shall be applied, such that additional padding bits are appended in order to make the length of the encoding already produced a multiple of eight bits.

2.6.6.3.3.6.1 Encoding as a single-ASN1-type is permitted for backward compatibility, but its use is deprecated.

2.6.6.3.4 Supported parameter values

The mechanism-name field in AARQ and AARE APDUs shall be omitted when sending, and ignored when receiving. (Use of the authentication-mechanism-name field is reserved for use in future versions of the ATN profile.)

2.6.7 Mapping to the presentation service

The mapping of ACSE APDUs and parameters to presentation service primitives shall be performed by the CF as specified in 2.3, which takes precedence over the direct mapping defined in Clause 8 of ISO/IEC 8650-1: 1996 | ITU-T Rec. X.227 (1995).

2.7 CONNECTIONLESS DIALOGUE SERVICE (CLDS) AND PROFILE

The CLDS allows the exchange of unconfirmed datagrams between communicating users. The CLDS and supporting upper layer profiles are not used by any of the current CNS/ATM applications specified in Parts I and II of this manual, therefore, this section is merely a placeholder for a possible future development.

2.8 ATN MESSAGE INTEGRITY CHECK ALGORITHM

2.8.1 The integrity check algorithm may optionally be invoked by the ATN application-user specification to provide a proof of message integrity. If other information (e.g. sender and/or receiver identity) is also bound to the message when the integrity sequence is computed and verified, then it can provide additional proof (e.g. a proof of delivery to an intended recipient).

2.8.2 The specification of the default ATN integrity check algorithm is included in Part I of this manual.

Chapter 3

INTERNET COMMUNICATIONS SERVICE (ICS)

3.1 INTRODUCTION

3.1.1 This chapter of Doc 9880 defines the provisions that ATN compliant end systems (ESs) and intermediate systems (ISs) must implement in order to provide the ATN "Internet Communications Service" to the "User" i.e. the upper layer architecture as defined in Doc 9880, Part III, Chapter 2. For the protocols, the majority of such provisions are specified in a tabular fashion under the title of "ATN Protocol Requirements Lists" (APRLs).

3.1.2 This chapter of Doc 9880 comprises nine sections as introduced below.

Section 3.1 contains introductory material to the remainder of the chapter.

Section 3.2 contains pertinent definitions of the Internet routing architecture and components including routing domains, administrative domains, routing domain confederations, ATN backbone, ATN islands, etc. Furthermore it contains system level provisions related to communications protocol support for ATN end systems and intermediate systems, and requirements related to security and priority handling within the ATN Internet.

Section 3.3 contains provisions related to the deployment of ATN components within the ATN Internet, to the use of routing information, to the definition of routing policies, and to the procedures for initiating the exchange of routing information.

Section 3.4 contains provisions related to the ATN Internet addressing architecture and responsibilities related to the definition and allocation of ATN Internet address fields.

Section 3.5 contains "Transport Layer" provisions applicable to ATN end systems. Provisions for the ISO connection oriented transport protocol (Class 4) are defined.

Section 3.6 contains "Inter-Network Layer" provisions, based on the ISO connectionless network protocol (CLNP), applicable to ATN end systems and ATN intermediate systems.

Section 3.7 contains provisions related to the use of the various candidate ground-ground and air-ground subnetworks of the ATN in order to ensure successful inter-operation of ATN intermediate systems and the subnetworks to which they are attached. Compression techniques are also defined to enable the efficient use of the limited bandwidth available over such air-ground subnetworks.

Section 3.8 contains provisions related to the exchange of routing information between ATN intermediate systems using the inter domain routing information exchange protocol (IDRP) and specific features of the ES-IS protocol.

Section 3.9 contains a set of notes regarding the implementation of Internet systems management.

3.2 DEFINITIONS AND CONCEPTS

3.2.1 Objectives and goals

Note 1.— In computer data networking terminology, the infrastructure required to support the inter-connection of automated ATM (Air Traffic Management) systems is referred to as an Internet. Simply stated, an Internet comprises the interconnection of computers with gateways or routers via real subnetworks. This allows the construction of a homogeneous virtual data network in an environment of administrative and technical diversity. Given the desire to interconnect an evolving and ever wider variety of aircraft- and ground-based computers to accomplish ATM automation, it is clear that the civil aviation community needs a global data Internet. The internetworking infrastructure developed by ICAO for this purpose is the ATN.

Note 2.— The ATN design allows communication services for different user groups, i.e. air traffic services (ATS), aeronautical operational control (AOC), aeronautical administrative communications (AAC) and aeronautical passenger communications (APC). The design provides for the incorporation of different air-ground subnetworks (e.g. SSR Mode S, AMSS, VDL) and different ground-ground subnetworks, resulting in a common data transfer service. These two aspects are the basis for interoperability of the ATN and will provide a reliable data transfer service for all users. Furthermore, the design is such that user communications services can be introduced in an evolutionary manner.

Note 3.— The ATN is capable of operating in a multinational environment with different data communication service providers. The ATN is capable of supporting air traffic service communication (ATSC) as well as aeronautical industry service communication (AINSC).

Note 4.— The ATN is capable of supporting the interconnection of end systems (ESs) and intermediate systems (ISs) using a variety of subnetwork types.

3.2.2 Definitions

Note.— This specification makes extensive use of the definitions, concepts and terminology derived from the OSI Reference Model (ISO 7498 parts 1-4) and the OSI Routing Framework (ISO/IEC TR 9575).

3.2.2.1 The ATN Internet

3.2.2.1.1 The ATN shall consist of a set of interconnected Routing Domains (RDs), within the global OSI Environment (OSIE). Each such RD shall contain ATSC- and/or AINSC-related intermediate and end systems.

3.2.2.1.2 A routing domain that declares itself to be a transit routing domain (TRD) shall implement a routing policy that supports the relaying of network protocol data units (NPDUs) received from at least one other routing domain to destinations in another routing domain.

3.2.2.1.3 Otherwise, the routing domain shall be defined as an end routing domain (ERD).

3.2.2.2 ATN RDs

3.2.2.2.1 General

3.2.2.2.1.1 An ATN RD shall meet the requirements specified in ISO/IEC TR 9575 for a routing domain and shall include one or more ATN routers.

3.2.2.2.1.2 Every ATN RD shall have at least one routing domain identifier (RDI).

3.2.2.2.1.3 Each RDI shall unambiguously identify a single RD.

Note.— An RDI is a generic network entity title (NET) and has the same syntax as an ATN NSAP address; alias RDIs are permitted.

3.2.2.2.2 Fixed RDs

Each State and organization participating in the ATN shall operate one or more ATN RDs, comprising air-ground and ground-ground routers as required to interconnect with mobile RDs and other ground-based ATN RDs, respectively.

Note.— Adjacent States and/or organizations may alternatively combine their RDs into a single RD.

3.2.2.2.3 Mobile RDs

3.2.2.2.3.1 Each ATN-equipped mobile platform (e.g. an aircraft) shall operate at least one ATN RD. This shall be an end routing domain.

3.2.2.2.3.2 This ERD shall include ATSC- and AINSC-related intermediate and end systems contained within this mobile platform and at least one airborne router (Router Class 6 or 7 as defined in Table 3-1).

Note.— An ATN mobile platform may operate multiple ERDs.

3.2.2.2.3.3 When more than one airborne router (BIS) is installed on board an aircraft, then each shall be in a separate routing domain.

3.2.2.2.3.4 ATSC and AINSC end systems and intermediate systems (non-BISs) located within a mobile platform should form a single routing domain including the airborne router (BIS) referred to in the above note, within the appropriate administrative domain.

Note 1.— A single routing domain minimizes the transfer of routing information over low-bandwidth air-ground subnetworks.

Note 2.— It is anticipated that other classes of mobile platforms (airport surface vehicles, etc.) may be operated as ATN routing domains in the future.

3.2.2.3 The ground ATN Internet

3.2.2.3.1 General

The ground ATN Internet shall consist of one or more ATN island RDCs (routing domain confederations).

3.2.2.3.2 ATN island RDC

3.2.2.3.2.1 Each ATN island shall comprise one or more ATN RDs forming a single ATN island RDC.

3.2.2.3.2.2 An ATN island RDC shall not contain any ATN mobile RDs.

Note.— An example ATN island RDC topology is presented in Figure 3-1.

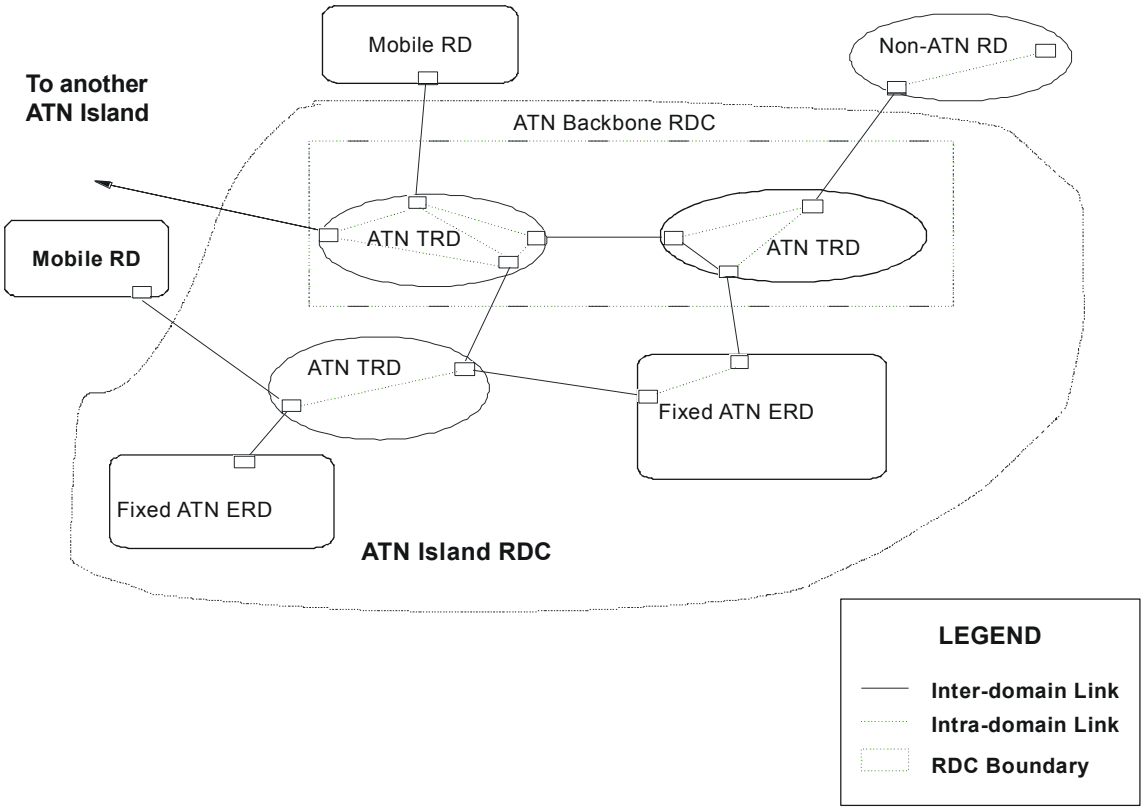


Figure 3-1. Interdomain routing in an ATN island

3.2.2.3.3 The fixed ATN RDC

The fixed ATN RDC shall comprise all ATN RDs other than ATN mobile RDs.

Note.— The fixed ATN RDC enables a ground ATN router to advertise a route to a mobile, the destination of which is the entire fixed ATN, without having to enumerate the RDIs of all ATN RDs in the RD_Path Attribute.

3.2.2.4 The global ATN backbone

3.2.2.4.1 General

The global ATN backbone shall comprise at least one ATN RD from each ATN island, interconnected either directly or indirectly via other members of the global ATN backbone.

Note.— The purpose of the global ATN backbone is to provide a high availability core network of ATN routers supporting ATN mobile routing.

3.2.2.4.2 ATN island backbone RDCs

3.2.2.4.2.1 Within each ATN island, those ATN RDs that are members of the global ATN backbone should form a single RDC, which is referred to as the ATN island backbone RDC.

3.2.2.4.2.2 An ATN island backbone RDC, when present, shall be nested within an ATN island RDC.

Note 1.— The purpose of the ATN island backbone RDC is to permit more than one ATN RD to act as the default route provider for an ATN island. It also provides a containment boundary to limit the impact of changes in routes to mobile RDs to only the members of the backbone RDC and not to the rest of the ATN island.

Note 2.— This is a recommended practice only as in some regions, simpler, or other alternative structures may be more appropriate for an ATN island.

3.2.2.5 The "Home" domain

Aircraft for which inter-island communications are required shall have a "Home" domain, which is a routing domain in an ATN island.

Note 1.— This "Home" need not be in either the ATN island through which the aircraft is currently reachable or in the ATN island with which communication is required.

Note 2.— The role of the "Home" domain is to advertise a default route to all the aircraft belonging to an airline or the general aviation aircraft of a given country of registration. This default route is advertised to the ATN global backbone in line with the routing policies specified in 3.3.7.

3.2.2.6 Administrative domains and the ATN

The administrative domain of each administration and aeronautical industry member that operates one or more ATN RDs shall comprise both their ATN RDs and any non-ATN RDs that they operate.

Note 1.— The routing policies for communication between ATN and non-ATN RDs within the same administrative domain is a local matter.

Note 2.— While meeting the ATN requirements, the distribution of end system and intermediate system functionality and the use of interworking processes exclusively within an administrative domain is a local matter.

3.2.2.7 Default routes

3.2.2.7.1 The default route to all aircraft shall be a route in the context of IDRP that:

a) is available to all traffic types (see 3.2.7.1.2); and

b) has in its destination two NSAP address prefixes. One of these is the NSAP address prefix that is common to all AINSC airborne systems and only AINSC airborne systems, and the other is the NSAP address prefix that is common to all ATSC airborne systems and only ATSC airborne systems.

3.2.2.7.2 The default route to all the aircraft belonging to an airline or the general aviation aircraft of a given country of registration shall be a route in the context of IDRP that:

a) is available to all traffic types (see 3.2.7.1.2); and

b) has in its destination an NSAP address prefix which is common to all airborne systems and only those airborne systems of the aircraft that belong to that airline or are registered in that country.

3.2.3 ATN end systems

Note 1.— ATN end systems are capable of communicating with other ATN end systems, either directly or indirectly, to provide end-to-end communication service for air-ground or ground-ground applications, or both.

Note 2.— An ATN end system is a realization of the OSI end system architectural entity.

Note 3.— An ATN end system supports one or more ATN applications and supports their communication over the ATN by providing either the connection mode transport service, or the connectionless mode transport service, or both.

3.2.3.1 Physical and data link layer

ATN end systems shall implement the appropriate physical and data link layer functions for access to the ATN subnetwork(s) to which they are attached.

3.2.3.2 Network layer

3.2.3.2.1 ATN end systems shall implement:

a) the end system provisions of ISO/IEC 8473, as specified in ⁋3.6, as the subnetwork independent convergence function (SNICF);

b) a subnetwork access protocol (SNAcP) suitable for each underlying subnetwork;

c) a subnetwork dependent convergence function (SNDCF) providing byte and code independent service to the SNICF (i.e. ISO/IEC 8473) via the appropriate subnetwork access protocol, as specified in ⁋3.7.

3.2.3.2.2 ATN end systems should implement the end system provisions of ISO/IEC 9542 to facilitate the exchange of routing information between the ES and any locally attached IS(s).

3.2.3.3 Transport layer

Depending on the requirements of the application and its supporting upper-layer protocols, ATN end systems shall implement either one or both of the following:

a) ISO/IEC 8073 as specified in ⁋3.5

b) ISO/IEC 8602 as specified in ⁋3.5.

3.2.3.4 Upper layers

Note.— The requirements for session, presentation and application layer protocols to support end-user applications on ATN end systems are defined in Doc 9880, Part III, Chapter 2.

3.2.3.5 Applications

Note.— The requirements for air-ground and ground-ground applications are contained in Doc 9880, Parts I and II, respectively.

3.2.4 ATN routers

Note 1.— ATN routers are capable of the relaying and routing of network layer protocol data units with other ATN routers and with directly connected ATN end systems.

Note 2.— An ATN router is a realization of the OSI intermediate system architectural entity. ATN routers that additionally implement ISO/IEC 10747 are also known as boundary intermediate systems (BISs).

3.2.4.1 ATN router classes

3.2.4.1.1 The classes of ATN router and the routing protocols supported, that are recognized by this specification, are listed in Table 3-1.

Table 3-1. ATN router classes

Class	*Name*	*Routing protocols supported*
1.	Static router	ISO/IEC 9542 (optional)
2.	Level 1 router	ISO/IEC 9542 (optional) ISO/IEC 10589 Level 1 only
3.	Level 2 router	ISO/IEC 9542 (optional) ISO/IEC 10589 Level 1 and Level 2
4.	Ground-ground router	ISO/IEC 9542 (optional) ISO/IEC 10589 (optional) ISO/IEC 10747
5.	Air-ground router (ground based)	ISO/IEC 9542 ISO/IEC 10589 (optional) ISO/IEC 10747 Route initiation procedures (see 3.3.5.2)
6.	Airborne router with IDRP	ISO/IEC 9542 ISO/IEC 10747 Route initiation procedures (see 3.3.5.2)
7.	Airborne router without IDRP	ISO/IEC 9542 Route initiation procedures (see 3.3.5.2)

Note 1.— Classes 1, 2 and 3 are only for use within an ATN routing domain and their specification is a local matter.

Note 2.— The intra-domain parts of router classes 4 and 5 are also a local matter.

Note 3.— The intra-domain parts of router classes 6 and 7 are concerned with the interconnection of avionics to the airborne router and are the subject of aeronautical industry standards.

Note 4.— Router classes 5, 6 and 7 describe routers that support at least one ATN mobile subnetwork.

3.2.4.1.2 All ATN routers (i.e. router classes 1 to 7 inclusive) shall support the ISO/IEC 8473 connectionless network protocol (CLNP) as specified in §3.6, including the use of the CLNP options security parameter, and shall interpret and obey the routing policy requirements expressed therein, whilst routing the packet in accordance with any restrictions placed on the traffic types that may be carried over a given ATN subnetwork, by forwarding CLNP NPDUs.

3.2.4.1.3 With the exception of airborne routers that implement the procedures for the optional non-use of IDRP (i.e. router class 7), all ATN inter-domain routers (i.e. router classes 4 to 6 inclusive) shall support the ISO/IEC 10747 inter-domain routing protocol (IDRP) as specified in §3.8 for the exchange of inter-domain routing information according to §3.3.6 and §3.3.7.

3.2.4.1.4 An airborne (router classes 6 or 7) or air-ground router (router class 5) shall support the mobile SNDCF specified in §3.7 for the use of CLNP over an ATN mobile subnetwork, and the ISO/IEC 9542 ES-IS routing information exchange protocol, as specified in §3.8 for support of the route initiation procedures specified in §3.3.5.2.

3.2.4.2 Physical and data link layers

ATN routers shall implement the appropriate physical and data link layer functions for access to the ATN subnetwork(s) to which they are attached.

3.2.4.3 Network layer

3.2.4.3.1 An ATN router shall implement:

a) the intermediate system provisions of ISO/IEC 8473, as specified in §3.6, as the SNICF;

b) a SNAcP suitable for each underlying subnetwork;

c) a SNDCF providing byte and code independent service to the SNICF (i.e. ISO/IEC 8473) via the selected subnetwork access protocol, as specified in §3.7;

d) the routing protocols specified in Table §3-1 for the router's router class, as specified in §3.8;

e) the route initiation procedures appropriate to the router class, as specified in §3.3;

f) Where an ATN router is directly connected to one or more mobile subnetworks, it shall implement a sub-set of the ISO/IEC 9542 for operation over those subnetworks to facilitate the exchange of addressing information (BIS network entity title) between the router and its peer as specified in §3.3 (see §3.3.5.2) and in §3.8.

3.2.4.3.2 ATN routers of class 5 (air-ground routers) and of class 7 (airborne routers without IDRP) shall also implement the mechanisms necessary to support the "optional non-use of ISO/IEC 10747" as specified in §3.3.

3.2.4.3.3 All ATN airborne routers should support the use of ISO/IEC 10747 (i.e. class 6 is the preferred airborne router class).

Note.— Some States may elect to support the optional non-use of airborne IDRP procedures in their air-ground routers; however, regional implementation planning groups must acknowledge the requirement for aircraft using IDRP within the region to communicate with an air-ground router, independent of how that is accomplished.

3.2.5 ATN subnetworks

Note.— An ATN subnetwork is any fixed or mobile data communications network that fulfils the following requirements.

3.2.5.1 Requirements for all ATN subnetworks

3.2.5.1.1 Byte and code independence

Data shall be transferred through ATN subnetworks in a byte and code independent manner.

Note.— If necessary, this byte and code independence may be ensured through the services of the SNDCF.

3.2.5.1.2 Subnetwork QoS

A subnetwork service provider shall provide an indication of the subnetwork QoS available, in order to support the internetwork routing decision process.

3.2.5.1.3 Subnetwork addressing

An ATN subnetwork shall provide a mechanism for uniquely and unambiguously identifying each ATN router attached to that subnetwork.

3.2.5.1.4 Internal subnetwork routing

Routing between specified source and destination subnetwork point of attachment (SNPA) addresses on an ATN subnetwork shall be carried out by mechanisms internal to the subnetwork.

3.2.5.2 Requirements for ATN mobile subnetworks

3.2.5.2.1 Invocation of subnetwork priority

When priority is implemented within that subnetwork, an ATN mobile subnetwork shall provide a SNAcP mechanism for invocation of subnetwork priority.

3.2.5.2.2 Invocation of subnetwork QoS for mobile subnetworks

ATN mobile subnetworks should provide a mechanism for invocation of subnetwork QoS.

Note 1.— Subnetwork QoS parameters include transit delay, protection against unauthorized access, cost determination and residual error probability.

Note 2.— ATN mobile subnetworks may allocate subnetwork resources on a per user or per subnetwork connection basis in order to make available a different QoS.

3.2.5.2.3 Connection-mode subnetwork service

3.2.5.2.3.1 An ATN mobile subnetwork shall provide a connection-mode service between SNPAs, with a well-defined start and end to a connection, and with reliable, sequenced SNSDU transfer over that connection.

3.2.5.2.3.2 When QoS is available on a per subnetwork connection basis, the SNAcP shall provide mechanisms for selecting a specific QoS when the subnetwork connection is established.

Note 1.— A mobile subnetwork implementing ISO/IEC 8208 to provide a connection-mode service between SNPAs meets this requirement; however, where appropriate, an alternative protocol providing the same service may be used.

Note 2.— This requirement does not imply the need for a single mobile SNAcP.

3.2.5.2.4 Connectivity status changes

Note.— ATN mobile subnetworks are assumed to provide a mechanism for detection of change in media connectivity. The mechanism is both subnetwork and implementation dependent and is outside the scope of this specification.

3.2.5.2.4.1 An ATN mobile subnetwork shall provide subnetwork connectivity information to connected subnetwork service users (i.e. connected ATN routers), in order to initiate operation of the internetwork routing protocols as specified in ⁋3.3.

Note 1.— The mechanism by which the subnetwork connectivity information is conveyed to connected ATN routers is both subnetwork and implementation dependent and is outside the scope of this specification.

Note 2.— It is desirable for the Intermediate System – Systems Management Entity (IS-SME) to be notified as soon as possible by the SN-SME when communication is possible with a newly attached BIS and for an immediate decision to be made as regards bringing up the link.

3.2.5.2.4.1.1 ATN mobile subnetworks shall issue a join event (see ⁋3.3.5.2) to the attached IS-SME to indicate the availability of a physical communication path between a pair of SNPAs.

3.2.5.2.4.1.2 ATN mobile subnetworks shall issue a leave event (see ⁋3.3.5.2.13) to the attached IS-SME to indicate that a previously available physical communication path between a pair of SNPAs is no longer available.

3.2.5.2.4.1.2.1 ATN mobile subnetworks supporting the ATN operational communications traffic type and the ATSC traffic category (see ⁋3.2.7.1.2) shall have a maximum delay, at 95 per cent probability, for issuing a leave event consistent with the requirements in ⁋3.2.7.1.3 for the ATSC class supported by that subnetwork.

3.2.5.2.5 Segmentation/reassembly mechanism

An ATN mobile subnetwork should provide a mechanism that allows the conveyance of large SNSDUs greater than the subnetwork's internal packet size between SNPAs.

Note.— It is the responsibility of the subnetwork to ensure that this data is efficiently segmented and/or concatenated for efficient transfer over the physical medium. If this capability is not present within an ATN mobile subnetwork, ISO/IEC 8473 can support segmentation of NPDUs for transit over subnetworks with small maximum SNSDU sizes.

3.2.6 Quality of Service concept

Note 1.— In the ATN, the Quality of Service provided to applications is maintained using capacity planning techniques that are outside the scope of this specification. Network administrators are responsible for designing and implementing a network that will meet the QoS requirements of the ATN applications that use it.

Note 2.— Network administrators may take advantage of the QoS requirements signalled by the ATSC class (see 3.2.7.1.3), in order to ensure that only those parts of the ATN that support the QoS requirements of ATSC applications need be designed to meet those requirements.

Note 3.— In order to support the QoS requirements of ATSC applications, this specification defines the maximum one-way ATN end-to-end transit delay (see Table 3-2) as well as the maximum one-way ATN mobile subnetwork transit delay and the maximum delay in issuing a leave event for ATN mobile subnetworks supporting ATN operational communications – ATSC traffic (see Table 3-3).

Table 3-2. Transit delays for ATSC class

Maximum one-way ATN end-to-end transit delay at 95 per cent probability (seconds)	*ATSC Class*
Reserved	A
4.5	B
7.2	C
13.5	D
18	E
27	F
50	G
100	H
No value specified	no preference
Note 1.— The value for the ATN end-to-end transit delay represents approximately 90 per cent of the value for the total end-to-end transit delay between the ultimate users of the system. *Note 2.— The 95 per cent probability is based on the availability of a route conforming to the requested ATSC class.*	

3.2.7 ATN security concept

Note 1.— ATN security functions are concerned with:

a) protecting ATN data link applications from internal and external threats;

b) ensuring that application Quality of Service and routing policy requirements are maintained, including service availability; and

c) ensuring that air-ground subnetworks are used in accordance with ITU resolutions on frequency utilization.

Note 2.— There are no security mechanisms provided in the ATN Internet for protecting ATN data link applications. ATN data link applications are protected by upper layer security functions in ATN ESs which implement ATN security services as defined in Doc 9880, Part III, Chapter 2.

Note 3.— The ATN Internet does provide mechanisms to support items (b) and (c) above. These mechanisms are defined to take place in a common domain of trust, and use a security label in the header of each CLNP PDU to convey information identifying the "traffic type" of the data and the application's routing policy and/or strong QoS requirements. No mechanisms are provided to protect the integrity of this label or its binding to the application data.

Note 4.— In order to permit the later extension of the ATN to handle classified data, the security label in the CLNP PDU header can additionally be used to convey security classification information.

Note 5.— The routing information necessary to support this security label is maintained through information conveyed in the ISO/IEC 10747 security path attribute about each route. ATN routers of classes 4 and above reference this routing information during the NPDU forwarding process in order to meet the application's requirements expressed through the NPDU's security label and to enforce any applicable ITU resolutions on frequency utilization.

3.2.7.1 The ATN security label

3.2.7.1.1 General

3.2.7.1.1.1 The ATN security label shall be encoded according to 3.6.2.2.2.

3.2.7.1.1.2 An ATN security label shall be provided as part of the header of every CLNP NPDU, except for those that convey general communications applications data.

Note.— The above implies that any CLNP NPDU that does not contain an ATN security label contains general communications data.

3.2.7.1.2 Traffic types

3.2.7.1.2.1 A CLNP Ddta NPDU's security label shall identify the "Traffic Type" of its user data, as either:

a) ATN operational communications;

b) ATN administrative communications;

c) ATN systems management communications.

Note.— ATN operational communications traffic type is broken down into two categories: ATSC and AOC (see Table 3-9).

3.2.7.1.2.2 For the ATN operational communications traffic type and the ATSC traffic category, routing policy requirements shall be expressed through further information encoded into the security label, as either:

a) a preferred ATSC Class; or

b) no routing policy preference.

3.2.7.1.2.3 For the ATN operational communications traffic type and the AOC traffic category, routing policy

requirements shall be expressed through further information encoded into the security label, as either no routing policy preference, or an ordered list of appropriate air-ground subnetworks to be used.

Note.— The possible orderings of air-ground subnetworks are specified in Table 3-9.

3.2.7.1.3 ATSC class

3.2.7.1.3.1 ATN mobile subnetworks supporting the ATN operational communications traffic type and the ATSC traffic category shall satisfy the maximum subnetwork transit delay requirements specified in Table 3-3 for the advertised ATSC class.

3.2.7.1.3.2 ATN mobile subnetworks supporting the ATN operational communications traffic type and the ATSC traffic category shall satisfy the maximum delay requirements in issuing a leave event as indicated in either the third or/and the fourth column of Table 3-3 for the advertised ATSC class.

Table 3-3. Subnetwork transit delay and leave event issuance maximum delay

ATSC class	*Maximum one-way ATN mobile subnetwork transit delay at 95 per cent probability (in seconds)*	*Maximum delay, at 95 per cent probability, in issuing a leave event in the absence of NPDU traffic (in seconds)*	*Maximum delay, at 95 per cent probability, in issuing a leave event in the presence of NPDU traffic (in seconds)*
A	reserved	reserved	reserved
B	3.0	27	18
C	5.7	44	29
D	10	81	54
E	14.5	108	72
F	23.5	162	108
G	46.5	300	240
H	96.5	> 300	> 240

Note 1.— The ATN end-to-end transit delay semantics of the ATSC class are defined in Table 3-2.

Note 2.— The maximum one-way ATN mobile subnetwork transit delay is for data packets associated with ATSC high priority flight safety messages, as defined in Annex 10, Volume III, Part 1, Chapter 3, Table 3-1, when delivered by the mobile subnetwork operating at the nominal maximum subnetwork loading (e.g. serving the maximum number of users the subnet is designed to handle on the available radio frequency channel(s)).

Note 3.— The delay in issuing a leave event (see 3.2.5.2.4.1.2.1) is defined as the time from when a previously available physical communication path is no longer available until the time the leave event is actually issued to the attached IS-SME.

Note 4.— An example for the loss of a physical communication path would be an aircraft moving out of the coverage of the VDL Mode 2 ground stations belonging to a given VDL Mode 2 ground system.

Note 5.— In the case of ongoing air-ground data exchange, the arrival of an NPDU from an attached ATN

router may be used by the subnetwork as the event to detect loss of a previously available communication path. In this case (i.e. fourth column of Table 3-3) detection of the loss of subnetwork connectivity and issuance of a leave event is expected to be more expeditious than in the absence of data traffic (i.e. third column of Table 3-3).

Note 6.— The semantics of the ATSC class for other QoS metrics and availability are outside of the scope of this specification.

3.2.7.1.4 Security classification

Note.— The security classification may be used to convey the confidentiality level of application data.

3.2.7.2 Applications use of ATN security labels

3.2.7.2.1 ATN data link applications shall specify an ATN security label for each message category that they support. This ATN security label shall identify:

a) the traffic type appropriate for the message; and

b) for ATN operational communications applications, the application's requirements for the routing of the message, if any, expressed as specified in 3.2.7.1.2.

3.2.7.2.2 When sent using the connection-mode transport service, a message shall only be conveyed over a transport connection which is associated with the same ATN security label as that specified for the message's message category.

3.2.7.2.3 When sent using the connectionless-mode transport service, the TSDU conveying that message shall be associated with the ATN security label of the specified message category.

3.2.7.3 Transport layer security

3.2.7.3.1 In the connection mode

3.2.7.3.1.1 Except when a transport connection is used to convey general communications data, each transport connection shall be associated with a single ATN security label.

3.2.7.3.1.2 The value of this label shall be determined when the connection is initiated.

Note.— It is not possible to change an ATN security label during the lifetime of a transport connection.

3.2.7.3.1.3 Every NSDU passed to the network layer that contains a TPDU from a transport connection associated with an ATN security label shall be associated with the same ATN security label.

Note.— The network layer functions may then encode this ATN security label in the NPDU header.

3.2.7.3.1.4 TPDUs from transport connections associated with different ATN security labels shall not be concatenated into the same NSDU.

3.2.7.3.1.5 When an incoming CR TPDU is received, the ATN security label, if any, encoded into the header of the NPDU that conveyed it, shall define the ATN security label that is associated with the transport connection.

Note 1.— The mechanism by which the connection initiator provides the appropriate ATN security label is a local matter. For example, it may be identified by an extension to the transport service interface, be implicit in the choice of a given TSAP, or be identified using a systems management function.

Note 2.— Some applications may reject incoming transport connections for which the ATN security label is inappropriate. Again, the mechanism by which the transport provider passes to its user the ATN security label associated with an incoming transport connection is a local matter.

3.2.7.4 Network layer security

3.2.7.4.1 Service provider to the transport layer

The network service shall provide a mechanism that permits an ATN security label to be associated with an NSDU:

a) when passed from the transport layer to the network layer in an NS-UNITDATA.request. This ATN security label shall be encoded into the header of the corresponding CLNP NPDU(s) according to 3.6.2.2.2;

b) when passed from the network layer to the transport layer in an NS-UNITDATA.indication. This ATN security label shall be that received in the header of the associated CLNP NPDU(s).

3.2.7.4.2 Routing control

When present in an NPDU header, the network layer routing functions shall ensure that:

a) the routing policy requirements, if any, encoded into the ATN security label are obeyed; and

b) the NPDU is only routed over paths through the internetwork which both permit and are suitable for data of the traffic type identified by the ATN security label.

Note 1.— 3.3.2.2 specifies the forwarding procedures that ensure the above.

Note 2.— The security information conveyed in ISO/IEC 10747 (IDRP) routes is used to provide the forwarding process with the information needed to support the above.

3.2.7.4.3 Protection of the routing information base

3.2.7.4.3.1 IDRP Type 1 authentication, as specified in ISO/IEC 10747, shall be supported by all ATN routers implementing the ISO/IEC 10747 protocol (i.e. router classes 4 to 6, inclusive) as a mechanism for ensuring the integrity of routing information exchange by IDRP.

3.2.7.5 Subnetwork provisions

Note.— There are no requirements for security mechanisms in ATN subnetworks. However, administrations and other organizations implementing ATN subnetworks are encouraged to ensure the general security and availability of ATN subnetworks through the use of physical security mechanisms.

3.2.8 ATN use of priority

Note 1.— The purpose of priority is to signal the relative importance and/or precedence of data, such that when a decision has to be made as to which data to action first, or when contention for access to shared resources has to be resolved, the decision or outcome can be determined unambiguously and in line with user requirements both within and between applications.

Note 2.— In the ATN, priority is signalled separately by the application in the transport layer and network layer, and in ATN subnetworks. In each case, the semantics and use of priority may differ. Figure 3-2 illustrates where priority is applied in the ATN, and where it is necessary to map the semantics and syntax of ATN priorities.

Note 3.— In the ATN Internet, priority has the essential role of ensuring that high priority safety related data is not delayed by low priority non-safety data, and in particular when the network is overloaded with low priority data.

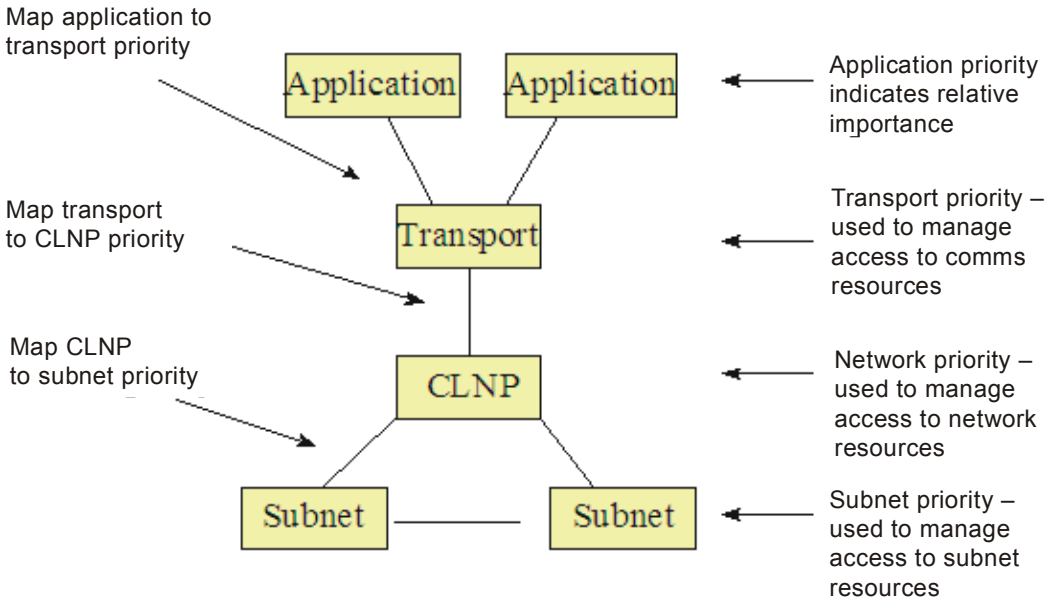


Figure 3-2. Use of priority in the ATN

3.2.8.1 Application priority

Note.— Priority in ATN application protocols is used to distinguish the relative importance and urgency of application messages within the context of that application alone.

3.2.8.1.1 For the purpose of:

a) distinguishing the relative importance and urgency of messages exchanged by different ATN applications; and

b) distinguishing the relative importance and urgency of messages of the same application during their transit through the ATN,

application messages shall be grouped into one or more categories listed in Annex 10, Volume III, Part 1, Chapter 3, Table 3-1.

Note.— An ATN application may include messages from more than one category.

3.2.8.1.2 When a message is sent between ATN application entities, the message shall be sent using either:

a) a transport connection established using the transport connection priority listed in Annex 10, Volume III, Part 1, Chapter 3, Table 3-1 for the message's message category; or

b) the connectionless transport service, signalling the connectionless transport service priority listed in Annex 10, Volume III, Part 1, Chapter 3, Table 3-1 for the message's message category.

Note.— The priority of an individual transport connection cannot be changed during the lifetime of the connection. Therefore, if an application exchanges messages belonging to more than one message category using the connection mode transport service, then a separate transport connection needs to be established for each message category.

3.2.8.2 Transport connection priority

Note 1.— Transport connection priority is concerned with the relationship between transport connections and determines the relative importance of a transport connection with respect to (a) the order in which TCs are to have their QoS degraded, if necessary, and (b) the order in which TCs are to be broken in order to recover resources.

Note 2.— The transport connection priority is specified by the transport user either explicitly or implicitly, when the transport connection is established.

3.2.8.2.1 When an ATN transport layer entity is unable to satisfy a request for a transport connection from either a local or remote TSAP, and which is due to insufficient local resources available to the transport layer entity, then it shall terminate a lower priority transport connection, if any, in order to permit the establishment of a new higher priority transport connection.

Note.— Implementations may also use transport connection priority to arbitrate access to other resources (e.g. buffers). For example, this may be achieved by flow control applied to local users, by discarding received but unacknowledged TPDUs, by reducing credit windows, etc.

3.2.8.2.2 All TPDUs sent by an ATN transport layer entity shall be transferred by the ATN Internet layer, using the network protocol priority that corresponds to the transport connection's priority according to Annex 10, Volume III, Part 1, Chapter 3, Table 3-1.

3.2.8.3 Connectionless transport service priority

Note.— There are no procedures required of the ATN connectionless transport entity in respect of priority, except for mapping the TSDU priority supplied by the service user (i.e. an ATN application), to the corresponding network layer priority, and vice versa.

All UD TPDUs sent by an ATN transport layer entity shall be transferred by the ATN Internet layer using the network protocol priority that corresponds to the TSDU priority provided by the service user according to Annex 10, Volume III, Part 1, Chapter 3, Table 3-1.

3.2.8.4 ATN Internet priority

Note.— In the ATN Internet layer, an NPDU of a higher priority is given preferred access to resources. During periods of higher network utilization, higher priority NPDUs may therefore be expected to be more likely to reach their destination (i.e. are less likely to be discarded by a congested router) and to have a lower transit delay (i.e. be more likely to be selected for transmission from an outgoing queue) than are lower priority packets.

3.2.8.4.1 ATN Internet entities shall maintain their queues of outgoing NPDUs in strict priority order, such that a higher priority NPDU in an outgoing queue will always be selected for transmission in preference to a lower priority NPDU.

Note.— Priority zero is the lowest priority.

3.2.8.4.2 During periods of congestion, or when any other need arises to discard NPDUs currently held by an ATN Internet entity, lower priority NPDUs shall always be discarded before higher priority NPDUs.

Note.— In addition to NPDUs containing user (i.e. transport layer) data, the Internet layer also forwards routing information contained in CLNP data PDUs (e.g. IDRP) and as distinct NPDUs (e.g. ES-IS). These must all be handled at the highest priority if changes to network topology are to be quickly actioned and the optimal service provided to users.

3.2.8.4.3 BISPDUs exchanged by IDRP shall be considered as network/systems management category messages and shall be sent using CLNP priority 14.

3.2.8.4.4 ES-IS (ISO/IEC 9542) PDUs shall be implicitly assumed to have priority 14 and shall be forwarded as if they were CLNP PDUs of priority 14.

Note.— The priority encoded in an ISH PDU conveys the priority of the sending system and not the priority of the PDU.

3.2.8.5 ATN subnetwork priority

3.2.8.5.1 Connection-mode subnetworks

Note 1.— In a connection-mode ATN subnetwork, priority is used to distinguish the relative importance of different data streams (i.e. the data on a subnetwork connection), with respect to gaining access to communications resources and to maintaining the requested Quality of Service.

Note 2.— On some subnetworks (e.g. public data networks), not all data streams will be carrying ATN messages. Therefore, subnetwork priority is also used to distinguish ATN and non-ATN data streams.

Note 3.— So as not to incur the overhead and cost of maintaining too many simultaneous subnetwork connections, NPDUs of a range of network layer priorities may be sent over the same subnetwork connection.

3.2.8.5.1.1 When an ATN connection mode subnetwork does not support prioritization of subnetwork connections, then the ATN Internet entity shall not attempt to specify a subnetwork connection priority, and NPDUs of any priority may be sent over the same subnetwork connection.

3.2.8.5.1.2 When an ATN connection mode subnetwork does support prioritization of subnetwork connections, then unless the relationship between ATN Internet priority and subnetwork priority is explicitly specified by the subnetwork specification, the following shall apply:

a) Subnetwork connections shall be established as either “High” or “Low” priority connections.

b) For the “Low” priority connection type, the priority to gain a connection, keep a connection and for data on the connection shall be the defaults for routine use of the subnetwork.

c) “High” priority connections shall be used to convey NPDUs of priority ten and above. “Low” priority connections shall be used to convey all other NPDUs.

Note.— The above does not apply to the AMSS subnetwork, which has specified its own priority mapping scheme.

3.2.8.5.1.3 When a subnetwork connection is established between two ATN Internet entities and no other subnetwork connection between these two entities exists over any subnetwork, then that subnetwork connection shall always be established at a priority suitable for conveying NPDUs of priority 14 (i.e. network/systems management).

Note.— This is to ensure that routing information can be exchanged at the appropriate priority.

3.2.8.5.2 Connectionless-mode subnetworks

Note 1.— The purpose of priority on a connectionless-mode subnetwork is to provide higher priority NPDUs with preferred access to subnetwork resources.

Note 2.— The relationship between NPDU priority and subnetwork priority is subnetwork specific.

When an NPDU is sent over a connectionless-mode ATN subnetwork which supports data prioritization, then the subnetwork priority assigned to the transmitted packet shall be that specified by the subnetwork provider as corresponding to the NPDU priority.

3.3 ATN ROUTING

3.3.1 Introduction

3.3.1.1 Scope

Note.— This section provides requirements and recommendations pertaining to the deployment of ATN components within the ATN Internet; use of routing information distributed according to ISO/IEC 10747 in order to support policy based and mobile routing in the ATN; and the route initiation procedures for initiating the exchange of

routing information using the ISO/IEC 10747 protocol. In the case of air-ground data links, route initiation also includes the use of the ISO/IEC 9542 protocol. This chapter is not concerned with compliance with the ISO/IEC 10747 and ISO/IEC 9542 protocols. This is the subject of §3.8.

3.3.1.2 Applicability of requirements

Note 1.— The classes of ATN router referred to below are defined in §3.2.4.1.

Note 2.— The ATN RDs referred to below are defined in §3.2.2.2.

3.3.1.2.1 ATN ground-ground routers shall comply with the provisions of §3.3.4 and §3.3.6.

3.3.1.2.2 When used as an ATN router in an ATN RD that is a member of an ATN island backbone RDC, an ATN ground-ground router shall also comply with the provisions of §3.3.7.1.

3.3.1.2.3 When used in any other ATN transit routing domain, an ATN ground-ground router shall also comply with the provisions of §3.3.7.3.

3.3.1.2.4 Otherwise, an ATN ground-ground router shall comply with the provisions of §3.3.7.4.

3.3.1.2.5 ATN air-ground routers shall comply with the provisions of §3.3.4 for ground-ground interconnection, §3.3.5 for air-ground interconnection and §3.3.6.

3.3.1.2.6 When used as an ATN router in an ATN RD that is a member of an ATN island backbone RDC, an ATN air-ground router shall also comply with the provisions of §3.3.7.1.

3.3.1.2.7 When used in any other ATN transit routing domain, an ATN air-ground router shall also comply with the provisions of §3.3.7.3.

3.3.1.2.8 ATN airborne routers shall comply with the provisions of §3.3.5, §3.3.6, and §3.3.7.2.

3.3.1.2.9 When an RD is declared to be an ATN RD, then it shall comply with the provisions of §3.2.2.2.

3.3.1.2.10 When an RD is declared to be a mobile RD, then it shall comply with the provisions of §3.2.2.2.3.

3.3.1.2.11 When an RDC is declared to be an ATN island RDC, then its member RDs shall comply with the provisions of §3.2.2.3.2.

3.3.1.2.12 When an RDC is declared to be an ATN island backbone RDC, then its member RDs shall comply with the provisions of §3.2.2.4.2.

3.3.2 Service provided by an ATN router

3.3.2.1 General

A route shall only be advertised by an ATN router to an adjacent ATN RD when it can be ensured that data sent over that route by the RD to which the route is advertised is acceptable to every RD and RDC in the route's path and will be relayed by them to the route's destination.

Note.— The acceptability of a route may be determined using a priori knowledge derived from interconnection agreements with other RDs.

3.3.2.2 Forwarding CLNP NPDUs

3.3.2.2.1 General

3.3.2.2.1.1 The forwarding processes for a CLNP NDPU shall operate by selecting the FIB identified by the combination of the QoS maintenance and security parameters found in the CLNP header, and selecting from that FIB, the entry, if any, identified by the longest matching NSAP address prefix.

3.3.2.2.1.2 The next hop information found in this FIB entry shall then be used to forward the NPDU.

Note.— Forwarding decisions that take into account the CLNP QoS maintenance parameter are a local matter, and an ATN router may hence ignore this parameter.

3.3.2.2.2 *Forwarding a CLNP NPDU when no security parameter is present in the PDU header*

Note.— This case applies for General Communications data (see §3.2.7.1).

3.3.2.2.2.1 When a CLNP NPDU is received by an ATN router and that NPDU does not contain a security parameter in the PDU header then that NPDU shall be forwarded over the selected route to the NPDU's destination with the longest matching NSAP address prefix and which, either:

1) contains a security path attribute comprising the ATN security registration Identifier and security information that does not contain an ATSC class security tag indicating support for only ATSC traffic, and comprises:

   a) either an air-ground subnetwork security tag that has "General Communications" in its set of permissible traffic types; or

   b) no air-ground subnetwork security tag;

or

2) does not contain any security path attribute.

3.3.2.2.2.2 If no such route can be found then the NPDU shall be discarded.

3.3.2.2.3 Forwarding a CLNP NPDU when a security parameter is present in the PDU header

3.3.2.2.3.1 *General*

3.3.2.2.3.1.1 When a CLNP NPDU is received by an ATN router and that NPDU contains a security parameter in the globally unique format, and encodes security-related information according to §3.6.2.2 under the ATN security registration identifier, then the NPDU shall be forwarded according to the procedures specified below.

Note 1.— The CLNP NPDU header security parameter is used to indicate the traffic type of the application data contained in the NPDU and the application's routing policy requirements.

Note 2.— The procedures for handling an NPDU with any other format of security parameter, or with any other security registration identifier, are outside the scope of this specification.

3.3.2.2.3.2 *ATN operational communications traffic type – ATSC traffic category*

Note.— In this case, either no traffic type policy preference may be specified, or an ATSC class may be specified.

3.3.2.2.3.2.1 *No traffic type policy preference*

Note.— This case corresponds to a traffic type and associated routing policy security tag value of 000 00001.

3.3.2.2.3.2.1.1 If the NPDU contains a CLNP NPDU header security parameter in the globally unique format, and encodes:

a) security-related information according to 3.6.2.2 under the ATN security registration identifier; and

b) a traffic type of ATN operational communications and a traffic category of air traffic service communications; and

c) no traffic type policy preference;

then the NPDU shall be forwarded over the selected route to the NPDU's destination with the longest matching NSAP address prefix, and which contains a security path attribute comprising the ATN security registration identifier and security information that comprises:

i. an air-ground subnetwork security tag that has "ATN Operational Communications – Air Traffic Services Communications" in its set of permissible traffic types; or

ii. no air-ground subnetwork security tag;

and an ATSC class security tag indicating support of the lowest class out of all such routes available.

Note 1.— The requirement in 3.3.2.2.1.1 always takes precedence over selection based on ATSC class i.e. a route with a longer matching NSAP address prefix with a higher ATSC class is always preferred over a route with a lower ATSC class but with a shorter NSAP address prefix. This is essential for the avoidance of routing loops.

Note 2.— ATSC Class "H" is the lowest and Class "A" is the highest.

3.3.2.2.3.2.1.2 If no such route can be found, then the NPDU shall be discarded.

3.3.2.2.3.2.2 *ATSC class specified*

Note.— This case corresponds to traffic type and associated routing policy security tag values 000 10000 to 000 10111 inclusive.

3.3.2.2.3.2.2.1 If the NPDU contains a CLNP header security parameter in the globally unique format, and encodes:

a) security-related information according to 3.6.2.2 under the ATN security registration identifier; and

b) a traffic type of ATN operational communications and air traffic service communications traffic category; and

c) a requirement to route the NPDU over a route of a specified ATSC class;

then the NPDU shall be forwarded over the selected route to the NPDU's destination with the longest matching NSAP address prefix, and which contains a security path attribute comprising the ATN security registration identifier and security information that comprises:

i. an air-ground subnetwork security tag that has "ATN Operational Communications – Air Traffic Services Communications" in its set of permissible traffic types; or

ii. no air-ground subnetwork security tag;

and an ATSC class security tag indicating:

I. support of the required class, or a higher class; or

II. if no such route is available then, the route with the highest ATSC class available is chosen.

Note 1.— The requirement in 3.3.2.2.1.1 always takes precedence over selection based on ATSC class i.e. a route with a longer matching NSAP address prefix with a higher ATSC class is always preferred over a route with a lower ATSC class but with a shorter NSAP address prefix. This is essential for the avoidance of routing loops.

Note 2.— ATSC Class "H" is the lowest and Class "A" is the highest.

3.3.2.2.3.2.2.2 If no such route can be found then the NPDU shall be discarded.

3.3.2.2.3.2.2.3 If multiple routes are available which meet or exceed the required ATSC class, then the route with the lowest relative cost, i.e. actual monetary cost, shall be selected.

Note.— The actual monetary cost is determined through means outside the scope of this specification.

3.3.2.2.3.2.2.4 If the monetary cost is the same or unknown, then the hop count shall be used as the relative cost metric.

3.3.2.2.3.3 *ATN operational communications traffic type – AOC traffic category*

Note.— In this case, either no routing policy may be specified, or an air-ground subnetwork type may be specified, or an air-ground subnetwork order of preference may be specified.

3.3.2.2.3.3.1 *No traffic type policy preference*

Note.— This case corresponds to a traffic type and associated routing policy security tag value of 001 00001.

3.3.2.2.3.3.1.1 If the NPDU contains a CLNP header security parameter in the globally unique format, and encodes:

a) security-related information according to 3.6.2.2 under the ATN security registration identifier; and

b) a traffic type of ATN operational communications and aeronautical operational control traffic category; and

c) no traffic type policy preference;

then the NPDU shall be forwarded over the selected route to the NPDU's destination with the longest matching NSAP address prefix, and which contains a security path attribute comprising the ATN security registration identifier and security information that comprises:

i. an air-ground subnetwork security tag that has “ATN Operational Communications – Aeronautical Operational Control” in its set of permissible traffic types; or

ii. no air-ground subnetwork security tag;

and which does not contain an ATSC class security tag indicating support for only ATSC traffic.

3.3.2.2.3.3.1.2 If no such route can be found, then the NPDU shall be discarded.

3.3.2.2.3.3.2 *Air-ground subnetwork type specified*

Note 1.— This case corresponds to traffic type and associated routing policy security tag values 001 00010 through to 001 00110 inclusive.

Note 2.— The air-ground subnetworks that may be specified are: Gatelink, VDL, AMSS, HF and Mode S.

3.3.2.2.3.3.2.1 If the NPDU contains a CLNP header security parameter in the globally unique format, and encodes:

a) security-related information according to 3.6.2.2 under the ATN security registration identifier; and

b) a traffic type of ATN operational communications and aeronautical operational control traffic category; and

c) a requirement to route traffic only via a specific air-ground subnetwork only,

then the NPDU shall be forwarded over the selected route to the NPDU’s destination with the longest matching NSAP address prefix, and which contains a security path attribute comprising the ATN security registration identifier and security information that comprises either:

i. an air-ground subnetwork security tag that indicates that the route passes over that air-ground subnetwork and has “ATN Operational Communications — Aeronautical Operational Control” in its set of permissible traffic types; or,

ii. no air-ground subnetwork security tag;

and which does not contain an ATSC class security tag indicating support for only ATSC traffic.

3.3.2.2.3.3.2.2 If no such route can be found, then the NPDU shall be discarded.

3.3.2.2.3.3.3 *Air-ground subnetwork order of preference specified*

Note 1.— This case corresponds to traffic type and associated routing policy security tag values 001 00111 through to 001 01001 inclusive.

Note 2.— The air-ground subnetworks for which an order of preference may be specified are: Gatelink, VDL, AMSS, HF and Mode S.

3.3.2.2.3.3.3.1 If the NPDU contains a CLNP header security parameter in the globally unique format, and encodes:

a) security-related information according to 3.6.2.2 under the ATN security registration identifier; and

b) a traffic type of ATN operational communications and aeronautical operational control traffic category; and

c) a requirement to route traffic only via certain air-ground subnetworks and with a specified order of preference;

then the NPDU shall be forwarded over the selected route to the NPDU's destination with the longest matching NSAP address prefix, and which contains a security path attribute comprising the ATN security registration identifier and security information that comprises:

i. an air-ground subnetwork security tag that indicates that the route passes over the first preference air-ground subnetwork and has "ATN Operational Communications – Aeronautical Operational Control" in its set of permissible traffic types, if present; or

ii. an air-ground subnetwork security tag that indicates that the route passes over the second preference air-ground subnetwork and has "ATN Operational Communications – Aeronautical Operational Control" in its set of permissible traffic types, if present, and so on until a suitable route is found or no further preferences are specified; or

iii. no air-ground subnetwork security tag;

and which does not contain an ATSC class security tag indicating support for only ATSC traffic.

3.3.2.2.3.3.3.2 If no such route can be found, then the NPDU shall be discarded.

3.3.2.2.3.3.3.3 If after applying the above procedures, a more specific route is available to the NPDU's destination, but

1) the route has an air-ground subnetwork security tag that indicates that the route passes over a lower preference air-ground subnetwork; while

2) having "ATN Operational Communications – Aeronautical Operational Control" in its set of permissible traffic types; then

3) the more specific route shall be selected in preference to the less specific route.

Note.— The purpose of this requirement is to ensure that the NPDU is not forced to visit a default route provider only to find that a higher preference route does not actually exist to the NPDU's destination.

3.3.2.2.3.4 *ATN administrative communications traffic type*

Note.— This case corresponds to a traffic type and associated routing policy security tag value of 001 10000.

3.3.2.2.3.4.1 If the NPDU contains a CLNP header security parameter in the globally unique format, and encodes:

a) security-related information according to §3.6.2.2 under the ATN security registration identifier; and

b) a traffic type of ATN administrative communications;

then the NPDU shall be forwarded over the selected route to the NPDU's destination with the longest matching NSAP address prefix, and which contains a security path attribute comprising the ATN security registration identifier and security information that comprises:

i. either an air-ground subnetwork security tag that has “ATN Administrative Communications” in its set of permissible traffic types; or

ii. no air-ground subnetwork security tag;

and which does not contain an ATSC class security tag indicating support for only ATSC traffic.

3.3.2.2.3.4.2 If no such route can be found, then the NPDU shall be discarded.

3.3.2.2.3.5 *ATN systems management communications traffic type*

Note.— This case corresponds to a traffic type and associated routing policy security tag value of 011 00000.

3.3.2.2.3.5.1 If the NPDU contains a CLNP header security parameter in the globally unique format, and encodes:

a) security-related information according to 3.6.2.2 under the ATN security registration identifier; and

b) a traffic type of ATN systems management communications,

then the NPDU shall be forwarded over the selected route to the NPDU’s destination with the longest matching NSAP address prefix, and which:

1) contains a security path attribute comprising the ATN security registration identifier and security information that comprises:

a) either an air-ground subnetwork security tag that has “ATN Systems Management Communications” in its set of permissible traffic types; or

b) no air-ground subnetwork security tag;

or

2) contains no security path attribute.

3.3.2.2.3.5.2 If no such route can be found, then the NPDU shall be discarded.

3.3.3 The deployment of ATN components

3.3.3.1 Interconnection of ATN RDs

3.3.3.1.1 General

3.3.3.1.1.1 ATN RDs shall be interconnected by real subnetworks permitting communication between ATN routers for each of the interconnection scenarios specified below.

Note 1.— Examples of possible interconnections between ATN routing domains are illustrated in Figure 3-1.

Note 2.— There is no requirement for all ATN RDs to be fully interconnected.

3.3.3.1.1.2 Except for the interconnection of mobile RDs with other ATN RDs, the real subnetwork(s) used for such an interconnection shall be chosen by bilateral agreement and may be any subnetwork that complies with the provisions of §3.2.5.1.

Note 1.— For example, the chosen subnetwork may be a point-to-point communications link, a public or private PSDN providing the CCITT X.25 network access service, an Ethernet or an ISDN, etc.

Note 2.— The dynamic procedures for the interconnection of two ground-based ATN routers are specified in §3.3.4, and for interconnection of an air-ground and an airborne router in §3.3.5. The remainder of this section is concerned with static interconnection requirements.

3.3.3.1.2 Interconnection between members of an ATN island backbone RDC

When there is more than one ATN RD in an ATN island backbone RDC, each administration or aeronautical industry member that has elected to participate in that ATN island's backbone RDC shall ensure that its RD is either:

a) interconnected directly with all other ATN RDs within the ATN island's backbone RDC, over suitable and mutually agreeable real subnetwork(s); or

b) interconnected directly as in a), with one or more ATN RDs that are also members of the ATN island's backbone RDC, and which are able and willing to provide routes to the remaining RDs within the backbone RDC.

Note.— The existence of the ATN backbone RDC prohibits routes between its member RDs via other ATN RDs in the same ATN island.

3.3.3.1.3 Interconnection between members of an ATN island backbone RDC and other ATN RDs within the ATN island

ATN RDs within an ATN island RDC that are not members of the ATN island's backbone RDC, shall ensure that they are either:

a) interconnected directly with one or more ATN RDs that are members of the ATN island’s backbone RDC, over suitable and mutually agreeable real subnetworks; or

b) interconnected with one or more other ATN RDs that are members of the same ATN island RDC and which are able and willing to provide routes to and from one or more ATN RDs within the same ATN island’s backbone RDC, and to all destinations reachable via the ATN island's backbone RDC.

3.3.3.1.4 Interconnection of ATN islands

3.3.3.1.4.1 ATN islands shall only interconnect via ATN RDs which are members of each ATN island’s backbone RDC.

3.3.3.1.4.2 When an ATN RD is a member of more than one ATN island RDC, its routing policy shall not permit it to operate as a TRD between sources and destinations in different ATN islands unless the RD is a member of each island's backbone RDC.

3.3.3.1.5 Interconnection of mobile and fixed RDs

Note.— A mobile RD may interconnect concurrently with multiple ATN RDs which are attached to the common mobile subnetworks and which are accessible to the mobile RD at any given time. The purpose of such

interconnections is to provide data link communications services when required by ATN data link applications and other aeronautical or airline industry applications.

In order to meet the availability requirements of ATN data link applications, airborne and air-ground routers shall be capable of supporting multiple concurrent adjacencies with other routers.

Note 1.— These adjacencies are supported by multiple subnetwork connections at the same or different priorities, using the same or different air-ground subnetworks.

Note 2.— Dynamically, such adjacencies may be established and released in a "make before break" fashion permitting continuous communications availability, and for the suitability of a newly available adjacency to be determined before a no longer needed adjacency is released.

Note 3.— It is not within the scope of this specification to set minimum requirements in respect of the number of adjacencies and subnetwork connections that an airborne or air-ground router must support. Such requirements are dependent on the published coverage and number of air-ground subnetworks, application availability requirements and additionally, in the case of airborne routers, on airline operating policies. Implementors are advised to interpret "multiple" as, in the context of the above requirement, implying at least two adjacencies or connections, and, in practice, a larger number is anticipated as being the likely minimum requirement.

3.3.3.1.6 Interconnection of ATN RDs and non-ATN RDs

Note.— ATN RDs may interconnect with non-ATN RDs whether they are members of the same administrative domain or not.

3.3.4 Ground-ground interconnection

3.3.4.1 Interconnection scenarios

Note 1.— Ground-ground interconnection procedures apply to the interconnection of:

a) two ground-ground routers;

b) the interconnection of an air-ground router and a ground-ground router.

Note 2.— Formally, these procedures only apply to interconnection between ATN routers in different administrative domains. However, in practice, they are also applicable to interconnection scenarios within the same administrative domain.

3.3.4.2 Ground interconnection of ATN routers

3.3.4.2.1 When the network administrators agree to the ground-ground interconnection of one or more ATN routers within their respective administrative domains, they shall:

a) make available suitable subnetwork connectivity including, where necessary the physical installation of suitable communications equipment for end-to-end communications between the ATN routers that supports the Quality of Service necessary for the applications data that will be routed over this interconnection;

Note 1.— The choice of appropriate subnetwork(s) to support the interconnection is a matter for bilateral agreement between network administrators, including agreement on responsibility for installation, operating and maintenance costs, and fault management.

Note 2.— Either connectionless or connection mode subnetworks may be used.

b) using global or local systems management mechanisms, append the NET of the remote ATN router to the **externalBISNeighbor** attribute of the BIS's **idrpConfig** MO;

c) using global or local systems management mechanisms, create an **AdjacentBIS** managed object (MO) in each ATN router to represent the other ATN router.

Note.— By bilateral agreement, one of the BISs may be configured to listen for incoming BIS OPEN PDUs by setting the ListenForOpen MO attribute to true.

3.3.4.2.2 Route initiation

Note.— Route initiation is defined to be the point at which routing information exchange can begin, and the route initiation procedures are those that permit the exchange of routing information to commence.

3.3.4.2.2.1 *Connection mode subnetworks*

3.3.4.2.2.1.1 Using global or local systems management mechanisms, a network manager shall establish one or more subnetwork connections between the two ATN routers.

Note 1.— Typically (e.g. with X.25), one ATN router will be placed in a state where it will accept an incoming connection from the other ATN router, and then the other ATN router is stimulated to initiate one or more subnetwork connection(s) to the other ATN router.

Note 2.— Multiple concurrent subnetwork connections over the same or different subnetworks may be required in order to meet throughput and other QoS requirements.

3.3.4.2.2.1.2 Using global or local systems management mechanisms, a network manager shall ensure that the forwarding information base in each ATN router, used to support the connectionless network protocol specified in 3.6, contains sufficient information to forward CLNP NPDUs addressed to the NET of the other ATN router over the newly established subnetwork connection(s).

Note.— This step is necessary to ensure that the connection mode subnetwork can be used to exchange the BISPDUs of IDRP.

3.3.4.2.2.1.3 Using global or local systems management mechanisms, a network manager shall invoke the activate action on each **AdjacentBIS** managed object in order to initiate a BIS-BIS connection between the two ATN routers.

3.3.4.2.2.2 *Connectionless subnetworks*

Note 1.— Connectionless subnetworks include Ethernets and IP subnetworks.

Note 2.— The subnetwork does not provide an explicit indication that a communications path is available.

3.3.4.2.2.2.1 Using global or local systems management mechanisms, a network manager shall ensure that the forwarding information base in each ATN router, used to support the connectionless network protocol specified in 3.6, contains sufficient information to forward CLNP NPDUs addressed to the NET of the other ATN router via the connectionless subnetwork.

Note.— This step is necessary to ensure that the connectionless subnetwork can be used to exchange the BISPDUs of IDRP.

3.3.4.2.2.2.2 Using global or local systems management mechanisms, a network manager shall invoke the activate action on each **AdjacentBIS** managed object in order to initiate a BIS-BIS connection between the two ATN routers.

3.3.4.2.2.2.3 For each such adjacency, and by bilateral agreement:

a) one BIS should be configured with the "ListenForOpen" MO attribute set to true and the activate action invoked on the **AdjacentBIS** MO either on system initiatization or when a network manager wishes to enable the adjacency; and

b) the activate action should be periodically invoked on the corresponding **AdjacentBIS** managed object in the other BIS.

Note 1.— Periodically generating activate actions in this manner will cause the BIS-BIS connection to "come up" automatically within a short time of the communications path being available.

Note 2.— The activate action has no effect when a BIS-BIS connection is established.

3.3.4.3 Ground-ground routing information exchange

3.3.4.3.1 Routing information shall be exchanged using the ISO/IEC 10747 inter-domain routing protocol according to the profile specified in ¶3.8.

3.3.4.3.2 In support of air-ground communications, the exchange of routing information shall be subject to appropriate routing policies specified in ¶3.3.7.1, ¶3.3.7.3 or ¶3.3.7.4, depending upon the role of the routing domain in which each ATN router is located.

3.3.4.4 Ground-ground route termination

Note 1.— Route termination is defined to be the point at which routing information ceases to be exchanged between two ATN routers, and, in consequence, the routes made available over the adjacency cease to be usable and must be withdrawn. The route termination procedures are those procedures which terminate the exchange of routing information.

Note 2.— Route termination may result from a failure in the underlying subnetwork(s) causing a loss of communication between the two ATN routers. Alternatively, it may result from a deliberate decision of network administrators to terminate the interconnection, either temporarily or permanently.

Note 3.— No special recovery procedures are specified if route termination is due to a network fault. Once the fault has been repaired, the procedures of ¶3.3.4.2 may be re-invoked, as appropriate to re-establish communication, and to exchange routing information.

3.3.4.4.1 When a network administrator decides to temporarily or permanently terminate an interconnection between two ATN routers then, using global or local systems management mechanisms applied to either or both of the two ATN routers, the deactivate action shall be invoked on the AdjacentBIS MO that represents the remote ATN router with which the BIS-BIS connection is to be terminated.

3.3.4.4.2 If the adjacency is to be permanently terminated, then the AdjacentBIS MO shall also be deleted, and the forwarding information base shall be updated to remove the route to the NET of the remote ATN router.

3.3.4.4.3 For either temporary or permanent termination, and if required, by using global or local systems management mechanisms, the network administrator(s) shall also terminate any underlying subnetwork connections.

3.3.5 Air-ground interconnection

3.3.5.1 Interconnection scenarios

Note 1.— Air-ground interconnection applies to the interconnection between an ATN airborne router and an ATN air-ground router over one or more mobile subnetworks.

Note 2.— The significant difference between air-ground and ground-ground interconnection is that in the former case interconnection is automatic and consequential on the availability of communications and local policy, while, in the latter case, interconnection is a deliberate and planned action with the direct involvement of network administrators.

Note 3.— While IDRP is also intended to be used over air-ground interconnections, as an interim measure, the optional non-use of IDRP over air-ground interconnections is permitted by this specification and according to 3.3.5.2.12.

Note 4.— For the purposes of this specification, the functional model of an ATN router illustrated in Figure 3-3 is assumed. This model illustrates the basic functional entities in an ATN air-ground (Class 5 router) and ATN airborne router with IDRP (Class 6 router), the data flow between them as solid lines, and the flow of certain events and control information, by dashed lines.

Note 5.— Figure 3-3 introduces a new architectural entity, the Intermediate System – Systems Management Entity (IS-SME). As specified below, this plays an important role in the realization of route initiation in air-ground operations, by responding to changes in subnetwork connectivity and thereby controlling the route initiation and termination procedures.

Note 6.— The ATSC class assigned to an air-ground subnetwork and the traffic type(s) allowed to pass over this air-ground subnetwork are known a priori to the air-ground router attached to each such subnetwork. They are communicated to an airborne router using the options part of an ISO/IEC 9542 ISH PDU which is uplinked to the airborne router as part of the route initiation procedure as described in 3.3.5.2.

3.3.5.2 Air-ground route initiation

3.3.5.2.1 General

3.3.5.2.1.1 BIS-BIS communications over a mobile subnetwork shall be either air-initiated or ground-initiated, with one of these two modes of operation selected for all instances of a given subnetwork type.

Note 1.— Three classes of procedures are distinguished by this specification. These are: (a) air-initiated i.e. when the airborne router initiates the procedure, (b) ground-initiated i.e. when the air-ground router initiates the procedure, and (c) air- or ground-initiated i.e. when either the airborne or the air-ground router may initiate the procedure.

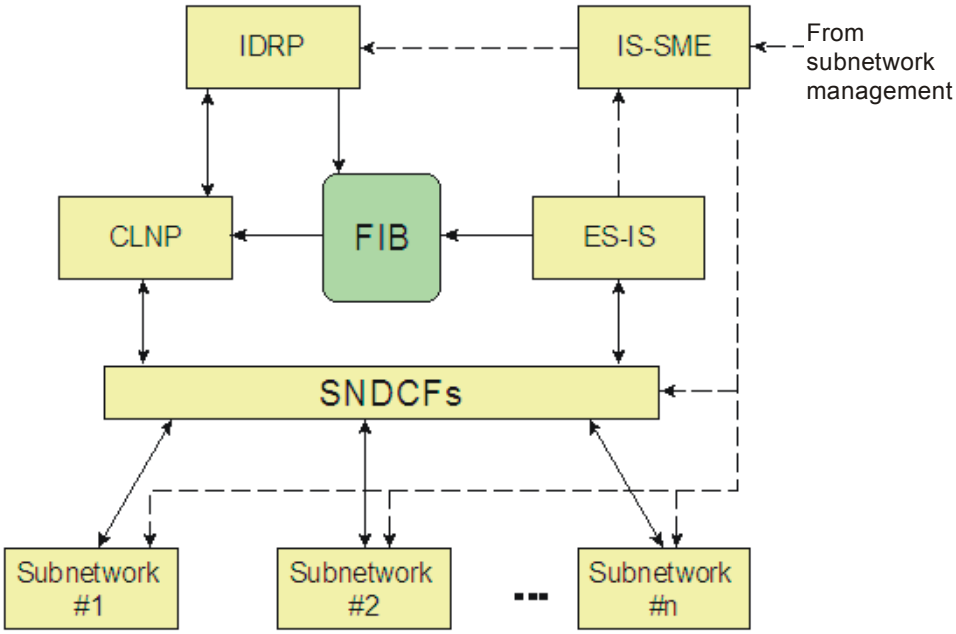


Figure 3-3. Assumed ATN router architecture for air-ground route initiation

Note 2.— For a given mobile subnetwork type, the use of air-initiated or ground-initiated procedures, and the implementation of join events is outside of the scope of this specification and is a matter for the relevant ICAO manual.

Note 3.— The interfaces to all mobile subnetworks are assumed to be compatible with ISO/IEC 8208. The ISO/IEC 8208 term data terminal equipment (DTE) is also used in this specification to refer to a system attached to a mobile subnetwork.

3.3.5.2.1.2 For air-initiated subnetworks, airborne routers shall comply with the procedures specified in 3.3.5.2.3.2, and air-ground routers shall comply with the procedures specified in 3.3.5.2.2.

3.3.5.2.1.3 For ground-initiated subnetworks, air-ground routers shall comply with the procedures specified in 3.3.5.2.4, and airborne routers shall comply with the procedures specified in 3.3.5.2.2.

3.3.5.2.1.4 For air or ground-initiated subnetworks, air-ground and airborne routers shall comply with the procedures specified in 3.3.5.2.2 and 3.3.5.2.5.

3.3.5.2.1.5 Air-ground subnetworks accessed using a network access service compatible with ISO/IEC 8208 shall use the mobile SNDCF specified in 3.7.4 for providing the SN-Service required by ISO/IEC 8473.

3.3.5.2.1.6 Other types of air-initiated air-ground subnetworks shall use the frame mode SNDCF specified in 3.7.8 for providing the SN-Service required by ISO/IEC 8473.

Note 1.— This SNDCF applies only to air-initiated subnetworks.

Note 2.— The frame mode SNDCF is generally applicable to air-ground data links. However, this does not exclude the possibility of introducing further SNDCFs for use of mobile subnetworks.

3.3.5.2.2 Route initiation procedures for a responding ATN router

3.3.5.2.2.1 *ISO/IEC 8208 subnetworks*

Note 1.— Route initiation is always asymmetric with a clearly defined initiator and responder. In all cases, the ATN router in the responder role, follows the same procedures, as specified below.

Note 2.— For air-initiated route initiation, the air-ground router is the responding ATN router. For ground-initiated route initiation, the airborne router is the responding ATN router.

3.3.5.2.2.1.1 Each ATN router that is specified to take the responder role for a given mobile subnetwork type, and when attached to a subnetwork of that subnetwork type, shall be configured into a state whereby it “listens” for call indications on that subnetwork.

3.3.5.2.2.1.2 For each call indication received, a responding ATN router shall, based on local policy, either:

a) accept the incoming call immediately using a call accept packet; or

b) validate the calling DTE address and either accept the call using a call accept packet, or if the call is unacceptable then it shall be rejected using a clear request packet.

Note 1.— The procedures used to validate the calling DTE address and to determine the acceptability of the call are outside the scope of this specification.

Note 2.— The number of simultaneous virtual circuits that the ATN router needs to support will be subject to an implementation limit that needs to be sufficient for the role in which the ATN router is deployed.

3.3.5.2.2.1.3 When a subnetwork connection is successfully established, then the procedures of 3.3.5.2.6 shall be applied to that subnetwork connection.

3.3.5.2.2.2 *Other subnetwork types*

Note.— Other subnetwork types make use of the air-ground communications service (A/GCS) to support communications over the subnetwork and to support the provision of the SN-Service.

3.3.5.2.2.2.1 Each ATN router specified to take a responder role for the subnetwork type shall be configured into a state whereby it listens for incoming A/GCS data link communications protocol (DLCP) data link start messages.

3.3.5.2.2.2.2 For each incoming A/GCS DLCP data link start message received, a responding ATN router shall, based on local policy:

a) accept the data link start immediately by returning its own data link start; or

b) validate the subnetwork address of the initiating system and either accept the data link start or reject it according to the specified DLCP procedures.

Note.— The rules for validation of the subnetwork address are outside of the scope of this specification.

3.3.5.2.2.2.3 The data link shall be made available for user data exchange according to the provisions of the frame mode SNDCF specified in ⁋3.7.8.

3.3.5.2.3 Air-initiated route initiation

Note.— This section specifies the procedures to be used by an airborne router for air-initiated route initiation.

3.3.5.2.3.1 *Airborne router procedures*

3.3.5.2.3.1.1 *General*

Note 1.— The connectivity information is provided as a "join event". This is an event generated by a mobile subnetwork when it is recognized that a system has attached to the subnetwork and is available for communication using the subnetwork. The join event provides the subnetwork address of the newly available system. It may also include other subnetwork specific information needed to route a call to that subnetwork address. For example, in the case of a VDL subnetwork, the call may need to be directed via a specific ground station and hence the ground station address must be provided in addition to the subnetwork address.

Note 2.— An actual implementation of a join event may concatenate several distinct join events as defined above into a single message.

Note 3.— For air-initiated subnetworks, the join event is received by the IS-SME in the airborne router. The mechanism by which it is received is both subnetwork and implementation dependent and is outside of the scope of this specification.

Note 4.— In certain subnetwork environments, for example in areas of poor signal strength, it is possible that join and leave events are generated frequently until either the signal is lost completely or becomes strong enough to maintain a service. Some mobile subnetworks have internal mechanisms to suppress the over-generation of join/leave events, but some do not.

3.3.5.2.3.1.1.1 On receipt of a join event from an ISO/IEC 8208 subnetwork with internal mechanisms to suppress the over-generation of join/leave events, the airborne router shall process that join event as described in ⁋3.3.5.2.3.1.2.1.

3.3.5.2.3.1.1.2 On receipt of a join event from a non-ISO/IEC 8208 subnetwork with internal mechanisms to suppress the over-generation of join/leave events, the airborne router shall process that join event as described in ⁋3.3.5.2.3.1.3.1.

3.3.5.2.3.1.1.3 For subnetworks that do not have internal mechanisms to suppress the over-generation of join/leave events, a local timer t_{le} shall be activated upon receipt of each leave event and the following procedure used on receipt of join events:

a) if timer t_{le} is not active, the airborne router processes the join event as described in ⁋3.3.5.2.3.1.2.1 for ISO/IEC 8208 subnetworks or ⁋3.3.5.2.3.1.3.1 for non-ISO/IEC 8208 subnetworks, respectively;

b) if timer t_{le} is active, the airborne router postpones processing of the join event; and then

   1) if a further leave event for the same reported DTE address from that mobile subnetwork is received before timer t_{le} expires, then the join event is discarded without further action; or

Note.— On receipt of the subsequent leave event, timer t_{le} would be restarted.

2) if timer t_{le} expires without a further leave event for the same reported DTE address arriving from the same mobile subnetwork, then the airborne router recommences processing of the join event as described in ¶3.3.5.2.3.1.2.1 for ISO/IEC 8208 subnetworks or ¶3.3.5.2.3.1.3.1 for non-ISO/IEC 8208 subnetworks, respectively.

3.3.5.2.3.1.1.4 The timer t_{le} defined in ¶3.3.5.2.3.1.1.3 should be configurable within the range of 0 to 1 000 seconds to enable performance optimization.

Note 1.— A different value of timer t_{le} is likely to be appropriate for different subnetwork types.

Note 2.— The value of timer t_{le} directly affects the speed of processing of join events and thus route availability. The value may need to take into account the availability of other subnetworks and a shorter value used if another subnetwork is not available.

3.3.5.2.3.1.2 *ISO/IEC 8208 subnetworks*

3.3.5.2.3.1.2.1 The airborne router shall process a join event by either:

a) issuing an ISO/IEC 8208 call request with the DTE address reported by the join event as the called address; or

b) validating the DTE address reported by the join event as to whether or not a subnetwork connection with it is acceptable according to local routing policy. If such a connection is acceptable then an ISO/IEC 8208 call request is issued with the DTE address reported by the join event as the called address. Otherwise, the join event is ignored.

Note.— The airborne router validates the DTE address that is the subject of the join event and determines the acceptability of a subnetwork connection with the so identified ATN router, using procedures outside of the scope of this specification.

3.3.5.2.3.1.2.2 On receipt of a call connected packet, and if the called line address modified notification optional user facility is used in the received packet and indicates that the returned called address is different from that used in the call request packet, and the subnetwork also generates “Handoff” events (see ¶3.3.5.2.14), then the IS-SME shall store the relationship between the originally called DTE address and the returned called address in the same local database. The knowledge of this relationship shall be retained as long as a subnetwork connection exists with the DTE.

3.3.5.2.3.1.2.3 When a subnetwork connection is successfully established, then the procedures of ¶3.3.5.2.6 shall be applied to that subnetwork connection.

3.3.5.2.3.1.3 *Non-ISO/IEC 8208 subnetworks*

3.3.5.2.3.1.3.1 On receipt of a join event, the airborne router shall either:

a) send an A/GCS DLCP data link start message to the identified subnetwork address; or

b) validate the subnetwork address reported by the join event as to whether or not a data link with it is acceptable according to local policy. If such a connection is acceptable then an A/GCS DLCP data link start message is issued to the identified subnetwork address. Otherwise, the join event shall be ignored.

Note.— The rules for validation of the subnetwork address are outside of the scope of this specification.

3.3.5.2.3.1.3.2 On receipt of a data link start returned in response to the above data link start, the data link shall be made available for user data exchange according to the provisions of the frame mode SNDCF specified in 3.7.8.

3.3.5.2.3.1.3.3 The procedures of 3.3.5.2.6 shall be applied.

3.3.5.2.4 Ground-initiated route initiation

Note 1.— Ground-initiated route initiation is only appropriate for mobile subnetworks that originate a join event from their ground component.

Note 2.— For ground-initiated subnetworks, the join event is received by the IS-SME in the air-ground router. The mechanism by which it is received is both subnetwork and implementation dependent and is outside of the scope of this specification.

Note 3.— In certain subnetwork environments, for example in areas of poor signal strength, it is possible that join and leave events are generated frequently until either the signal is lost completely or becomes strong enough to maintain a service. Some mobile subnetworks have internal mechanisms to suppress the over-generation of join/leave events, but some do not.

3.3.5.2.4.1 On receipt of a join event from a subnetwork with internal mechanisms to suppress the over-generation of join/leave events, the air-ground router shall process that join event as described in 3.3.5.2.4.3.

3.3.5.2.4.2 For subnetworks that do not have internal mechanisms to suppress the over-generation of join/leave events a local timer t_{le} shall be activated upon receipt of each leave event and the following procedure used on receipt of join events:

a) if timer t_{le} is not active, the air-ground router processes the join event as described in 3.3.5.2.4.3;

b) if timer t_{le} is active, the air-ground router postpones processing of the join event; and then

1) if a further leave event for the same reported DTE address from that mobile subnetwork is received before timer t_{le} expires, then the join event is discarded without further action; or

Note.— On receipt of the subsequent leave event, timer t_{le} would be restarted.

2) if timer t_{le} expires without a further leave event for the same reported DTE address arriving from the same mobile subnetwork, then the air-ground router recommences processing of the join event as described in 3.3.5.2.4.3.

3.3.5.2.4.3 The air-ground router shall process a join event by either:

a) issuing an ISO/IEC 8208 call request with the DTE address reported by the join event as the called address; or

b) validating the DTE address reported by the join event as to whether or not a subnetwork connection with it is acceptable according to local routing policy. If such a connection is acceptable then an ISO/IEC 8208 call request is issued with the DTE address reported by the join event as the called address. Otherwise, the join event is ignored.

Note.— Option (b) above permits an administration or organization operating a ground-initiated mobile subnetwork to implement procedures, according to its local policy, whereby an air-ground router may validate the DTE that is the subject of the join event and hence determine the acceptability of a subnetwork connection with the so

identified airborne router. The purpose of this facility is to enable efficient management of the available subnetwork resources in areas of overlapping coverage. This facility is not appropriate when its use may result in an aircraft being denied air-ground data communications.

3.3.5.2.4.4 The timer t_{le} defined in 3.3.5.2.4.2 should be configurable within the range of 0 to 1 000 seconds to enable performance optimization.

Note 1.— A different value of timer t_{le} is likely to be appropriate for different subnetwork types.

Note 2.— The value of timer t_{le} directly affects the speed of processing of join events and thus route availability. The value may need to take into account the availability of other subnetworks and a shorter value used if another subnetwork is not available.

3.3.5.2.4.5 On receipt of a call connected packet, and if the called line address modified notification optional user facility is used in the received packet and indicates that the returned called address is different from that used in the call request, and the subnetwork also generates "Handoff" events (see 3.3.5.2.14), then the IS-SME shall store the relationship between the originally called DTE address and the returned called address in the same local database. The knowledge of this relationship shall be retained as long as a subnetwork connection exists with the DTE.

3.3.5.2.4.6 When a subnetwork connection is successfully established, then the procedures of 3.3.5.2.6 shall be applied to that subnetwork connection.

3.3.5.2.5 Air or ground-initiated route initiation

Note 1.— Air or ground-initiated route initiation is only appropriate for mobile subnetworks that do provide connectivity information through a join event to the airborne or air-ground router, or both.

Note 2.— For air or ground-initiated subnetworks, the join event is received by the IS-SME in the airborne or air-ground router, respectively. The mechanism by which it is received is both subnetwork and implementation dependent.

Note 3.— In certain subnetwork environments, for example in areas of poor signal strength, it is possible that join and leave events are generated frequently until either the signal is lost completely or becomes strong enough to maintain a service. Some mobile subnetworks have internal mechanisms to suppress the over-generation of join/leave events, but some do not.

3.3.5.2.5.1 On receipt of a join event from a subnetwork with internal mechanisms to suppress the over-generation of join/leave events, the ATN router shall process that join event as described in 3.3.5.2.5.3.

3.3.5.2.5.2 For subnetworks that do not have internal mechanisms to suppress the over-generation of join/leave events, a local timer t_{le} shall be activated upon receipt of each leave event and the following procedure used on receipt of join events:

a) if timer t_{le} is not active, the ATN router processes the join event as described in 3.3.5.2.5.3;

b) if timer t_{le} is active, the ATN router postpones processing of the join event; and then

1) if a further leave event for the same reported DTE address from that mobile subnetwork is received before timer t_{le} expires, then the join event is discarded without further action; or

Note.— On receipt of the subsequent leave event, timer t_{le} would be restarted.

2) if timer t_{le} expires without a further leave event for the same reported DTE address arriving from the same mobile subnetwork, then the ATN router recommences processing of the join event as described in 3.3.5.2.5.3.

3.3.5.2.5.3 The ATN router shall process a join event by either:

a) issuing an ISO/IEC 8208 call request with the DTE address reported by the join event as the called address; or

b) validating the DTE reported by the join event as to whether or not a subnetwork connection with it is acceptable according to local routing policy. If such a connection is acceptable then an ISO/IEC 8208 call request is issued with the DTE address reported by the join event as the called address. Otherwise, the join event is ignored.

Note.— The ATN router validates the DTE address that is the subject of the join event and determines the acceptability of a subnetwork connection with the so identified ATN router, using procedures outside the scope of this specification.

3.3.5.2.5.4 The timer t_{le} defined in 3.3.5.2.5.2 should be configurable within the range of 0 to 1 000 seconds to enable performance optimization.

Note 1.— A different value of timer t_{le} is likely to be appropriate for different subnetwork types.

Note 2.— The value of timer t_{le} directly affects the speed of processing of join events and thus route availability. The value may need to take into account the availability of other subnetworks and a shorter value used if another subnetwork is not available.

3.3.5.2.5.5 On receipt of a call connected packet, and if the called line address modified notification optional user facility is used in the received packet and indicates that the returned called address is different from that used in the call request, and the subnetwork also generates “Handoff” events (see 3.3.5.2.14), then the IS-SME shall store the relationship between the originally called DTE address and the returned called address in the same local database. The knowledge of this relationship shall be retained as long as a subnetwork connection exists with the DTE.

3.3.5.2.5.6 When a subnetwork connection is successfully established, then the procedures of 3.3.5.2.6 shall be applied to that subnetwork connection.

Note.— When a call collision occurs, then the call collision resolution procedures are applied by the SNDCF in order to ensure that only a single virtual circuit is established and that connection initiator and responder are unambiguously identified.

3.3.5.2.6 Exchange of configuration information using the ISO/IEC 9542 ISH PDU

3.3.5.2.6.1 ATN airborne and air-ground routers shall implement the ISO/IEC 9542 “Configuration Information” function for use over each mobile subnetwork that they support.

3.3.5.2.6.2 Whenever a subnetwork connection is established over a mobile subnetwork, the ISO/IEC 9542 ”Report Configuration” function shall be invoked in order to send an ISH PDU containing the NET of the airborne or air-ground router network entity over the subnetwork connection.

Note.— As specified in 3.8.2.1.3, the ISH PDU exchange is also used by the air-ground and airborne router to inform each other about the extended capabilities which they support over the air-ground link.

3.3.5.2.6.3 In the case of an airborne router, if it supports the use of IDRP for the exchange of routing information over this subnetwork, then the SEL field of the NET inserted into the ISH PDU shall always be set to 00h (i.e. a binary pattern of all zeroes).

3.3.5.2.6.4 Alternatively, if the airborne router implements the procedures for the optional non-use of IDRP over this subnetwork, then the SEL field of the NET inserted into the ISH PDU shall always be set to FEh (i.e. a binary pattern of 1111 1110).

3.3.5.2.6.5 *Encoding of ATN data link capability parameter*

3.3.5.2.6.5.1 ATN air-ground and airborne routers shall include the ATN data link capabilities parameter, as defined in 3.8.2.1.3, in the options part of the ISH PDU.

Note.— Interoperability with ATN air-ground and airborne routers which comply with previous editions of this specification is maintained. These routers will ignore by definition any unknown parameter contained in a received ISO/IEC 9542 ISH PDU, but they will not discard the received PDU.

3.3.5.2.6.5.2 An ATN air-ground router shall set bit 0 of the ATN data link capabilities parameter value field to one indicating its capability to generate and forward UPDATE PDUs without air-ground subnetwork type security tag(s) to adjacent airborne routers.

3.3.5.2.6.5.3 An ATN airborne router which supports the use of IDRP for the exchange of routing information (i.e. a Class 6 airborne router) shall set bit 0 of the ATN data link capabilities parameter value field to one indicating its capability to receive and process UPDATE PDUs without air-ground subnetwork type security tag(s).

Note.— Information on traffic type(s) permitted to pass over a mobile subnetwork and supported ATSC class(es) which is normally conveyed in the air-ground subnetwork type security tag(s) is available to the airborne router as a result of the uplinked mobile subnetwork capability parameter.

3.3.5.2.6.6 An ATN air-ground router shall include the mobile subnetwork capabilities parameter, as defined in 3.8.2.1.3, in the options part of the uplinked ISH PDU, indicating any restrictions on traffic types permitted to pass over the mobile subnetwork and the ATSC class of the mobile subnetwork, if the ATN operational communications traffic type – Air Traffic Service communications traffic category is among the permissible traffic types for this mobile subnetwork.

Note 1.— The ATSC class assigned to a mobile subnetwork and the traffic type(s) allowed to pass over this mobile subnetwork are uplinked to the airborne router to enable this router to make the appropriate routing decision when downlinking packets over an air-ground adjacency which is made up of more than one mobile subnetwork.

Note 2.— The ISH PDU is only ever sent in the context of a single mobile subnetwork between the air-ground and airborne router. Thus the capability information carried in the mobile subnetwork capabilities parameter is unambiguously associated with this subnetwork.

3.3.5.2.6.7 When in the initiator role for:

a) an ISO/IEC 8208 subnetwork, an ATN router should use the ISO/IEC 8208 “Fast Select” facility, if supported by the subnetwork, and encode the first ISH PDU in the call request user data, according to the procedures for the mobile SNDCF specified in Chapter 3.7;

b) other types of subnetworks, an ATN router should use the data link start DLCP user data facility to exchange the first ISH PDU.

3.3.5.2.6.8 When in the responder role for:

a) an ISO/IEC subnetwork, and the initiator has proposed use of the fast select facility, the ATN router should encode the first ISH PDU in the call accept user data, according to the procedures for the mobile SNDCF specified in Chapter 3.7;

b) other types of subnetworks, an ATN router should use the data link start DLCP user data facility to exchange the first ISH PDU.

Note.— The purpose of encoding an ISH PDU in call request or call accept user data or as DLCP user data is to minimize the number of messages sent over limited bandwidth mobile subnetworks and the time taken to complete the route initiation procedures.

3.3.5.2.6.9 Whenever an ISO/IEC 9542 ISH PDU is received by an airborne router, this router shall evaluate the mobile subnetwork capabilities parameter contained in the options part of the received ISH PDU.

3.3.5.2.6.10 The airborne router shall use the received subnetwork capability information to update its local configuration data concerning the permissible traffic type(s) and the supported ATSC class of the mobile subnetwork over which the ISH PDU was received.

3.3.5.2.6.11 Whenever an ISO/IEC 9542 ISH PDU is received, either as call request, call accept or DLCP user data, or as data sent over the connection, the ISO/IEC 9542 record configuration function shall be invoked and the routing information necessary for NPDUs to be sent over the subnetwork connection shall be written into the forwarding information base for use by ISO/IEC 8473.

3.3.5.2.6.12 A systems management notification shall be generated to report the arrival of the ISH PDU to the ATN router's IS-SME.

3.3.5.2.7 Validation of the received NET

3.3.5.2.7.1 The IS-SME shall, using the received NET to identify the remote ATN router, validate the acceptability of a BIS-BIS connection with that remote ATN router.

3.3.5.2.7.2 If a BIS-BIS connection is unacceptable, then a clear request shall be generated to terminate the subnetwork connection. Forwarding information associated with the subnetwork connection shall be removed from the forwarding information base.

Note.— The acceptability of a BIS-BIS connection with the ATN router identified by the received NET is determined using procedures outside of the scope of this specification.

3.3.5.2.7.3 If a BIS-BIS connection is acceptable, then an air-ground router shall apply the procedures of 3.3.5.2.8, and an airborne router shall apply the procedures of 3.3.5.2.9.

3.3.5.2.8 Determination of the routing information exchange procedure by an air-ground router

When the arrival of the ISH PDU is reported to the IS-SME of an air-ground router, then the SEL field of the NET contained in this ISH PDU shall be inspected:

a) if the SEL field takes the value of 00h (i.e. a binary pattern of all zeroes), then this shall be taken to imply that the airborne router that sent this ISH PDU supports the use of IDRP for the exchange of routing information. The procedures of 3.3.5.2.10 shall be applied;

b) if the SEL field takes the value of FEh (i.e. a binary pattern of 1111 1110), then this shall be taken to imply that the airborne router that sent this ISH PDU supports the procedures for the optional non-use of IDRP for the exchange of routing information. The procedures of ⁋3.3.5.2.12 shall be applied.

3.3.5.2.9 Determination of the routing information exchange procedure by an airborne router

When the arrival of the ISH PDU is reported to the IS-SME of an airborne router, then if the airborne router supports the use of IDRP for the exchange of routing information, then the procedures of ⁋3.3.5.2.10 shall be applied. If the airborne router supports the procedures for the optional non-use of IDRP for the exchange of routing information, then the procedures of ⁋3.3.5.2.12 shall be applied.

3.3.5.2.10 Establishment of a BIS-BIS connection

3.3.5.2.10.1 The IS-SME shall append the NET received on the ISH PDU to the externalBISNeighbor attribute of the BIS's idrpConfig managed object, if not already present, and create an adjacentBIS managed object for the remote ATN router identified by this NET, if one does not already exist.

3.3.5.2.10.2 If the ISH PDU was received from a subnetwork connection or data link which was established with the local ATN router in the responder role, then an IDRP activate action shall be invoked to start the BIS-BIS connection according to ISO/IEC 10747, if such a BIS-BIS connection does not already exist.

3.3.5.2.10.3 If the ISH PDU was received from a subnetwork connection or data link which was established with the local ATN router in the initiator role, then no IDRP activate action shall be invoked, but the ListenForOpen MO attribute shall be set to true if a BIS-BIS connection does not already exist.

Note.— This procedure minimizes the route initiation exchanges over a bandwidth limited mobile subnetwork. The reversal of initiator and responder roles for the BIS-BIS connection compared with the subnetwork connection ensures the fastest route initiation procedure.

3.3.5.2.10.4 If a BIS-BIS connection was already established with the remote ATN airborne router, then the IS-SME of the air-ground router shall cause:

a) the update of the security path attribute’s security information of all routes contained in the Adj-RIB-In associated with the remote ATN airborne router; and

b) the IDRP routing decision function to be invoked in order to rebuild the FIB, the Loc_RIB and relevant Adj-RIB-Out(s) taking into account the additional subnetwork connectivity.

3.3.5.2.10.5 If a BIS-BIS connection was already established with the remote ATN air-ground router, then the IS-SME of the airborne router shall cause the IDRP routing decision function to be invoked in order to rebuild the FIB, the Loc-RIB and relevant Adj-RIB-Out(s) taking into account the additional subnetwork connectivity.

3.3.5.2.10.6 Furthermore the air-ground router shall re-advertise all routes affected by the change in subnetwork connectivity that are contained in the Adj-RIB-Out associated with the remote ATN airborne router subsequent to the update of the security path attribute’s security information of these routes as specified in ⁋3.8.

Note.— When a change in the mobile subnetwork connectivity occurs over an adjacency with an airborne router that has signalled its capability to support UPDATE PDUs without air-ground subnetwork type security tag, the security path attribute's security information of the routes contained in the Adj-RIB-Out associated with the remote airborne router is not updated (see ⁋3.8.3.2.4.2.8). As a consequence, these routes are not affected by the changes and do not need to be re-advertised to the airborne router.

3.3.5.2.10.7 The IS-SME shall also ensure that the procedures for the optional non-use of IDRP are not concurrently being applied to routing information exchange with an ATN router with the same NET over a different subnetwork connection.

3.3.5.2.10.8 This is an error and shall be reported to systems management; a BIS-BIS connection shall not be established in this case.

3.3.5.2.10.9 When IDRP is used to exchange routing information over an air-ground subnetwork, the value of the holding time field in the ISH PDU should be set to 65534.

3.3.5.2.10.10 When IDRP is used to exchange routing information over an air-ground subnetwork, the configuration timer should be set such that no further ISH PDUs are exchanged following the route initiation procedure.

Note 1.— The purpose of the above is to effectively suppress the further generation of ISH PDUs.

Note 2.— Normally, the IDRP KeepAlive mechanism is sufficient to maintain a check on the "liveness" of the remote ATN router. However, when watchdog timers are necessary it is also necessary to ensure a "liveness" check on a per subnetwork connection basis. The ISH PDU fulfils this role.

3.3.5.2.11 Exchange of routing information using IDRP

3.3.5.2.11.1 Once a BIS-BIS connection has been established with a remote ATN router, then:

a) an airborne router shall advertise routes to the air-ground router in accordance with the routing policy specified in 3.3.7.2;

b) an air-ground router shall advertise routes to the airborne router in accordance with the routing policy specified in 3.3.7.1.4 or 3.3.7.3.4 as appropriate for the role of the air-ground router's RD.

3.3.5.2.11.2 On receipt of an UPDATE PDU from an air-ground router which has signaled its capability to generate UPDATE PDUs without air-ground subnetwork type security tag(s), an airborne router shall invoke the IDRP routing decision function in order to rebuild its FIB, Loc_RIB and relevant Adj-RIB-Out(s) taking into account both the routing information contained in the received UPDATE PDU and local configuration data concerning the permissible traffic type(s) and supported ATSC class(es) of the air-ground adjacency received in the mobile subnetwork capability parameter of the uplinked ISH PDU during air-ground route initiation (see 3.3.5.2.6.11).

Note.— An ATN air-ground router signals its capability to generate UPDATE PDUs without air-ground subnetwork type security tag(s) using the ATN data link capabilities parameter (see 3.8.2.1.3) included in the options part of uplinked ISH PDU(s).

3.3.5.2.12 Procedures for the optional non-use of IDRP over an air-ground data link

3.3.5.2.12.1 *General*

Note.— In this case, there is no recommendation to suppress the periodic retransmission of ISH PDUs according to the ISO/IEC 9542 report configuration function. In the absence of IDRP, this retransmission is necessary to maintain the "liveness" of the connection.

When the procedures for the optional non-use of IDRP are employed by an airborne router, then all ATN airborne systems on the same aircraft shall be located in the same routing domain.

Note.— This is because the procedures specified below make assumptions on the value and length of the NSAP address prefix that is common to all systems on board an aircraft, and these assumptions are invalidated if a single aircraft hosts multiple RDs.

3.3.5.2.12.2 *Air-ground router*

3.3.5.2.12.2.1 Through the actions of the IS-SME as specified below, an air-ground router shall simulate the existence of a BIS-BIS connection with an airborne router that implements the procedures for the optional non-use of IDRP by implementing the following procedure:

a) the NET of the remote ATN router shall be appended to the externalBISNeighbor attribute of the BIS's idrpConfig managed object, if not already present, and an adjacentBIS managed object shall be created for the remote ATN router identified by this NET, if one does not already exist. An Adj-RIB-In shall hence be created for this remote ATN router and for the security RIB-Att.

Note.— No activate action will be applied to this MO and the implementation will hence need to be able to process information in the Adj-RIB-In even though the MO is in the "idle" state. Implementations may choose to optimize the operation of these procedures with a special interface to IDRP.

b) truncating the NET received on the ISH PDU to the first eleven octets and using the resulting NSAP address prefix as the NLRI of a route which shall then be inserted into the Adj-RIB-In for the remote ATN router and which shall be identified by the security RIB-Att, as if it had been received over a BIS-BIS connection. This route shall include an RD_Path attribute with the received NET as the routing domain identifier of the originating RD, and an empty security path attribute.

Note.— According to the rules for the update of path information specified in 3.8, the security path attribute will be updated by the routing decision process to include an air-ground subnetwork type security tag and an ATSC class security tag, if this is appropriate. This procedure is identical to the normal use of IDRP over a mobile subnetwork.

c) the well-known mandatory path attribute RD_HOP_COUNT shall be set to 1 in the routes to be inserted into the Adj-RIB-In for the remote router implementing the procedures for the optional non-use of IDRP. In addition, for routes to be inserted into the Adj-RIB-In for an adjacent airborne router implementing the procedures for the optional non-use of IDRP, the well-known mandatory path attribute CAPACITY shall be set according to the capacity of the mobile subnetwork(s) over which the airborne router is reachable.

3.3.5.2.12.2.2 If a subnetwork connection is concurrently established with the remote ATN router over which the procedures for the optional non-use of IDRP have been applied, then the IS-SME shall not repeat the above procedures for the new subnetwork connection.

3.3.5.2.12.2.3 Instead, the IS-SME shall cause the IDRP routing decision function to be invoked in order to rebuild the FIB taking into account the additional subnetwork connectivity.

3.3.5.2.12.2.4 This shall include re-update of the security information contained in routes received from the remote ATN router, according to 3.8.

3.3.5.2.12.2.5 The IS-SME shall also ensure that a normal BIS-BIS connection does not concurrently exist with an ATN router with the same NET.

3.3.5.2.12.2.6 This is an error and shall be reported to systems management; the procedures for the optional non-use of IDRP shall not be applied in this case.

3.3.5.2.12.3 *Airborne router*

3.3.5.2.12.3.1 An airborne router implementing the procedures for the optional non-use of IDRP over a mobile subnetwork shall simulate the operation of IDRP by maintaining a Loc-RIB for the security RIB_Att, which is then used to generate FIB information.

3.3.5.2.12.3.2 Through the actions of its IS-SME, an airborne router shall derive entries for this Loc-RIB from the ISH PDU received from an air-ground router as follows:

a) the IS-SME shall insert into the Loc-RIB a route derived by truncating the NET received on the ISH PDU to the first eleven octets and using the resulting NSAP address prefix as the NLRI of a route. This route shall include a security path attribute with the air-ground subnetwork type and ATSC class security tags (if any) determined from the mobile subnetwork capabilities parameter contained in the options part of the received ISH PDU, or from locally known information if such a parameter is not present in the received ISH PDU.

Note.— This provides routing information for destinations in the air-ground router's RD and assumes that the eleven octet prefix of the air-ground router's NET is common to all destinations in that RD.

b) the IS-SME shall insert into the Loc-RIB other routes available through the air-ground router determined using locally known information. These routes shall include a security path attribute with the air-ground subnetwork type and ATSC class security tags (if any) determined from the mobile subnetwork capabilities parameter contained in the options part of the received ISH PDU, or from locally known information if such a parameter is not present in the received ISH PDU.

Note.— As these routes are not subject to dynamic update, their availability must be ensured by the operator of the air-ground router, within the limits specified for the applications that will use them.

3.3.5.2.13 Air-ground route termination

3.3.5.2.13.1 *ISO/IEC 8208 subnetworks*

Note 1.— The "Leave Event" is defined to signal when a previously available physical communication path with a remote ATN router over a mobile subnetwork ceases to be available. This event may be generated by (a) the subnetwork itself using mechanisms outside of the scope of this specification, or (b) the SNDCF when it receives a clear indication from the subnetwork reporting either a network or a user initiated call clearing. The leave event is always reported to the IS-SME.

Note 2.— When a leave event is generated by a subnetwork, it applies to all subnetwork connections to a given DTE. When it is generated locally by the SNDCF, it typically applies to a single subnetwork connection.

3.3.5.2.13.1.1 A "leave event" should not be generated by the mobile SNDCF when a subnetwork connection is closed due to the expiration of the X.25 Idle timer, except if this subnetwork connection fails to be re-established.

3.3.5.2.13.1.2 When an IS-SME receives a leave event for a subnetwork connection or a DTE on a subnetwork, then it shall ensure that respectively, either the affected subnetwork connection or all subnetwork connections on that subnetwork and with the identified DTE, are cleared.

3.3.5.2.13.1.3 If, as a result of this procedure, no other subnetwork connection exists anymore on that subnetwork and with the identified DTE, then the IS-SME shall remove the configuration information that was extracted from the ISH PDU previously received from that DTE on that specified subnetwork, without waiting for the expiration of the configuration information holding timer.

3.3.5.2.13.2 *Non-ISO/IEC 8208 subnetworks*

When the IS-SME receives a "leave event" from a subnetwork supported by the A/GCS, then the frame mode SNDCF's data link termination service shall be invoked.

3.3.5.2.13.3 *Update of routing information*

3.3.5.2.13.3.1 If, as a result of the procedures specified in §3.3.5.2.13.1 or §3.3.5.2.13.2 respectively or subsequent to the execution of the ISO/IEC 9542 "Flush Old Configuration" function, configuration information that was extracted from an ISH PDU previously received from that DTE still exists, then:

a) in the case of an ATN air-ground router having established a BIS-BIS connection with that ATN router, or having simulated a BIS-BIS connection if that ATN router implements the procedures for the optional non-use of IDRP, then:

   1) the IS-SME shall cause the update of the security path attribute's security information of all routes contained in the Adj-RIB-In associated with the remote ATN airborne router; and,

   2) the IS-SME shall cause the IDRP routing decision function to be invoked in order to rebuild the FIB, the Loc_RIB and relevant Adj-RIB-Out(s) taking into account the loss of subnetwork connectivity; and,

   3) the air-ground router shall re-advertise all routes affected by the change in subnetwork connectivity that are contained in the Adj-RIB-Out(s) subsequent to the update of the security path attribute's security information of these routes as specified in §3.8;

   Note.— When a change in the mobile subnetwork connectivity occurs over an adjacency with an airborne router that has signalled its capability to support UPDATE PDUs without air-ground subnetwork type security tag, the security path attribute's security information of the routes contained in the Adj-RIB-Out associated with the remote airborne router is not updated (see §3.8.3.2.4.2.8). As a consequence, these routes are not affected by the changes and do not need to be re-advertised to the airborne router.

b) in the case of an airborne router implementing the procedures for the optional non-use of IDRP, the IS-SME shall update the security path attribute's security information of all routes in the Loc-RIB that had been inserted according to the procedures of §3.3.5.2.12.3 as a result of an ISH PDU having been received from the air-ground router for which loss of connectivity is reported;

c) in the case of an airborne router which supports the use of IDRP for the exchange of routing information (i.e. a Class 6 ATN router), the IS-SME of the airborne router shall cause the IDRP routing decision function to be invoked in order to rebuild the FIB, the Loc_RIB and relevant Adj-RIB-Out(s) taking into account the loss of subnetwork connectivity.

3.3.5.2.13.3.2 If, as a result of the procedures specified in §3.3.5.2.13.1 or §3.3.5.2.13.2 respectively or subsequent to the execution of the ISO/IEC 9542 "Flush Old Configuration" function, no configuration information exists anymore for the ATN router for which loss of connectivity is reported, then:

a) in the case of an ATN router having established a BIS-BIS connection with that ATN router, an IDRP deactivate action shall be invoked to terminate that BIS-BIS connection;

Note.— As a consequence of the deactivate action and following normal IDRP operation, the IDRP routing decision process will be invoked, the local FIB updated and routes previously available via the remote ATN router may be withdrawn if suitable alternatives are not available.

b) in the case of an air-ground router having simulated a BIS-BIS connection to an ATN airborne router, implementing the procedures for the optional non-use of IDRP, all routes shall be removed from the Loc-RIB that had been inserted into it according to the procedures of §3.3.5.2.12.2 as a result of an ISH PDU having been received from the airborne router for which a loss of connectivity is reported.

c) in the case of an airborne router implementing the procedures for the optional non-use of IDRP, all routes shall be removed from the Loc-RIB that had been inserted into it according to the procedures of §3.3.5.2.12.3 as a result of an ISH PDU having been received from the air-ground router for which a loss of connectivity is reported.

3.3.5.2.13.3.3 If the BIS-BIS connection is not re-established within a period configurable from 1 minute to 300 minutes, or when the resources are required for other use, then the adjacentBIS managed object associated with the initiating BIS shall be deleted, and the initiating BIS's NET removed from the externalBISNeighbor attribute of the BIS's idrpConfig managed object.

3.3.5.2.14 Subnetwork handoff

Note 1.— Handoff is implemented by some ISO/IEC 8208 subnetworks, for example, the VHF digital link (VDL), when an aircraft moves out of the coverage of a ground station it is currently using and into the coverage of another – typically operated by the same service provider. When the change of ground station also requires a change of ATN air-ground router then the subnetwork may simply generate a join event for the new air-ground router, followed by a leave event for the old air-ground router. However, when the air-ground router accessed through the old ground station is also accessible through the new ground station then a different procedure is required if the full overhead of route initiation is to be avoided.

Note 2.— A further event – the "handoff event" – and additional to the "join" and "leave" events is defined to initiate such a procedure. A handoff event may be received by an airborne or an air-ground router irrespective of whether the subnetwork is air- or ground-initiated, or both. The handoff event is also processed by the IS-SME.

Note 3.— The parameters of a handoff event include the DTE address of the system for which handoff is to take place and may also include subnetwork specific information (e.g. to direct a call request via a specific ground station).

3.3.5.2.14.1 On receipt of a handoff event, the IS-SME shall check to see if a subnetwork connection already exists with the DTE identified by the handoff event. If it does not, then the handoff event shall be processed identically to a join event.

3.3.5.2.14.2 If a subnetwork connection already exists with the identified DTE, then the ATN router shall issue an ISO/IEC 8208 call request to that DTE. If a different DTE address to the originally called DTE address was reported when the connection had previously been made to that DTE, then the returned Called DTE address shall be used and not the originally called DTE address.

3.3.5.2.14.3 If more than one subnetwork connection exists with the identified DTE, each with a distinct subnetwork connection priority, then a new subnetwork connection shall be initiated for each such subnetwork connection priority.

Note 1.— If the maintenance/initiation of the local reference directory option is selected (see §3.7.4.2.1.5.4.8), then the subnetwork connection(s), once established, may become part of the same subnetwork connection group(s) as the one(s) of the old subnetwork connection(s). If this is the case, then the LREF directory will be taken over by the new subnetwork connection(s).

Note 2.— If the option for the maintenance of the deflate history windows is selected (see §3.7.4.2.1.5.4.21), then the subnetwork connection(s), once established, may become part of the same subnetwork connection group(s) as the one(s) of the old subnetwork connection(s).

Note 3.— No further action needs to be taken once the subnetwork connection(s) have been successfully established. This is because no change is implied to the routing information base, and the underlying subnetwork is responsible for timing out and disconnecting the old subnetwork connections, once all data in transit has been delivered.

Note 4.— In the case that a new (set of) connection(s) is established, existing old connections between the same pair of DTEs are likely to become unavailable shortly. Implementations are advised to use these new subnetwork connection(s) in preference to the old subnetwork connections(s).

3.3.5.2.15 Re-establishment of BIS-BIS connection

The IS-SME shall attempt to re-establish a BIS-BIS connection using the procedures in §3.3.5.2.10 irrespective of which side first initiated the adjacency when:

a) a previously established BIS-BIS connection with the same remote ATN router is terminated for reasons other than the receipt of a leave event by the IS-SME; or

b) a previous attempt to establish a BIS-BIS connection failed;

and at least one ISO/IEC 8208 subnetwork connection between the local and remote ATN router exists.

Note 1.— This procedure guarantees that whenever a subnetwork connectivity is available between an ATN airborne and ATN air-ground router routes are made available via IDRP and NPDUs can be exchanged via the air-ground adjacency.

Note 2.— This procedure will cause an OPEN BISPDU to be sent irrespective of which side was the initiator of the initial BIS-BIS connection in order to force the resynchronization of the local and remote IDRP protocol machines which may be out of sync as a result of the failure causing the termination of a BIS-BIS connection.

3.3.5.2.16 APRL for air-ground route initiation

3.3.5.2.16.1 *General*

Item	*Description*	*ATN Reference*	*ATN Support*
jSubnet	Support of subnetworks that do provide a join event	§3.3.5.2	M
giSubnet	Support of ground-initiated subnetworks	§3.3.5.2	O.1
aiSubnet	Support of air-initiated subnetworks	§3.3.5.2	O.1
agSubnet	Support of air- or ground-initiated subnetworks	§3.3.5.2	O.1
fsSubnet	Support of subnetworks that support fast select	—	O

Item	*Description*	*ATN Reference*	*ATN Support*
noIDRP-a	Support of optional non-use of IDRP by airborne BIS	§3.3.5.2.12.3	O
noIDRP-ag	Support of optional non-use of IDRP by air-ground BIS	§3.3.5.2.12.2	M
lvSubnet	Support of subnetworks that provide a leave event	§3.3.5.2.13	M
HoSubnet	Support of subnetworks that provide a handoff event	§3.3.5.2.14	O

3.3.5.2.16.2 *Airborne router – Subnetwork connection responder*

Item	*Description*	*ATN Reference*	*ATN Support*
respAR-ar	Response to incoming call request	§3.3.5.2.2	giOragSubnet: M
valCR-ar	Validation of incoming call request	§3.3.5.2.2	giOragSubnet:O
RespISH-ar	Generation of ISH PDU	§3.3.5.2.6	giOragSubnet: M
ISHinCC-ar	Encoding ISH PDU in call accept user data	§3.3.5.2.6	RespISH-ar and fsSubnet: O
negNoIDRP-ar	Transmission of ISH PDU with SEL field of NET set to FEh	§3.3.5.2.6	giOragSubnet and noIDRP-a:M
negIDRP-ar	Transmission of ISH PDU with SEL field of NET set to zero	§3.3.5.2.6	giOragSubnet and ^noIDRP-a:M
dlCap-ar	Encoding of ATN data link capability parameter in ISH PDU	§3.3.5.2.6.5	RespISH-ar:M
autoRoute-ar	Inference of available routes from received NET of A/G Router	§3.3.5.2.12	giOragSubnet and noIDRP-a:M
initIDRP-ar	IDRP startup procedures – Invoke activate action	§3.3.5.2.10	giOragSubnet and ^noIDRP-a:M
supISH-ar	Suppression of multiple ISH PDUs	§3.3.5.2.10	giOragSubnet and ^noIDRP-a: O
valNET-ar	Validation of received NET	§3.3.5.2.7	giOragSubnet and ^noIDRP-a: O
Handoff-ar	Processing of handoff event	§3.3.5.2.14.1	HoSubnet:M

giOragSubnet: giSubnet or agSubnet

3.3.5.2.16.3 *Airborne router – Subnetwork connection initiator*

Item	*Description*	*ATN Reference*	*ATN Support*
connect-ai	Connect on receipt of join event	§3.3.5.2.3.2	EventDrvn:M
ValJoin-ai	Validation of join event	§3.3.5.2.3.2	EventDrvn:O
SendISH-ai	Generation of ISH PDU	§3.3.5.2.6	EventDrvn:M

Item	*Description*	*ATN Reference*	*ATN Support*
ISHinCR-ai	Encoding of ISH PDU in call request	§3.3.5.2.6	SendISH-ai and fsSubnet: O
negNoIDRP-ai	Transmission of ISH PDU with SEL field of NET set to FEh	§3.3.5.2.8	EventDrvn and no IDRP-a:M
negIDRP-ai	Transmission of ISH PDU with SEL field of NET set to zero	§3.3.5.2.8	EventDrvn and ^noIDRP-a:M
dlCap-ai	Encoding of ATN data link capability parameter in ISH PDU	§3.3.5.2.6.5	SendISH-ai:M
autoRoute-ai	Inference of available routes from received NET of A/G router	§3.3.5.2.12.3	EventDrvn and no IDRP-a:M
initIDRP-ai	IDRP startup procedures - listenForOpen set to true	§3.3.5.2.10	EventDrvn and ^noIDRP-a:M
supISH-ai	Suppression of multiple ISH PDUs	§3.3.5.2.10	EventDrvn and ^noIDRP-a: O
valNET-ai	Validation of received NET	§3.3.5.2.7	EventDrvn and ^noIDRP-a: O
RelateDTE-ai	Maintain relationship between originally called and returned called DTE address	§3.3.5.2.3.2.2	HoSubnet: M
Handoff-ai	Processing of handoff event	§3.3.5.2.14	HoSubnet: M

EventDrvn: jSubnet and (aiSubnet or agSubnet)

3.3.5.2.16.4 *Air-ground router – Subnetwork connection responder*

Item	*Description*	*ATN Reference*	*ATN Support*
respAR-agr	Response to incoming call request	§3.3.5.2.2	aiOragSubnet: M
valCR-agr	Validation of incoming call request	§3.3.5.2.2	aiOragSubnet:O
RespISH-agr	Generation of ISH PDU	§3.3.5.2.6	aiOragSubnet: M
ISHinCC-agr	Encoding ISH PDU in call accepted user data	§3.3.5.2.6	RespISH-agr and fsSubnet: O
dlCap-agr	Encoding of ATN data link capability parameter in ISH PDU	§3.3.5.2.6.5	RespISH-agr:M
msCap-agr	Encoding of mobile subnetwork capability parameter in ISH PDU	§3.3.5.2.6.6	RespISH-agr:M
negNoIDRP-agr	Receipt of ISH PDU with SEL field of NET set to FEh	§3.3.5.2.8	aiOragSubnet:M
negIDRP-agr	Receipt of ISH PDU with SEL field of NET set to zero	§3.3.5.2.8	aiOragSubnet:M
autoRoute-agr	Inference of available routes from received NET of airborne router	§3.3.5.2.12.2	aiOragSubnet:M
initIDRP-agr	IDRP startup procedures – Invoke activate action	§3.3.5.2.10	aiOragSubnet:M

Item	*Description*	*ATN Reference*	*ATN Support*
supISH-agr	Suppression of multiple ISH PDUs	§3.3.5.2.10	aiOragSubnet:O
valNET-agr	Validation of received NET	§3.3.5.2.7	aiOragSubnet:O
Handoff-agr	Processing of handoff event	§3.3.5.2.14.1	HoSubnet:M

aiOragSubnet: aiSubnet or agSubnet

3.3.5.2.16.5 *Air-ground router – Subnetwork connection initiator*

Item	*Description*	*ATN Reference*	*ATN Support*
connect-agi	Connect on receipt of join event	§3.3.5.2.4	goOragSubnet: M
ValJoin-agi	Validation of join event	§3.3.5.2.4	connect-agi: O
SendISH-agi	Generation of ISH PDU	§3.3.5.2.6	connect-agi: M
ISHinCR-agi	Encoding of ISH PDU in call request	§3.3.5.2.6	Send-ISH-agi and fsSubnet: O
dlCap-agi	Encoding of ATN data link capability parameter in ISH PDU	§3.3.5.2.6.5	SendISH-agi:M
msCap-agi	Encoding of mobile subnetwork capability parameter in ISH PDU	§3.3.5.2.6.6	SendISH-agi:M
negNoIDRP-agi	Receipt of ISH PDU with SEL field of NET set to FEh	§3.3.5.2.8	goOragSubnet:M
negIDRP-agi	Receipt of ISH PDU with SEL field of NET set to zero	§3.3.5.2.8	goOragSubnet:M
autoRoute-agi	Inference of available routes from received NET of airborne router	§3.3.5.2.12.2	goOragSubnet:M
initIDRP-agi	IDRP startup procedures – listenForOpen set to true	§3.3.5.2.10	goOragSubnet:M
supISH-agi	Suppression of multiple ISH PDUs	§3.3.5.2.10	goOragSubnet:O
valNET-agi	Validation of received NET	§3.3.5.2.7	goOragSubnet:O
RelateDTE-agi	Maintain relationship between originally called and returned called DTE address	§3.3.5.2.4.2	HoSubnet:M
Handoff-agi	Processing of Handoff Event	§3.3.5.2.14.1	HoSubnet: M

goOragSubnet: giSubnet or agSubnet

3.3.5.2.16.6 *Termination procedures*

Item	*Description*	*ATN Reference*	*ATN Support*
lvEvent	Processing of leave event	§3.3.5.2.13	M
conLeave	Processing of a per connection leave event	§3.3.5.2.13	M
subnetLeave	Processing of a per subnetwork leave event	§3.3.5.2.13	M

3.3.6 Handling routing information

All ATN routers in the same RD shall implement the same routing policy.

Note 1.— As specified in §3.8, an ATN router supports both the empty (default) RIB_Att, and the RIB_Att comprising the security path attribute identifying the ATN security registration identifier. An ATN router therefore includes two RIBs known as the default RIB and the security RIB, each of which comprises a Loc-RIB, and an Adj-RIB-In and an Adj-RIB-Out for each adjacent BIS.

Note 2.— Each ATN RD will necessarily have a distinct routing policy that depends on its nature, and the nature of the RDs to which it is interconnected. Section §3.3.7 specifies the baseline routing policy for each class of RD identified in §3.2.2.2 to §3.2.2.5 inclusive. ATN RDs may then extend the specified baseline to match their actual requirements.

Note 3.— Each routing policy is expressed as a set of policy statements or rules.

Note 4.— These baseline policy statements given below are always subject to the ISO/IEC 10747 requirement that routes are only advertised when the DIST_LIST_INCL and DIST_LIST_EXCL path attributes, if present, permit the route to be so advertised. Routes may never be advertised to an RD or RDC which the route has already traversed.

3.3.7 Policy-based selection of routes for advertisement to adjacent RDs

Note.— In general, the selection of routes for advertisement to adjacent routing domains is performed according to local routing policy rules. This specification mandates such routing policy rules for support of air-ground routing only. Routing policy rules for support of ground-ground routing are a local matter.

3.3.7.1 Routing policy requirements for members of an ATN island backbone RDC

3.3.7.1.1 General

An ATN RD that is a member of an ATN island backbone RDC shall implement a routing policy that is compatible with the policy statements given in this section and its subordinate sections.

3.3.7.1.2 Adjacent ATN RDs within the backbone RDC

Note.— These policy statements apply to the routes advertised by an ATN router in an RD that is a member of an ATN island backbone RDC, to an adjacent ATN router in a different RD, which is also a member of the same ATN island backbone RDC.

Each ATN router that is in an RD that is a member of an ATN island backbone RDC shall provide the following routes to each adjacent ATN RD within the same ATN island backbone RDC, and for the security RIB-Att:

a) a route to NSAPs and NETs contained within the RD; the route's destination shall be one or more NSAP address prefixes common to all NSAP addresses and NETs in the RD. If restrictions on distribution scope are applied by local routing policy, then they shall not prevent distribution of this route to any member of the same ATN island backbone RDC.

Note 1.— The well-known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN island backbone RDC only.

The RDIs of other RDs and RDCs may also be present at the discretion of the local administrative domain, and by bilateral agreement.

Note 2.— The objective of this rule is to ensure that a member of an ATN island backbone RDC will tell all its neighbours within the backbone RDC about itself.

b) the selected route to every mobile RD for which a route is available;

Note.— The objective of this rule is to ensure that a member of an ATN island backbone RDC will inform all other backbone RDC members within the island about all mobiles that it has available.

c) the selected route to every fixed ATN RD in the same ATN island, for which a route is available;

Note.— The objective of this rule is to ensure that a member of an ATN island backbone RDC will tell other members of the same backbone RDC about all fixed RDs that it knows about.

d) each selected route to a mobile RD's “home”;

Note 1.— The objective of this rule is to ensure that a member of an ATN island backbone RDC will tell all other members of the same backbone RDC about all the “homes” that it knows about.

Note 2.— Such a route can be characterized by an NSAP address prefix which ends at the ADM field.

e) a route to each “Home” that the ATN TRD itself provides for mobile RDs. This route has as its destination the common NSAP address prefix(es) for those mobile RDs. The security path attribute shall contain an ATSC class security tag indicating support for both ATSC and non-ATSC traffic, and for all ATSC classes supported for air-ground data interchange, if any.

Note.— The objective of this item is to ensure that all RDs in the ATN island backbone RDC are aware that the identified “Homes” are located here.

3.3.7.1.3 All other ATN RDs within the ATN island

Note.— These policy statements apply to the routes advertised by an ATN router in an RD that is a member of an ATN island backbone RDC to an adjacent ATN router in a different RD, which is also a member of the same ATN island RDC, but which is not a member of that ATN island backbone RDC.

An ATN router that is in an RD that is a member of an ATN island backbone RDC shall provide the following routes to each adjacent ATN RD within the ATN island RDC, which is not a member of the ATN island’s backbone RDC, and for the security RIB-Att:

a) a route to NSAPs and NETs contained within the RD; the route’s destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD. If restrictions on distribution scope are applied by local routing policy, then they shall not prevent distribution of this route to any member of the same ATN island RDC.

Note 1.— The well-known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN island only. The RDIs of other RDs and RDCs may also be present at the discretion of the local administrative domain and by bilateral agreement.

Note 2.— The objective of this rule is to ensure that a member of an ATN island backbone RDC will tell all RDs within the island about itself.

b) the selected route to every fixed ATN RD in the same ATN island for which a route is available.

Note.— The objective of this rule is to ensure that an ATN router located in an RD that is a member of an ATN island backbone RDC will tell all RDs within the island about all the fixed RDs it knows about.

c) a route to all AINSC mobiles and all ATSC mobiles. The well-known discretionary attribute DIST_LIST_INCL shall be present and shall contain the RDI of the ATN island RDC as its value. The security path attribute shall contain an ATSC class security tag indicating support for both ATSC and non-ATSC traffic, and for all ATSC classes supported for air-ground data interchange, if any.

Note 1.— The objective of this rule is to tell the rest of the island that each RD in the ATN island backbone RDC provides a default route to all aircraft.

Note 2.— The distribution scope of the route is limited because the ATN island defines the domain of the default route provider. This route is invalid outside of the local ATN island.

Note 3.— This route is formally the result of aggregating all the routes to mobile systems and routes to “Home” RDs, known to the ATN router.

d) a route to each mobile RD for which the adjacent RD is advertising a route to the mobile RD's “home”.

Note.— The objective of this rule is to ensure that a member of an ATN island backbone RDC will tell all adjacent off backbone RDs about all routes to mobile RDs which have “home” routes advertised.

3.3.7.1.4 Mobile RDs

Note.— These policy statements apply to the routes advertised by an ATN router in an RD that is a member of an ATN island backbone RDC to an adjacent ATN router in a mobile RD.

3.3.7.1.4.1 When IDRP is being used to exchange routing information with an airborne router, an ATN router in an RD that is a member of an ATN island backbone RDC shall provide to each adjacent mobile RD a route to NSAPs and NETs contained within the local RD for the security RIB-Att; the route’s destination shall be one or more NSAP address prefixes common to all NSAP addresses and NETs in the local RD.

Note.— The objective of this rule is to ensure that an RD that is a member of an ATN island backbone RDC will tell all adjacent mobiles about itself.

3.3.7.1.4.2 An ATN RD that is a member of an ATN island backbone RDC should also provide to each adjacent mobile RD, and for the security RIB-Att and for which a suitable route exists:

a) an aggregated route to NSAPs and NETs contained within the local ATN island RDC;

Note.— The objective of this rule is to ensure that an RD that is a member of an ATN island backbone RDC provides to each connected mobile RD, a route to all fixed ATN RDs within the island.

b) an aggregated route to NSAPs and NETs contained within all other ATN islands for which a route is available.

Note.— The objective of this rule is to ensure that an RD that is a member of an ATN island backbone RDC will provide to each connected mobile RD routing information to the backbone of other ATN islands.

3.3.7.1.5 ATN RDs in other ATN islands

Note.— These policy statements apply to the routes advertised by an ATN router in an RD that is a member of an ATN island backbone RDC to an adjacent ATN router in a different RD, which is a member of a different ATN island's ATN island backbone RDC.

An ATN router in an RD that is a member of an ATN island backbone RDC shall provide the following routes to each adjacent ATN router that is a member of a backbone RDC in another ATN island, and for the security RIB-Att:

a) an aggregated route to NSAPs and NETs contained within the ATN island RDC;

Note.— The objective of this rule is to ensure that an RD that is a member of an ATN island backbone RDC will tell all adjacent RDs that are members of ATN island backbone RDCs in different ATN islands about the local ATN island.

b) each selected route to a mobile RD's "home";

c) a route to each "home" that the ATN TRD itself provides for mobile RDs. This route has as its destination the common NSAP address prefix(es) for those mobile RDs. The security path attribute shall contain an ATSC class security tag indicating support for both ATSC and non-ATSC traffic, and for all ATSC classes supported for air-ground data interchange, if any;

Note 1.— The objective of this rule is to ensure that an ATN island backbone RD will tell all adjacent RDs that are member of an ATN island backbone RD in different ATN islands about routes to mobiles whose "home" is in the local island.

Note 2.— The "home" identified above need not correspond to a geographical notion of a home.

Note 3.— The "home" is typically identified by an NSAP address prefix that identifies all the RDs belonging to the organization responsible for the mobile RD (i.e. aircraft), or all the mobile RDs belonging to the organization. The former is only possible if all such fixed RDs are part of the same ATN island RDC.

d) a known route to each mobile RD for which the adjacent RD is advertising a route to the mobile RD's "home".

Note.— The objective of this rule is to ensure that a member of an ATN island backbone RDC will tell all adjacent RDs in different islands about all routes to mobile RDs which have "home" routes advertised.

3.3.7.2 Routing policy requirements for a mobile RD

When IDRP is being used to exchange routing information with an airborne router, a mobile RD shall provide to each ATN RD to which it is currently connected, a route to NSAPs and NETs contained within the mobile RD for the security RIB-Att.

Note 1.— The objective of this rule is to ensure that a mobile RD will tell adjacent RDs about itself.

Note 2.— This policy statement applies to the routes advertised by an ATN router in a mobile RD to an adjacent ATN air-ground router in a fixed ATN RD.

3.3.7.3 Routing policy requirements for an ATN TRD that is not a member of the ATN island backbone RDC

3.3.7.3.1 General

An RD that is a member of an ATN island RDC, and is a TRD, but which is not a member of that ATN island's backbone RDC shall implement a routing policy that is compatible with the policy statements given in this section and its subordinate sections.

Note.— An ATN RD that operates as a transit routing domain is referred to in this chapter as an ATN TRD.

3.3.7.3.2 Adjacent ATN RDs that are members of the ATN island's backbone RDC

Note.— These policy statements apply to the routes advertised by an ATN router in an ATN TRD to an adjacent ATN router in an RD which is a member of the local ATN island's backbone RDC.

When an ATN TRD that is not itself a member of an ATN island backbone RDC is adjacent to an RD that is a member of an ATN island backbone RDC, then it shall provide the following routes to each such adjacent ATN RD, and for the security RIB-Att:

a) a route to NSAPs and NETs contained within the RD; the route's destination shall be one or more NSAP address prefixes common to all NSAP addresses and NETs in the RD;

Note 1.— The well-known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN island only. The RDIs of other RDs and RDCs may also be present at the discretion of the local administrative domain, and by bilateral agreement.

Note 2.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of an ATN island backbone RDC will tell all adjacent ATN RDs which are members of an ATN island backbone RDC within the same ATN island about itself.

b) the selected route to every mobile RD for which a route is available;

Note.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of an ATN island backbone RDC will tell all adjacent ATN RDs which are members of an ATN island backbone RDC within the same ATN island about all mobiles it knows about.

c) the selected route to every fixed ATN RD in the ATN island for which a route is available;

Note.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of an ATN island backbone RDC will tell all adjacent ATN RDs which are members of an ATN island backbone RDC within the same ATN island about all fixed RDs it knows about in the same ATN island.

d) a route to each "home" that the ATN TRD itself provides for mobile RDs. This route shall have as its destination, the common NSAP address prefix(es) for those mobile RDs. The security path attribute shall contain an ATSC class security tag indicating support for both ATSC and non-ATSC traffic, and for all ATSC classes supported for air-ground data interchange.

Note.— The objective of this rule is to support the operation of the home domain concept on any ATN TRD directly connected to an ATN island backbone RD.

3.3.7.3.3 Adjacent ATN RDs within the same ATN Island and which are not members of the ATN island's backbone RDC

Note.— These policy statements apply to the routes advertised by an ATN router in an ATN TRD to an adjacent ATN router in an ATN RD on the same ATN island.

An ATN TRD shall provide the following routes to each adjacent ATN RD within the ATN island RDC, other than ATN RDs which are members of the ATN island backbone RDC, and for the security RIB-Att:

a) a route to NSAPs and NETs contained within the RD for the security RIB-Att; the route's destination shall be one or more NSAP address prefixes common to all NSAP addresses and NETs in the RD;

Note 1.— The well-known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN island only. The RDIs of other RDs and RDCs may also be present at the discretion of the local administrative domain, and by bilateral agreement, including the RDI of the ATN island backbone RD or RDC, when the adjacent RD is providing the local RD's route to the ATN island backbone.

Note 2.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of the ATN island backbone RDC will tell all adjacent RDs within the island about itself.

b) the selected route to every fixed RD in the same ATN island for which a route is available;

Note.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of the ATN island backbone RDC will tell all adjacent RDs within the island about all fixed ATN RDs in the same ATN island that it knows about.

c) if the RD is currently advertising the preferred route to all AINSC and ATSC mobiles, then every route to an AINSC mobile and an ATSC mobile that is known to the local RD shall be advertised to this RD, subject only to constraints imposed by any DIST_LIST_INCL and DIST_LIST_EXCL path attributes.

Note.— The objective of this rule is to ensure that the provider of the default route to all aircraft (i.e. the backbone) is kept informed of the actual location of every aircraft adjacent to the island.

d) the preferred route to all mobiles, except when the RD is the source of this route.

Note.— The objective of this rule is to ensure propagation of the default route to all mobiles throughout the ATN island.

e) a route to each mobile RD for which the adjacent RD is advertising the preferred route to the mobile RD's "home".

Note.— The objective of this rule is to ensure routes to mobile RDs are propagated to off backbone homes.

f) a route to each "home" that the ATN TRD itself provides for mobile RDs. This route has as its destination the common NSAP address prefix(es) for those mobile RDs. The security path attribute shall contain an ATSC class security tag indicating support for both ATSC and non-ATSC traffic, and for all ATSC classes supported for air-ground data interchange, if any.

Note.— The objective of this item is to ensure that all RDs in the ATN island are aware that the identified "homes" are located here.

3.3.7.3.4 Mobile RDs

Note.— These policy statements apply to the routes advertised by an ATN router in an ATN TRD to an adjacent ATN router in a mobile RD.

3.3.7.3.4.1 When IDRP is being used to exchange routing information with the airborne router, an ATN TRD shall provide to each adjacent mobile RD a route to NSAPs and NETs contained within the RD for the security RIB-Att; the route's destination shall be one or more NSAP address prefixes common to all NSAP addresses and NETs in the RD.

Note.— The objective of this rule is to ensure that an ATN TRD will tell adjacent mobile RDs about itself.

3.3.7.3.4.2 An ATN TRD should also provide to each adjacent mobile RD, and for the security RIB-Att and for which a suitable route exists:

a) an aggregated route to NSAPs and NETs contained within the local ATN island RDC;

b) an aggregated route to NSAPs and NETs contained within all other ATN islands for which a route is available.

Note.— The objective of this rule is to encourage an RD to provide to each adjacent mobile RD routing information about: a) all fixed RDs within the island, and b) other ATN islands.

3.3.7.4 Routing policy for a fixed ATN ERD

A fixed ATN ERD shall provide to each ATN RD to which it is currently connected, a route to NSAPs and NETs contained within the RD, for the security RIB-Att.

Note 1.— The well-known discretionary attribute DIST_LIST_INCL may be present, unless the RD permits routes to destinations within itself to be advertised by other ATN RDs without restriction to any other ATN RD, or non-ATN RD.

Note 2.— This policy statement applies to the routes advertised by an ATN router in a fixed ATN ERD to an adjacent ATN router in an ATN RD.

Note 3.— An ERD does not advertise routes to destinations in any other RD, to another RD.

3.4 NETWORK AND TRANSPORT ADDRESSING SPECIFICATION

3.4.1 Introduction

Note 1.— The ATN Internet addressing plan defines an OSI network service access point (NSAP) address structure which can support efficient Internet routing procedures and which conforms to common abstract syntax, semantic and encoding rules throughout the ATN OSI environment.

Note 2.— This addressing plan also defines the format and use of TSAP selectors to enable the unambiguous identification of multiple transport service users within a single end system.

3.4.1.1 Addressing plan scope

The ATN Internet addressing plan shall be used by ATN end systems and intermediate systems.

Note.— The ATN internet addressing plan serves the needs of a variety of aeronautical data communication user groups, including ATSC and AINSC users.

3.4.1.2 Addressing plan applicability

Note.— The ATN Internet addressing plan defines the network and transport layer addressing information to be utilized by ATN end systems, and by ATN intermediate systems.

3.4.1.3 Reserved values in address fields

Address field values specified as “reserved” shall not be used until assigned by future editions of this specification.

3.4.1.4 Values of character format fields

3.4.1.4.1 When the value of a field is defined as a character string, then the actual value of the field shall be derived from the IA-5 encoding of each character in the character string.

3.4.1.4.2 The IA-5 encoding of the first character in the string shall be taken as the value of the first octet of the field and so on until all octets in the field have been given a value.

3.4.1.4.3 If the length of the character string is smaller than the number of octets in the field, then the character string shall be right padded with the space character.

3.4.1.4.4 The most significant bit of each octet shall be set to zero.

Note.— For example, the character string >EUR= would be encoded as 455552 hexadecimal, in a three octet field.

3.4.2 Transport layer addressing

3.4.2.1 General

Note 1.— This section provides requirements on the format of ATN TSAP addresses. An ATN TSAP address is an NSAP address and a TSAP selector.

Note 2.— The requirements in this section apply to the administration of transport addresses local to an ATN end system. They do not apply to all systems in a global OSI environment. An ATN system may allow remote transport addresses to obey different standards, e.g. when interworking with a non-ATN system is required.

3.4.2.2 ATN TSAP selector

3.4.2.2.1 An ATN TSAP selector shall be either one or two octets in length.

3.4.2.2.2 The TSAP selector field shall be administered on a local basis.

3.4.2.2.3 Valid ATN TSAP selector field values shall be in the range 0 to 65535.

3.4.2.2.4 The TSAP selector field shall be encoded as an unsigned binary number.

3.4.2.2.5 If the TSAP selector needs to be encoded in more than one octet, then the number shall be encoded with the most significant octet first.

Note.— This follows the encoding rules specified in ISO/IEC 8073.

3.4.2.2.6 TSAP selector values in the range 0 to 255 shall be encoded using one octet.

3.4.3 Network layer addressing

3.4.3.1 NSAP addresses and network entity titles (NETs)

Note 1.— The NSAP address is formally defined in ISO/IEC 8348. It is the name of a network service access point (NSAP) located in an end system and uniquely identifies that NSAP. It is also an address that may be used to find that NSAP.

Note 2.— The network entity title (NET) is also formally defined in ISO/IEC 8348 and is the name of a network entity located within an end or intermediate system. NETs are syntactically identical to NSAP addresses and are allocated from the same address space. An NET is also an address that may be used to find the network entity.

Note 3.— An NSAP address prefix is a substring of an NSAP address or NET that is comprised of the first >n= characters of the NSAP address or NET.

3.4.3.2 Network addressing domains

Note 1.— A network addressing domain comprises all NSAP addresses and NETs with a common NSAP address prefix and is always a sub-domain of the global NSAP addressing domain which contains all NSAP addresses. This nesting of network addressing domains within the global network addressing domain is conceptually illustrated in Figure 3-4.

Note 2.— A network addressing domain has a single administrator responsible for the assignment of NSAP addresses and NSAP address prefixes within the domain. A network addressing domain is often subdivided into a number of sub-ordinate domains each characterized by a unique NSAP address prefix. Management of such sub-ordinate network addressing domains may then be devolved to another administrator.

3.4.3.2.1 An ATSC network addressing domain shall be a network addressing domain administered by an ATSC authority.

3.4.3.2.2 An AINSC network addressing domain shall be a network addressing domain administered by a member of the aeronautical industry.

3.4.3.2.3 ATN end systems or intermediate systems located on board general aviation aircraft shall belong to an ATSC network addressing domain, whereas ATN systems installed on board commercial aircraft shall belong to an AINSC network addressing domain.

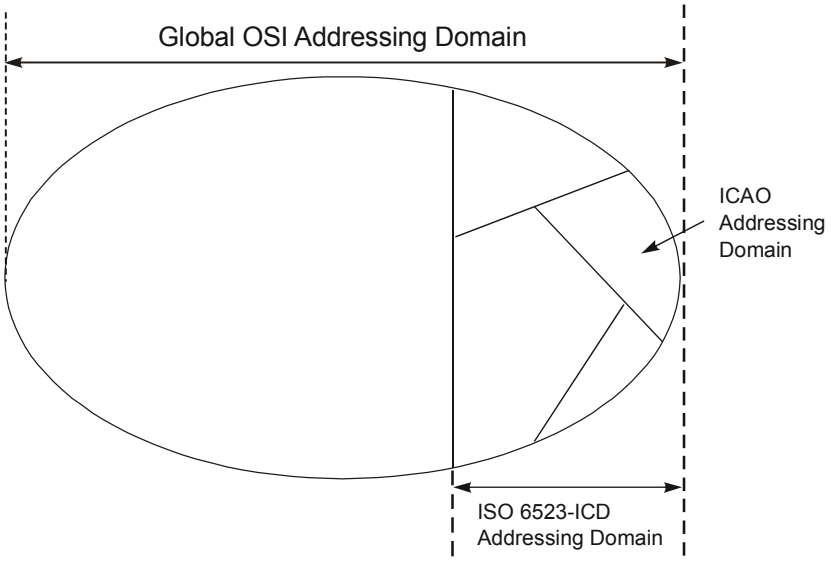


Figure 3-4. The global OSI network addressing domain

3.4.3.3 The syntax of an NSAP address

Note 1.— Following ISO/IEC 10589, a router interprets an NSAP address as a three-fields bit string. This is illustrated in Figure 3-5.

Area Address	System Identifier	SEL

Figure 3-5. ISO/IEC 10589 NSAP address syntax

Note 2.— An area address is typically common to all NSAP addresses and NETs assigned to systems in a single routing area.

Note 3.— An area address is an example of an NSAP address prefix.

Note 4.— A system identifier uniquely identifies an end or intermediate system within a routing area.

Note 5.— A selector (SEL) identifies a network service user or the network entity within an end or intermediate system.

3.4.3.4 The ATN addressing plan

Note 1.— ISO/IEC 8348 has specified how the global network addressing domain is broken down into a number of sub-ordinate network addressing domains, each of which is identified by a unique identifier that forms the initial part of all NSAP addresses and NETs in those sub-ordinate domains. This initial part is known as the initial domain part (IDP). The IDP itself is defined as comprising two parts: an authority format identifier (AFI) and an initial domain identifier (IDI). The AFI identifies the format and allocation procedures for the IDI and the format of the remainder of the NSAP address.

Note 2.— The ATN network addressing domain is such a sub-ordinate network addressing domain and has an IDP that uses an ISO 6523-ICD IDI.

Note 3.— The IDP is always expressed as decimal digits. However, ISO/IEC 8348 permits NSAP addresses in an ISO 6523-ICD domain to have either a binary or a decimal format for the remainder of the address – the domain specific part (DSP). The format of the DSP is determined by the AFI.

3.4.3.4.1 All ATN NSAP addresses shall have an AFI with the value 47 decimal.

Note.— This AFI value is defined by ISO/IEC 8348 to imply an ISO 6523-ICD IDI with a binary format DSP.

3.4.3.4.2 All ATN NSAP addresses shall have an IDI value of 0027 decimal.

Note.— This value has been allocated by ISO to ICAO under the ISO 6523-ICD scheme. An IDP of 470027 therefore forms the common NSAP address prefix to all ATN NSAP addresses and effectively defines the ATN network addressing domain, as a sub-domain of the global network addressing domain.

3.4.3.5 The reference publication format

Note.— The reference publication format is defined by ISO/IEC 8348 for the publication of NSAP addresses and NETs in a form suitable for text documents.

3.4.3.5.1 For the purposes of publication in a text format, ATN NSAP addresses and NETs should be written as the character sequence “470027+”, identifying the common prefix for all ATN NSAP addresses, followed by the DSP expressed as a sequence of hexadecimal characters.

Note.— The “+”sign is used as a separator between the decimal syntax IDP and the hexadecimal syntax DSP.

3.4.3.5.2 Each successive pair of hexadecimal digits shall correspond to the next binary octet of the DSP.

3.4.3.6 The ATN NSAP address format

Note 1.— The derivation of the ATN NSAP address format is illustrated in Figure 3-6. This starts with the AFI and IDI fields required by ISO/IEC 8348. It ends with the system ID (SYS) and SEL fields required by ISO/IEC 10589. The remaining DSP fields are specified below and used to coordinate the allocation of ATN NSAP addresses.

Note 2.— The VER field is used to partition the ATN addressing domain into a number of sub-ordinate addressing domains, each of which provides a different approach to address management.

Note 3.— The ADM field is then used to break down each such partition into a number of sub-ordinate addressing domains, each of which may then be managed by a different manager.

Note 4.— In fixed network addressing domains, the ARS field may then be used to identify a network addressing domain that will correspond to each routing domain under the control of each such manager, and the LOC field may then be used to identify each routing area within each routing domain.

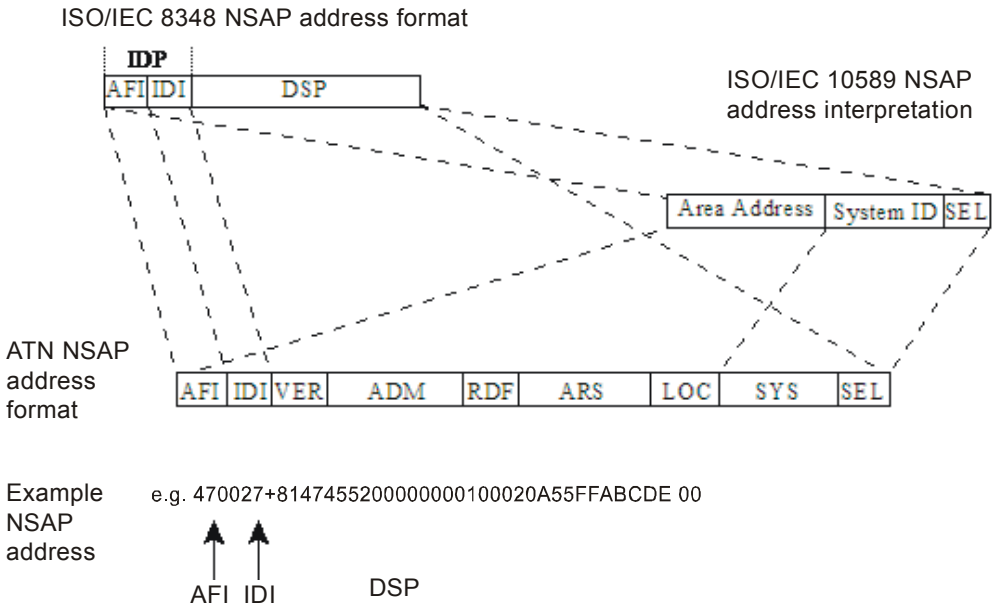


Figure 3-6. Derivation of the ATN NSAP address format

Note 5.— In mobile network addressing domains, the ARS field identifies an aircraft. Where all ATN systems onboard an aircraft form a single routing domain, the ARS field also identifies the addressing domain that will correspond to that routing domain, and the LOC field is used as above. However, when the ATN systems on board a single aircraft form more than one routing domain, then part of the LOC field is also used to identify such an addressing domain.

Note 6.— The reason for the existence of the RDF field is historical.

3.4.3.7 NSAP address encoding

Note 1.— In ISO/IEC 8348 terms, the IDP has an abstract decimal syntax, and the DSP has an abstract binary syntax. The reason for the use of the word abstract is to emphasize the fact that the actual encoding is outside of the scope of ISO/IEC 8348 and instead is the responsibility of the standards that specify the encoding of network layer protocols.

Note 2.— ISO/IEC 8348 does, however, describe two possible encoding schemes, the "preferred binary encoding" and the "preferred decimal encoding". ISO/IEC 8473 mandates the use of the preferred binary encoding for CLNP, while ISO/IEC 10747 mandates a modified version of the preferred binary encoding in order to cope with bit aligned NSAP address prefixes.

Note 3.— In consequence, this specification only specifies how each field of the DSP is allocated as an unsigned binary number. The actual encoding of the resulting bitstring in an NPDU is then according to the applicable protocol specification.

3.4.3.8 Allocation of the DSP

Note.— The DSP fields of an ATN NSAP address are the VER, ADM, RDF, ARS, LOC, SYS and SEL fields. The size of each of these fields is given in Table 3-4.

Table 3-4. DSP NSAP address field sizes

Address field name	*Address field size*
VER	1 octet
ADM	3 octets
RDF	1 octet
ARS	3 octets
LOC	2 octets
SYS	6 octets
SEL	1 octet

3.4.3.8.1 The Version (VER) field

Note 1.— The purpose of the VER field is to partition the ATN network addressing domain into a number of sub-ordinate addressing domains.

Note 2.— The values currently specified for the VER field and the network addressing domains so defined, are summarized in Table 3-5.

Table 3-5. VER field assigned values

VER field value	*Network addressing domain*	*Common NSAP address prefix for domain*
[0000 0001]	Fixed AINSC	470027+01
[0100 0001]	Mobile AINSC	470027+41
[1000 0001]	Fixed ATSC	470027+81
[1100 0001]	Mobile ATSC	470027+C1

3.4.3.8.1.1 The VER field shall be one octet in length.

3.4.3.8.1.2 A VER field value of [0000 0001] shall be used for all NSAP addresses and NETs in the network addressing domain that comprises all fixed AINSC NSAP addresses and NETs.

Note.— The NSAP address prefix "470027+01" is therefore the common NSAP address prefix for the fixed AINSC network addressing domain.

3.4.3.8.1.3 A VER field value of [0100 0001] shall be used for all NSAP addresses and NETs in the network addressing domain that comprises all mobile AINSC NSAP addresses and NETs.

Note.— The NSAP address prefix "470027+41" is therefore the common NSAP address prefix for the mobile AINSC network addressing domain.

3.4.3.8.1.4 A VER field value of [1000 0001] shall be used for all NSAP addresses and NETs in the network addressing domain that comprises all fixed ATSC NSAP addresses and NETs.

Note.— The NSAP address prefix "470027+81" is therefore the common NSAP address prefix for the fixed ATSC network addressing domain.

3.4.3.8.1.5 A VER field value of [1100 0001] shall be used for all NSAP addresses and NETs in the network addressing domain that comprises all mobile ATSC NSAP addresses and NETs.

Note.— The NSAP address prefix "470027+C1" is therefore the common NSAP address prefix for the mobile ATSC network addressing domain.

3.4.3.8.1.6 All other VER field values shall be reserved.

3.4.3.8.2 The Administration (ADM) field

3.4.3.8.2.1 *General*

Note.— The purpose of the ADM field is to subdivide each of the network addressing domains introduced by the VER field into a further set of sub-ordinate network addressing domains and to permit devolved administration (i.e. address allocation) of each resulting domain to an individual State or organization.

The ADM field shall be three octets in length.

3.4.3.8.2.2 *Fixed AINSC NSAP addresses and NETs*

Note.— In the fixed AINSC network addressing domain, the ADM field is used to subdivide this addressing domain into a number of sub-ordinate network addressing domains, each of which comprises NSAP addresses and NETs for fixed systems operated by a single AINSC organization.

3.4.3.8.2.2.1 Allocation of NSAP addresses and NETs in each such network addressing domain subordinate to the fixed AINSC network addressing domain shall be the responsibility of the organization identified by the value of the ADM field.

3.4.3.8.2.2.2 The field value should be derived from the set of three-character alphanumeric symbols representing an IATA airline or aeronautical stakeholder designator, according to 3.4.1.4.

Note.— AINSC organizations are intended to register their ADM values with IATA.

3.4.3.8.2.3 *Fixed ATSC NSAP addresses and NETs*

Note.— In the fixed ATSC network addressing domain, the ADM field is used to subdivide this addressing domain into a number of sub-ordinate network addressing domains, each of which comprises NSAP addresses and NETs for fixed systems operated by a single State or within an ICAO Region.

3.4.3.8.2.3.1 Allocation of NSAP addresses and NETs in each such network addressing domain subordinate to the fixed ATSC network addressing domain shall be the responsibility of the State or ICAO Region identified by the value of the ADM field.

3.4.3.8.2.3.2 When used for identifying a State, the ADM field shall be derived from the State's three-character alphanumeric ISO 3166 country code, represented as upper case characters.

3.4.3.8.2.3.3 In this case, the value of the field shall be determined according to 3.4.1.4.

Note.— For example, the encoding of "GBR" is 474252 in hexadecimal. Therefore the NSAP address prefix 470027+81474252 is the common NSAP address prefix for all NSAP addresses and NETs in the UK fixed ATSC network addressing domain.

3.4.3.8.2.3.4 When used to identify an ICAO Region, the first octet of the ADM field shall identify the ICAO Region, according to Table 3-6, while the values of the remaining two octets shall be assigned by the identified ICAO Region.

Table 3-6. ICAO Region identifiers

ADM Field First Octet	*ICAO Region*
[1000 0000]	Africa
[1000 0001]	Asia
[1000 0010]	Caribbean
[1000 0011]	Europe
[1000 0100]	Middle East
[1000 0101]	North America
[1000 0110]	North Atlantic
[1000 0111]	Pacific
[1000 1000]	South America

Note 1.— The ISO 3166 character codes are always represented as binary octets, each of which has a zero most significant bit. Therefore, it is possible to guarantee that the field values listed in Table 3-6 do not conflict with ISO 3166 derived State identifiers.

Note 2.— This addressing plan enables ICAO Regions to allocate ADM field values in the fixed ATSC network addressing domain to States and Organizations within the ICAO Region in a structured manner. This is in order to permit the efficient advertisement of routing information, for example, in the advertisement of routes to "all RDs in the same ATN island" as recommended in 3.3.7.1.4.2.

3.4.3.8.2.3.5 All ADM field values in the fixed ATSC network addressing domain that do not correspond to valid ISO 3166 country codes or which are not assigned to ICAO Regions shall be reserved.

3.4.3.8.2.4 *Mobile NSAP addresses and NETs*

Note.— In both the mobile AINSC and the mobile ATSC network addressing domains, the ADM field is used to subdivide this addressing domain into a number of sub-ordinate network addressing domains, each of which comprises NSAP addresses and NETs for mobile systems operated by a single airline or onboard the general aviation aircraft of a single State.

3.4.3.8.2.4.1 For mobile AINSC NSAP address and NETs, the ADM field value shall be set according to §3.4.3.8.2.2, and the corresponding sub-ordinate network addressing domain administered by the organization identified by the value of the ADM field.

3.4.3.8.2.4.2 For mobile ATSC NSAP address and NETs, the ADM field value shall be set according to §3.4.3.8.2.3, and the corresponding sub-ordinate network addressing domain administered by the State identified by the value of the ADM field.

3.4.3.8.3 The Routing Domain Format (RDF) field

Note 1.— There is no absolute requirement for the remainder of the DSP in each of the above defined network addressing domains to be allocated according to a coordinated addressing plan, or for even the same fields to exist, or the NSAP addresses to have the same length. However, in order to encourage common equipment development, this specification specifies the existence, size and use of the RDF, ARS and LOC fields.

Note 2.— The reason for the existence of the RDF field is historical.

3.4.3.8.3.1 The RDF field shall be one octet in length and its value shall be [0000 0000] in binary.

3.4.3.8.3.2 All other values shall be reserved.

3.4.3.8.4 The Administrative Region Selector (ARS) field

Note 1.— In fixed network addressing domains, the purpose of the ARS field is to distinguish routing domains or routing domains and subordinated routing areas respectively operated by the same State or organization.

Note 2.— In mobile network addressing domain, the purpose of the ARS field is to identify the aircraft on which the addressed system is located. When the systems on board an aircraft form a single routing domain, then the ARS field also identifies the routing domain. When the systems on board an aircraft form multiple RDs, then part of the LOC field is used to distinguish them.

3.4.3.8.4.1 The ARS field shall be three octets in length.

3.4.3.8.4.2 In the fixed AINSC and ATSC network addressing domains, the value of the ARS field shall be a 24-bit unsigned binary number which is used to uniquely identify a routing domain or a routing domain and a subordinated routing area, respectively.

Note.— A State or organization may choose to use either the most significant 8 bits, the most significant 16 bits or all 24 bits of the ARS field to uniquely distinguish its routing domains.

3.4.3.8.4.3 In the case that the body responsible for the assignment of the ARS field chooses to use only the leading bits of the ARS field to distinguish its routing domains, the remaining part of the ARS field shall, together with the LOC field (see §3.4.3.8.5), be used to uniquely identify the routing areas within those routing domains.

3.4.3.8.4.4 In the fixed AINSC and ATSC network addressing domains, the State or organization identified by the value of the ADM field shall be responsible for assigning the ARS field.

Note 1.— For example, 470027+8147425200000000 and 470027+8147425200000001 are therefore NSAP address prefixes common to all NSAP addresses and NETs assigned to fixed systems in two distinct routing domains operated by the UK ATSC authority.

Note 2.— Where necessary, the allocation of NSAP addresses and NETs may thus readily be delegated to a network administrator responsible for each network addressing domain that corresponds to each routing domain.

3.4.3.8.4.5 In mobile AINSC and ATSC network addressing domains, the value of the ARS field shall be the 24-bit ICAO aircraft address that uniquely identifies the NSAP addresses and NETs in a single routing domain.

Note 1.— If the aircraft is operated by an IATA airline then the NSAP address or NET is in a mobile AINSC network addressing domain.

Note 2.— For general aviation aircraft, the NSAP address or NET is in a mobile ATSC network addressing domain.

3.4.3.8.5 The Location (LOC) field

Note 1.— In fixed network addressing domains, the purpose of the LOC field is to distinguish routing areas within the same routing domain.

Note 2.— In mobile network addressing domains, the LOC field is used:

a) to distinguish routing areas within the same mobile routing domain; or,

b) when more than one routing domain is located on a single aircraft, to distinguish each routing domain and the routing areas contained within them.

Note 3.— For example, the first octet of the LOC field may be used to distinguish each routing domain on board a single aircraft, and the second octet to distinguish each routing area.

Note 4.— The combination of AFI, IDI, VER, ADM, RDF, ARS and LOC fields therefore forms an area address.

3.4.3.8.5.1 The LOC field shall be two octets in length and may be given any binary value.

3.4.3.8.5.2 The administrator of the network addressing domain that coincides with the routing domain in which a given routing area is located shall be responsible for the allocation of a LOC field value that provides a unique area address for that routing area.

Note.— For example, 470027+81474252000000010045 is an area address in a routing domain operated by the UK ATSC Administration.

3.4.3.8.6 The System Identifier (SYS) field

Note.— ISO/IEC 10589 defines the system identifier as a variable length field which uniquely identifies an end or intermediate system within a ISO/IEC 10589 routing area. Within a routing area, all system identifiers are of the same length, although a router is not able to make assumptions about the length of this field outside of its own routing area. However, the ATN addressing plan does specify this field to always be six octets in length in order to encourage a common equipment base.

3.4.3.8.6.1 In an ATN NSAP address or NET, the System Identifier (SYS field) shall be six octets in length.

3.4.3.8.6.2 The value of the SYS field shall be a unique binary number assigned by the addressing authority responsible for the network addressing domain that corresponds with the routing area in which the identified system is located.

Note.— If the system is attached to an IEEE 802 local area network (e.g. an Ethernet), then a common approach is to use the 48-bit LAN address as the value of the SYS field.

3.4.3.8.7 The NSAP Selector (SEL) field

Note.— The NSAP Selector (SEL) field identifies the end system or intermediate system network entity or network service user process responsible for originating or receiving Network Service Data Units (NSDUs).

3.4.3.8.7.1 The SEL field shall be one octet in length.

3.4.3.8.7.2 The SEL field value for an intermediate system network entity shall be [0000 0000], except for the case of an airborne intermediate system implementing the procedures for the optional non-use of IDRP.

3.4.3.8.7.3 In the case of an airborne intermediate system implementing the procedures for the optional non-use of IDRP, the SEL field value shall be [1111 1110].

3.4.3.8.7.4 The SEL field value [1111 1111] shall be reserved.

Note 1.— In an intermediate system, any other SEL field value may be assigned to NSAPs. The actual value chosen is a local matter.

Note 2.— SEL field values in stand-alone end systems (i.e. in end systems not co-located with intermediate systems) are not constrained.

3.4.3.8.7.5 SEL field values other than those defined for intermediate system network entities in ⁋3.4.3.8.7.2 and ⁋3.4.3.8.7.3 or being reserved, shall be assigned by the addressing authority responsible for the identified end or intermediate system.

3.4.3.9 Pre-defined NSAP address prefixes

3.4.3.9.1 All AINSC mobiles

The NSAP address prefix 470027+41 shall provide a common NSAP address prefix for all AINSC mobiles.

3.4.3.9.2 All ATSC mobiles

The NSAP address prefix 470027+C1 shall provide a common NSAP address prefix for all ATSC mobiles.

Note.— The NLRI for the default route to all mobiles comprises both the NSAP address prefixes defined above.

3.4.3.9.3 All aircraft belonging to an airline

The NSAP address prefix 470027+41 plus the value of the ADM field assigned to the airline shall provide a common NSAP address prefix for all AINSC mobiles operated by a single airline.

Note.— The NLRI for the route to the "home" for the aircraft belonging to a given airline contains this NSAP address prefix.

3.4.3.9.4 All general aviation and other types of aircraft registered by a State

The NSAP address prefix 470027+C1 plus the value of the ADM field assigned to the State shall provide a common NSAP address prefix for all ATSC mobiles registered by a single State.

Note.— The NLRI for the route to the "home" for the general aviation and other types of aircraft registered by a single State contains this NSAP address prefix.

3.5 TRANSPORT SERVICE AND PROTOCOL SPECIFICATION

3.5.1 General

3.5.1.1 Overview

3.5.1.1.1 The COTP (Connection Oriented Transport Protocol) shall be used to provide an end-to-end reliable data transfer service between transport service users on two ATN end systems.

3.5.1.1.2 In ATN end systems, the implementation of the COTP shall conform to ISO/IEC 8073 and the mandatory requirements given in this chapter.

3.5.1.1.3 The CLTP (Connectionless Mode Transport Protocol) shall be used to provide a connectionless data transfer service between transport service users on two ATN end systems.

3.5.1.1.4 In ATN End Systems, the implementation of the CLTP shall conform to ISO/IEC 8602 and the mandatory requirements given in this chapter.

Note.— The transport protocols specified for use in ATN end systems provide both connection mode and connectionless mode communication services. The implementation and use of a particular mode of the transport layer service depends on the requirements of the application(s) supported by a given ATN end system.

3.5.1.2 Transport service description

Note 1.— When the TS-user requires use of the connection mode transport service the TS-user will provide the following information to the TS-provider on a per transport connection basis:

a) called and calling TSAP address;

b) whether or not the expedited data option is required;

c) the required residual error rate (RER) to determine whether use or non-use of the transport checksum is required, or whether the extended 32-bit checksum is to be used;

d) the application service priority to be mapped into the resulting CLNP NPDUs according to Annex 10, Volume III, Part 1, Chapter 3, Table 3-1;

e) the ATN security label specifying the ATN traffic type, i.e.

- *ATN operational communications;*
- *ATN administrative communications;*
- *General communications;*
- *ATN systems management communications.*

Note 2.— In the case where the traffic type specified is ATN operational communications the TS-user will additionally provide the traffic category, i.e. air traffic services communications (ATSC) or aeronautical operational control (AOC).

Note 3.— In the case of the ATSC traffic category the TS-user will further specify the required ATSC class as defined in Table 3-2, or no traffic type policy preference.

Note 4.— In the case of the AOC traffic category the TS-user will further specify the subnetwork preference (including no preference).

Note 5.— The ATN traffic types and their associated traffic categories are specified in Table 3-9. The encoding of the ATN security label is specified in Figure 3-7 and 3.6.2.2.2.2 bullet b).

Note 6.— The TS-user is not required to specify any other transport service Quality of Service parameters.

3.5.1.3 Transport service access point addresses

3.5.1.3.1 A TSAP address shall comprise two elements, a NSAP address and a TSAP selector.

3.5.1.3.2 The NSAP address and the TSAP selector shall conform to the provisions in 3.4.

3.5.1.4 Exchange of transport-selector parameters

Note.— TSAP selectors are transmitted in calling and called transport-selector parameters in COTP, and in source and destination transport-selector parameters in CLTP.

3.5.1.4.1 The transport entity shall support transport-selector parameters to accommodate the ATN TSAP selector syntax and encoding requirements as specified in 3.4.

3.5.1.4.2 The transport entity should support remote transport-selector parameters of variable size from 0 up to 32 octets using any encoding and any value.

Note.— The absence of a calling and called transport-selector assumes the network address alone unambiguously defines the transport address.

3.5.1.4.3 In COTP, on receipt of CR (Connection Request) TPDU, the absence of a calling or called transport-selector shall be treated as equivalent to a zero length calling or called transport-selector.

3.5.1.4.4 The absence of a calling or called transport-selector in a received CC (Connection Confirm) TPDU shall indicate that calling or called transport-selector is equivalent to the corresponding parameter specified in the sent CR TPDU.

3.5.1.4.5 When present in a received CC TPDU, calling and called transport-selector parameters shall be identical in length and value to the corresponding parameter specified in the sent CR TPDU.

3.5.1.4.6 In CLTP, on receipt of UD (User Data) TPDU, the absence of a source or destination transport-selector shall be treated as equivalent to a zero length source or destination transport-selector.

3.5.2 Connection mode transport layer operation

3.5.2.1 Connection mode transport service primitives

Note 1.— For the purpose of describing the notional interfaces between different OSI protocol layers, each protocol layer is assumed to provide a service to the next higher protocol layer. The assumed service provided by the ATN transport layer to its user is described in ISO/IEC 8072.

Note 2.— ATN applications may specify their use of the COTP implemented in ATN end systems using the transport service specified in ISO/IEC 8072, including use of ATN priority, and security parameters as defined in this specification.

Note 3.— There is no requirement to implement the service specified in ISO/IEC 8072 as a software interface.

3.5.2.2 ATN specific requirements

3.5.2.2.1 ATN end systems shall implement the ISO/IEC 8073 Class 4 transport protocol in order to provide connection mode communications over the ATN Internet.

3.5.2.2.2 The COTP shall operate using the CLNS (Connectionless Network Service) as specified in 3.6.

Note.— TPDUs (Transport Protocol Data Units) are sent via the N-UNITDATA request primitive.

3.5.2.2.3 The transport entity shall not concatenate TPDUs from TCs with different transport priorities or different security labels.

3.5.2.2.4 The selective acknowledgement mechanism should be used for conservation of bandwidth by preventing retransmission of correctly received out-of-sequence TPDUs.

3.5.2.2.5 The request of acknowledgement mechanism should be used to reduce AK traffic.

3.5.2.2.6 The maximum TPDU size should be at least 1 024 octets.

Note.— This is to support efficient transmission of anticipated application data exchanges.

3.5.2.2.7 The transport layer should propose a TPDU size of at least 1 024 octets.

3.5.2.2.8 The transport layer should use the TPDU size parameter rather than the preferred maximum TPDU size parameter.

3.5.2.2.9 Implementations of the ATN transport layer should propose use of normal format in the CR TPDU.

3.5.2.2.10 The extended format should only be proposed when explicitly necessary to meet application Quality of Service requirements.

Note.— Because the increased TPDU size resulting from use of extended data TPDU numbering may be more inefficient, this option is used on a TC only when absolutely required.

3.5.2.2.11 The transport layer should accept non-use of checksum when proposed in a CR TPDU.

3.5.2.2.12 Implementations of the transport protocol shall support configurable values for all timers and protocol parameters, rather than having fixed values, in order to allow modification as operational experience is gained.

3.5.2.2.13 When intended for operation over air-ground subnetworks, transport protocol implementations shall support the minimum–maximum ranges for COTP timer values as presented in Table ⁋3-7.

3.5.2.2.13.1 When intended for operation over air-ground subnetworks, the nominal values indicated in Table ⁋3-7 should be used to initialize the COTP timers and protocol parameters.

Note.— The local retransmission time (T1) is dynamically updated as a function of the round-trip time measured on a given transport connection (see ⁋3.5.2.8). The recommended algorithms for the dynamic computation of the local retransmission time are specified in ⁋3.5.2.8.

3.5.2.2.13.2 The assignment of initial values for timers and parameters other than the nominal values indicated in Table ⁋3-7 should be based on operational experience.

3.5.2.2.14 When intended for operation exclusively over ground-ground subnetworks, implementations of transport protocol timer values should be optimized to ensure interoperability.

Table 3-7. COTP timer value ranges

Name	*Description*	*Minimum value*	*Nominal value*	*Maximum value*
M_{RL}, M_{LR}	NSDU lifetime, seconds	26	400	600
E_{RL}, E_{LR}	Maximum transit delay, seconds	1	100	150
A_L, A_R	Acknowledgement time, seconds	0	1	400
T1	Local retransmission time, seconds	2	202	701
R	Persistence time, seconds	1	405	6 310
N	Maximum number of transmissions	1	3	10
L	Time bound on reference and/or sequence numbers, seconds	160	1 206	7 910
I	Inactivity time, seconds	600	4 500	6 000
W	Window time, seconds	160	4 000	5 500

Note 1.— In Table 3-7, the subscripts "R" and "L" refer to "remote" and "local", respectively. The variable E_{RL}, for example, refers to the maximum transit delay from the remote entity to the local entity. The variable E_{LR} is the maximum transit delay from the local entity to the remote entity. It is assumed that these values may be different.

Note 2.— The initial, minimum and maximum values of several of the timers and variables listed in Table 3-7 may not be directly configurable. They may be determined based on the relationships defined in clause 12.2.1.1 of ISO/IEC 8073.

3.5.2.3 Connection mode transport Quality of Service

3.5.2.3.1 Connection mode transport priority

3.5.2.3.1.1 The transport layer shall allow a TC (Transport Connection) priority in the range [0 - 14].

3.5.2.3.1.2 The transport layer shall not alter the proposed TC priority specified by the TS-user.

3.5.2.3.1.3 The transport layer shall treat all connections without expressed priority as being at the default TC priority.

3.5.2.3.1.4 The default TC priority shall be the lowest priority, i.e. priority **[14]**.

3.5.2.3.1.5 When a TS-user specifies a TC priority, the relationship between this TC priority and the CLNP priority shall be as specified in Annex 10, Volume III, Part 1, Chapter 3, Table 3-1.

3.5.2.3.2 Connection mode transport security

Note.—The ATN security mechanism does not make use of the ISO/IEC 8073 protection parameter. The support of the protection parameter is therefore optional.

3.5.2.3.2.1 The transport layer shall allow a TS-user to specify a security label for a transport connection. The transport security procedure shall be implemented as specified in 3.2.7.3.1.

3.5.2.3.2.2 The security label format shall be according to 3.2.7.1. The transport layer shall not alter the security label specified by the TS-user.

Note.— When no security label is present, a "General Communications" traffic type is implied. In this case, CLNP NPDUs are generated without the security parameter.

3.5.2.3.3 Connection mode residual error rate

Note.— Three qualitative levels of RER are defined for use with the connection mode transport service. These correspond to no checksums, the use of the 16-bit checksum specified in ISO/IEC 8073, and the use of the extended 32-bit checksum described in this specification.

3.5.2.3.3.1 The transport layer shall allow a TS-user to specify a residual error rate as three qualitative levels, i.e. low, medium and high.

3.5.2.3.3.2 When supported, a low residual error rate shall correspond to the use of the extended 32-bit checksum described in 3.5.4. Otherwise, a low residual error rate shall be equivalent to a medium residual error rate.

3.5.2.3.3.3 A medium residual error rate shall correspond to the use of the 16-bit TPDU checksum specified in ISO/IEC 8073.

3.5.2.3.3.4 A high residual error rate shall correspond to non-use of any transport layer checksum.

3.5.2.4 Encoding of transport protocol data units

3.5.2.4.1 General

The encoding of TPDUs shall conform to ISO/IEC 8073 for the COTP.

3.5.2.4.2 Encoding of the acknowledgment time parameter

In ATN-compliant systems, the acknowledgement time parameter of the CR and CC TPDUs shall be encoded as follows:

Parameter code: 1000 0101

Note 1.— This is identical to the ISO/IEC 8073 standard parameter.

Parameter length: 2 or 3 octets.

Parameter value: Acknowledgment Timer (A_L) value expressed in milliseconds (per ISO/IEC 8073 standard)

Note 1.— This enhancement is in response to the unique requirements of the aeronautical environment which may require longer acknowledgment times than foreseen in ISO/IEC 8073.

Note 2.— Initial values of these timers may depend upon the subnetwork, traffic type and routing policy requirements expressed in the associated ATN security label.

Note 3.— In cases where the A_L value is expressed in 2 octets (less than 65 536 milliseconds), the ATN implementation will behave in compliance with the ISO/IEC 8073 standard.

Note 4.— Implementors are advised to permit systems administrators to readily specify initial values.

3.5.2.4.3 Encoding of the extended 32-bit checksum parameter

The extended 32-bit checksum parameter shall be encoded as a variable part TPDU parameter using the following format:

Parameter code: 0000 1000, indicating extended 32-bit checksum parameter

Parameter length: 4

Parameter value: Result of the checksum algorithm as specified in 3.5.4.5

Note 1.— When supported, the parameter is included in a CR TPDU and is thereafter included in all other TPDUs except when the connection responder indicates non-support of the parameter by omitting it from the variable part of the CC TPDU.

Note 2.— This parameter is not defined by ISO/IEC 8073. However, it is not a protocol error to use it in a CR TPDU as the ISO standard explicitly requires unknown options parameters in CR TPDUs to be ignored if unrecognized. Hence, as long as this parameter is only used in other TPDUs when both initiator and receiver indicate support by including it in the CR TPDU, and in a CC TPDU in response to such a CR TPDU, its implementation will not result in interoperability problems.

Note 3.— Parameter codes with bits 7 and 8 set to zero are explicitly not assigned by ISO/IEC 8073, but nor is their use precluded. It is theoretically possible that another non-ATN implementation may make alternative use of the same parameter code. Such implementations will not be interoperable with ATN implementations as CR TPDUs containing such a parameter will be ignored as the expected checksum will not verify as correct.

3.5.2.5 Transport layer congestion avoidance

3.5.2.5.1 General

Note 1.— The congestion avoidance mechanisms in the transport layer make use of the notification by the network layer of congestion experienced flags in received NPDUs. This mechanism allows transport entities to reduce the window, i.e. the number of DT TPDUs allowed to be sent without acknowledgement, when the proportion of NPDUs indicating congestion reaches a certain threshold.

Note 2.— This congestion information consists of the total length of the sequence of NPDUs forming the associated NSDU, and the number of NPDUs of that sequence that had their congestion experienced flag set upon reception.

Note 3.— Transport congestion avoidance measures are applicable to the connection mode transport service only.

3.5.2.5.1.1 The transport entity shall implement the congestion avoidance algorithm defined in this section.

3.5.2.5.1.2 This algorithm shall be applied for each transport connection individually.

3.5.2.5.2 Advertised window

3.5.2.5.2.1 *General*

A receiving transport entity shall provide the sending transport entity with the lower window edge and the size of the advertised window (W) by using the explicit flow control mechanisms specified in ISO/IEC 8073.

*Note.— The **advertised window** is the window advertised by the receiver of the data to the sender of the data. It indicates the number of DT TPDUs that the receiver is willing to accept.*

3.5.2.5.2.2 *Initialization of the advertised window*

3.5.2.5.2.2.1 The initial value of the window W_0 that is advertised to the sending transport entity shall have a locally configurable value.

3.5.2.5.2.2.2 This initial window shall be sent to the sending transport entity in the first CDT field transmitted.

3.5.2.5.3 Receiving transport entity congestion avoidance

3.5.2.5.3.1 *General*

3.5.2.5.3.1.1 Congestion avoidance shall be performed within repeated update phases.

3.5.2.5.3.1.2 Each update phase shall terminate with the possible advertisement of a new window size to the sending transport entity.

3.5.2.5.3.2 *Start of update phase*

An update phase of the advertised window shall start after the receiving transport entity has advertised a new value of the window W_{new} to the sending transport entity.

3.5.2.5.3.3 *Ignoring congestion information*

3.5.2.5.3.3.1 After having advertised a new window size, the receiving transport entity shall ignore congestion information coming from the network layer, until it has received W (i.e. the « old » advertised window size) further DT-TPDUs. It then shall enter the sampling sub-phase.

3.5.2.5.3.3.2 When the sending transport entity advertises the initial window size W_0, it shall set W to 0.

3.5.2.5.3.4 *Sampling congestion information*

3.5.2.5.3.4.1 The receiving transport entity shall maintain a count N equal to the total number of NPDUs that convey DT-TPDUs, and a count NC equal to the number of such NPDUs that had their congestion experienced flag set upon reception.

3.5.2.5.3.4.2 Upon entering the sampling sub-phase, these counts shall be reset to zero.

3.5.2.5.3.4.3 These counts shall be updated upon receipt of a DT-TPDU using the congestion information supplied by the network layer.

3.5.2.5.3.4.4 The sampling sub-phase shall end as soon as the transport entity has received W_{new} DT-TPDUs within the sampling sub-phase. The end of the sampling sub-phase also terminates the update phase.

3.5.2.5.3.5 *Action upon the end of the update phase*

The receiving transport entity shall take the following actions at the end of each update phase:

a) if the count *NC* is less than λ % of the count *N*, the receiving transport entity shall increase the size of the advertised window by adding δ up to a maximum based on the local buffer management policy. Otherwise, it shall decrease the size of the advertised window by multiplying it by β. If the result of this multiplication has a decimal part, the new window size shall be the truncated to its integer value. The size of the advertised window shall not go to a value smaller than 1.

b) the counts *N* and *NC* shall be reset to 0.

c) the new window size shall be transmitted to the sending transport entity in accordance with the explicit flow control mechanisms specified in ISO/IEC 8073.

Note.— This procedure does not explicitly require the reduction of the upper window edge, as it is possible to gradually reduce the credit window.

3.5.2.5.4 Recommended algorithm values

The value settings defined in Table 3-8 should be implemented and configurable by a System Manager:

Table 3-8. Congestion avoidance algorithm values

Name	*Description*	*Recommended value/range*
®	Window decrease factor	0.75 to 0.95
δ	Window increase amount	1
W_0	Initial window	1
⌊	Congestion ratio	50 per cent

3.5.2.6 Use of the ATN network service

Note.— This section specifies how the COTP operates over the CLNS provided by the ATN network layer.

3.5.2.6.1 Use of the N-UNITDATA request

3.5.2.6.1.1 *General*

3.5.2.6.1.1.1 The transport layer shall use the N-UNITDATA request primitive, as defined in ISO/IEC 8073, to transmit TPDUs.

Note.— The way the parameters are exchanged between the transport entity and the network service is a local matter.

3.5.2.6.1.1.2 The length indication given to the network service shall be equal to the length of the TPDU(s).

Note.— The maximum size of each TPDU is restricted to the locally defined maximum NSDU size.

3.5.2.6.1.2 *NS-user-data*

Note.— Transport entities transmit TPDUs as NS-user-data of the N-UNITDATA request primitive.

3.5.2.6.1.3 *Network service access point addresses*

Note.— The transport layer has knowledge of the source and destination address parameters only as octet strings.

3.5.2.6.1.4 *Network Quality of Service*

3.5.2.6.1.4.1 *General*

The COTP shall use the network QoS parameters as defined in the sections below.

3.5.2.6.1.4.2 *Network layer priority*

3.5.2.6.1.4.2.1 The COTP shall use the network priority parameter to indicate the relative priority of a NSDU.

3.5.2.6.1.4.2.2 When a transport priority has been specified, the value of network priority shall be determined based on the transport connection priority, as defined in Annex 10, Volume III, Part 1, Chapter 3, Table 3-1.

3.5.2.6.1.4.2.3 If the transport layer supports levels of TC priority numerically greater than 14, TPDUs associated with the TC shall be transmitted using a network priority level of zero.

Note.— As specified in ISO/IEC 8073, the transport layer priority level zero is highest. ISO/IEC 8473 specifies zero as the lowest network priority and fourteen as the highest. Annex 10, Volume III, Part 1, Chapter 3, Table 3-1 defines the required mapping between these two schemes for use by ATN systems.

3.5.2.6.1.4.3 *Network layer security*

Note.— The use of the network layer security is specified in 3.2.7.4.

3.5.2.6.2 Use of the N-UNITDATA indication

3.5.2.6.2.1 *General*

The transport layer shall be capable of receiving TPDUs from the ATN network service using the N-UNITDATA indication primitive, as defined in ISO/IEC 8073.

Note.— The way the parameters are exchanged between the transport entity and the Network Service is a local matter.

3.5.2.6.2.2 *NS-user-data*

Note.— Transport entities receive TPDUs as NS-user-data of the N-UNITDATA indication primitive.

3.5.2.7 Connection mode transport APRL

3.5.2.7.1 Mandatory and optional functions

3.5.2.7.1.1 *General*

Note.— The requirements for the COTP are provided in the form of an ATN protocol requirements list (APRL). The APRL has been prepared using the PICS (Protocol Implementation Conformance Statement) proforma provided with ISO/IEC 8073.

An implementation of the ISO/IEC 8073 transport protocol shall be used in an ATN end system if and only if its PICS is in compliance with the APRL provided in this part of Doc 9880.

3.5.2.7.1.2 *Protocol implementation*

3.5.2.7.1.2.1 Classes implemented

Index	*Class*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
C0	Class 0	14.2	O.1	O
C1	Class 1	14.4	C0:O	O
C2	Class 2	14.2	O.1	O

Index	*Class*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
C3	Class 3	14.3	C2:O	O
C4	Class 4 operation over CONS	14.3	C2:O	O
C4L	Class 4 operation over CLNS	14.3	C2:O	M

3.5.2.7.1.2.2 Specific ATN requirements

Index	*Feature*	*Reference*	*ATN support*
ATN1	Support of congestion avoidance procedures?	§3.5.2.5	M
ATN2	Transport to network priority mapping?	§3.5.2.6.1.4.2	M
ATN3	Support of ATN security label?	§3.5.2.6.1.4.3	M
ATN4	Configurable transport timers?	§3.5.2.2.12	M
ATN5	Enhanced encoding of acknowledgment time parameter?	§3.5.2.4.2	M
ATN6	Support of extended 32-bit checksum?	§3.5.4	M
ATN7	Dynamic local retransmission time adaptation?	§3.5.2.8	M

3.5.2.7.1.3 *Initiator/responder capability for Protocol Classes 0-4*

Index		*ISO/IEC 8073 references*	*ISO status*	*ATN support*
IR1	Initiating CR TPDU	14.5 a)	O.2	M
IR2	Responding to CR TPDU	14.5 a)	O.2	M

3.5.2.7.1.4 *Supported functions*

3.5.2.7.1.4.1 Supported functions for Class 4 (C4 or C4L::)

3.5.2.7.1.4.1.1 Mandatory functions for Class 4

Index	*Function*	*ISO/IEC 8073 References*	*ISO status*	*ATN support*
T4F1	TPDU transfer	6.2	M	M
T4F2	Segmenting	6.3	M	M

Index	*Function*	*ISO/IEC 8073 References*	*ISO status*	*ATN support*
T4F3	Reassembling	6.3	M	M
T4F4	Separation	6.4	M	M
T4F5	Connection establishment	6.5	M	M
T4F6	Connection refusal	6.6	M	M
T4F7	Data TPDU numbering (normal)	6.10	M	M
T4F8	Retention and acknowledgement of TPDUs (AK)	6.13.4.1	M	M
T4F9	Explicit flow control	6.16	M	M
T4F10	Checksum	6.17	M	M
T4F11	Frozen references	6.18	M	M
T4F12	Retransmission on time-out	6.19	M	M
T4F13	Resequencing	6.20	M	M
T4F14	Inactivity control	6.21	M	M

3.5.2.7.1.4.1.2 Mandatory functions for operation over connectionless network service

Index	*Function*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
T4F23	Transmission over CLNS	6.1.2	M	M
T4F24	Normal release when operating over CLNS (explicit)	6.7.2	M	M
T4F25	Association of TPDUs with transport connections when operating over CLNS	6.9.2	M	M
T4F26	Expedited data transfer when operating over CLNS (Network normal)	6.11.2	M	M
T4F27	Treatment of protocol errors when operating over CLNS	6.22.2	M	M

3.5.2.7.1.4.1.3 ISO/IEC 8073 optional functions

Index	*Feature*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
T4F28	Data TPDU numbering (extended)	6.10	O	O
T4F29	Non-use of checksum	6.17	O	M
T4F30	Concatenation	6.4	O	O
T4F31	Retention and acknowledgement of TPDUs Use of selective acknowledgement	6.13.4.4	O	O
T4F32	Retention and acknowledgement of TPDUs Use of request acknowledgement	6.13.4.3	O	O

3.5.2.7.1.5 *Supported TPDUs*

Index	*TPDUs*		*ISO/IEC 8073 References*	*ISO status*	*ATN support*
ST1	CR	supported on transmission	13.1	IR1:M	M
ST2	CR	supported on receipt	13.1	IR2:M	M
ST3	CC	supported on transmission	13.1	IR2:M	M
ST4	CC	supported on receipt	13.1	IR1:M	M
ST5	DR	supported on transmission	13.1	IR2:M	M
ST6	DR	supported on receipt	13.1	IR1:M	M
ST7	DC	supported on transmission	13.1	C4L:M	M
ST8	DC	supported on receipt	13.1	C4L:M	M
ST9	DT	supported on transmission	13.1	M	M
ST10	DT	supported on receipt	13.1	M	M
ST11	ED	supported on transmission	13.1	C4L:M	MO
ST12	ED	supported on receipt	13.1	C4L:M	MO
ST13	AK	supported on transmission	13.1	C4L:M	M
ST14	AK	supported on receipt	13.1	C4L:M	M
ST15	EA	supported on transmission	13.1	C4L:M	MO
ST16	EA	supported on receipt	13.1	C4L:M	MO
ST19	ER	supported on receipt	13.1	M	M

Note 1.— The classification "MO" indicates mandatory to implement, optional to use.

Note 2.— The following table states for which classes, if any, ER TPDU is supported on transmission.

Index	*Class*	*ISO/IEC 8073 reference*	*ISO status*	*ATN support*
SER4L	ER support on transmission of Class 4 over CLNS	6.22.2	O	O

3.5.2.7.1.6 *Supported parameters of issued TPDUs*

3.5.2.7.1.6.1 Parameter values for CR TPDU (C4L::)

Index	*Feature*	*ISO/IEC 8073 reference*	*ISO status*	*ATN support*
ICR1	Bits 8 and 7 in the additional options selection parameter of a CR TPDU set to zero?	13.3.4 g)	M	M

3.5.2.7.1.6.1.1 If the preferred class in the CR is 2,3 or 4:

Index	*Feature*	*ISO/IEC 8073 reference*	*ISO status*	*ATN support*
ICR2	Is class 0 always offered as an alternative class?	14.4	O	X

3.5.2.7.1.6.2 Supported parameters for Class 4 TPDUs (C4L::)

3.5.2.7.1.6.2.1 Optional parameters for a connection request TPDU

Index	*Supported parameters*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4CR7	Called transport-selector	13.3.4 a)	O	M
I4CR8	Calling transport-selector	13.3.4 a)	O	M
I4CR9	TPDU size	13.3.4 b)	O	O
I4CR10	Version number	13.3.4 d)	O	O
I4CR11	Protection parameters	13.3.4 e)	O	O
I4CR12	Additional option selection	13.3.4 g)	O	M

Index	*Supported parameters*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4CR13	Throughput	13.3.4 k)	O	O
I4CR14	Residual error rate	13.3.4 m)	O	O
I4CR15	Priority	13.3.4 n)	O	M
I4CR16	Transit delay	13.3.4 p)	O	O
I4CR17	Acknowledgement time	13.3.4 j)	O	M
I4CR18	Preferred maximum TPDU size	13.3.4 c)	O	O
I4CR19	Inactivity timer	13.3.4 r)	O	M

3.5.2.7.1.6.2.2 Optional parameters for a connection confirm TPDU

Note 1.— According to ISO, the following parameters are optional if a CC TPDU is issued in class 4:

Index	*Supported parameters*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4CC6	Called transport-selector	13.4.4	O	M
I4CC7	Calling transport-selector	13.4.4	O	M
I4CC8	TPDU size	13.4.4	O	O
I4CC9	Protection parameters	13.4.4	O	O
I4CC10	Additional option selection	13.4.4	O	M
I4CC11	Acknowledgement time	13.4.4	O	M
I4CC12	Throughput	13.4.4	O	O
I4CC13	Residual error rate	13.4.4	O	O
I4CC14	Priority	13.4.4	O	M
I4CC15	Transit delay	13.4.4	O	O
I4CC16	Preferred maximum TPDU size	13.4.4	I4CR18:O	O
I4CC17	Inactivity timer	13.4.4	O	M

Note 2.— The support of T4F26 implies that the additional options selection parameter is mandatory.

3.5.2.7.1.6.2.3 Optional parameter for a disconnect request TPDU

Index	*Supported parameter*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4DR4	Additional information	13.5.4 a)	O	O

3.5.2.7.1.6.2.4 Mandatory parameter for a data TPDU

Note.— According to ISO, the following parameter is mandatory in a DT TPDU if request of acknowledgement has been selected.

Index	*Supported parameter*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4DT4	Request of acknowledgement	13.7.3 b)	T4F32:M	T4F32:M

3.5.2.7.1.6.2.5 Optional parameter for an acknowledgement TPDU

Note.— According to ISO, an AK TPDU containing flow control information will be transmitted if an AK TPDU is received under the conditions specified in ISO/IEC 8073 12.2.3.9. The following parameter is mandatory for ATN-compliant systems if an AK TPDU is issued in Class 4.

Index	*Supported parameter*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4AK4	Flow control confirmation	13.9.4 c)	O	M

3.5.2.7.1.6.2.6 Use of the subsequence number parameter in the acknowledgement TPDU

Note.— According to ISO, if an implementation can reduce credit and does so in the manner outlined in ISO/IEC 8073 12.2.3.8.2 then the subsequence number in AK TPDU is mandatory.

Index	*Supported parameters*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4AK5	Subsequence number	13.9.4. b)	O	M

3.5.2.7.1.6.2.7 Use of the selective acknowledgement parameter in the acknowledgement TPDU

Note.— According to ISO, the following parameter is optional in an AK TPDU if selective acknowledgement has been negotiated.

Index	*Supported parameter*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4AK6	Selective acknowledgement parameters	13.9.4. d)	T4F31:O	T4F31:O

3.5.2.7.1.6.2.8 Optional parameters for an error TPDU

Index	*Supported parameter*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
I4ER3	Invalid TPDU	13.12.4 a)	O	O

3.5.2.7.1.7 *Supported parameters for received TPDUs*

Note.— ISO/IEC 8073 requires implementations to be capable of receiving and processing all possible parameters for all possible TPDUs, depending upon the class and optional functions implemented.

TPDUs in Class 4 (C4L::)

Note.— According to ISO, if use of checksum has been selected then it is mandatory to process a checksum parameter in the following TPDUs.

Index	*TPDU*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
R4CCch	CC TPDU	13.4.4	M	M
R4DRch	DR TPDU	13.5.4 b)	M	M
R4DCch	DC TPDU	13.6.4	M	M
R4DTch	DT TPDU	13.7.4	M	M
R4EDch	ED TPDU	13.8.4	M	M
R4AKch	AK TPDU	13.9.4 a)	M	M
R4EAch	EA TPDU	13.10.4	M	M
R4ERch	ER TPDU	13.12.4 b)	M	M

3.5.2.7.1.8 *User data in issued TPDUs*

Class 4 (C4 or C4L::)

Index	*User data*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
D4ICR	User data of up to 32 octets in a CR with preferred class 4	13.3.5	M	M
D4ICC	User data of up to 32 octets in a CC	13.4.5	M	M
D4IDR	User data of up to 64 octets in a DR	13.5.5	M	M

3.5.2.7.1.9 *User data in received TPDUs*

Index	*User data*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
DRCC	32 octets of user data in a CC TPDU	13.4.5	IR1:M	IR1:M
DRDR	64 octets of user data in a DR TPDU	13.5.5	IR1:M	IR1:M
DRCR	32 octets of user data in a CR TPDU	13.3.5	IR2:M	IR2:M

3.5.2.7.1.10 *Negotiation*

Note.— If an option is not returned in the CC, it is considered to have been refused. This allows compatible negotiation between versions of the ISO/IEC 8073 transport protocol.

3.5.2.7.1.10.1 Class negotiation – Initiator

Index	*Feature*	*ISO/IEC 8073 references*	*ATN supported value*
NC	The preferred class in the CR TPDU may contain any of the classes supported by the implementation	6.5.5 j)	Class 4

Note 1.— Negotiation of other protocol classes is out of scope. If this is the only profile supported then it is not possible to negotiate any other protocol class.

Note 2.— The table below specifies valid alternative classes.

Index	*Preferred class*	*ISO/IEC 8073 references*	*ISO allowed values*	*ATN supported values*
NAC5	Class 4 over CLNS	6.5.5 j)	None	None

Note 3.— The class cannot be negotiated since class 4 is the only class allowed over CLNS.

3.5.2.7.1.10.2 Class negotiation – Responder side

Index	*Preferred class*	*ISO/IEC 8073 references*	*ISO allowed responses*	*ATN supported values*
RC4	What classes can you respond with if CR proposes only class 4?	6.5.4 j) Table 3	2,4 or connection refused depending on classes supported	Class 4

Index	*Preferred class*	*ISO/IEC 8073 references*	*ISO allowed responses*	*ATN supported values*
RC4a	What classes can you respond with if CR proposes class 4 as preferred class and the alternative class parameter is present?	6.5.4 j) Table 3	0,1,2,3,4 or connection refused depending on classes supported and coding of alternative class	Class 4

Note.— This table does not preclude connection refusal for other reasons.

3.5.2.7.1.10.3 TPDU size negotiation

Index	*TPDU size*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
TS1	If maximum TPDU size is proposed in a CR TPDU then the initiator shall support all TPDU sizes from 128 octets to the maximum proposed	14.6 e)	I4CR9:M	I4CR9:M
TS2	If the preferred maximum TPDU size parameter is used in a CR TPDU then the initiator shall support all TPDU sizes, except 0, that are multiples of 128 octets up to the preferred maximum proposed	14.6 e)	I4CR18:M	I4CR18:M

Index	*TPDU size*	*ISO/IEC 8073 references*	*ISO allowed values*	*ATN supported values*
TS3	What is the largest value of the preferred maximum TPDU size parameter in a CR TPDU?	14.6 e)	any multiple of 128 octets	any multiple of 128 octets
TS4	What is the largest value of the preferred maximum TPDU size parameter in a CC TPDU?	14.6 e)	any multiple of 128 octets	any multiple of 128 octets

Note.— An implementation of the transport layer can support a preferred maximum TPDU size larger than 1 024 octets.

Index	*TPDU size*	*ISO/IEC 8073 references*	*ISO allowed values*	*ATN supported values*
T4S1	What is the largest value of the maximum TPDU size parameter in a CR TPDU with preferred class 4?	14.6 e)	One of 128, 256, 512, 1 024, 2 048, 4 096, 8 192	One of 128, 256, 512, 1 024, 2 048, 4 096, 8 192

Index	*TPDU size*	*ISO/IEC 8073 references*	*ISO allowed values*	*ATN supported values*
T4S2	What is the largest value of the maximum TPDU size parameter which may be sent in the CC TPDU when class 4 is selected?	14.6 e)	128, 256, 512, 1 024, 2 048, 4 096, 8 192	128, 256, 512, 1 024, 2 048, 4 096, 8 192

3.5.2.7.1.10.4 Use of extended format

Index	*Extended format*	*ISO/IEC 8073 references*	*ISO allowed values*	*ATN supported value*
NEF3	What formats can you propose in the CR TPDU in class 4?	6.5.5 n)	normal, extended	normal, extended
NEF6	What formats can you select in CC when extended has been proposed in CR in class 4?	6.5.5 n)	normal, extended	normal, extended

Note.— This table does not preclude proposal of the extended format.

3.5.2.7.1.10.5 Expedited data transport service

Index	*Expedited data*	*ISO/IEC 8073 references*	*ISO status*	*ATN supported*
TED1	Is the expedited data indication supported in CR and CC TPDU?	6.5.5 r)	M	MO

Note 1.— The classification “MO” indicates mandatory to implement, optional to use.

Note 2.— Expedited data is proposed using the additional options parameters in the CR and CC TPDUs.

3.5.2.7.1.10.6 Non-use of checksum (C4L and T4F29::)

Index	*Non-use of checksum*	*ISO/IEC 8073 references*	*ISO allowed values*	*ATN supported values*
NUC1	What proposals can you make in the CR?	6.5.5 p)	non-use, use	non-use, use
NUC2	What proposals can you make in CC when non-use of checksum has been proposed in CR?	6.5.5 p)	non-use, use	non-use, use

Note 1.— A transport layer is able to propose either use or non-use of checksum in a CR TPDU.

Note 2.— The term “non-use” means that the transport layer may respond accepting non-use of checksum. A transport layer may also respond with use of checksum if non-use has been proposed.

3.5.2.7.1.10.7 Use of selective acknowledgement

Index	*Selective acknowledgement*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
USA1	Is use of selective acknowledgement proposed in CR TPDUs ?	6.5.5 s)	O	O
USA2	Is use of selective acknowledgement selected in a CC when it has been proposed in a CR ?	6.5.5 s)	O	O

3.5.2.7.1.10.8 Use of request acknowledgement

Index	*Request of acknowledgement*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
ROA1	Is use of request of acknowledgement proposed in CR TPDUs ?	6.5.5 t)	O	O
ROA2	Is use of request of acknowledgement selected in a CC when it has been proposed in a CR ?	6.5.5 t)	O	O

3.5.2.7.1.11 *Error handling*

Note.— Using class 4 over CLNS, a TPDU with an invalid checksum will be discarded.

3.5.2.7.1.11.1 Action on detection of a protocol error

Index	*Item*	*ISO/IEC 8073 references*	*ISO allowed values*	*ATN supported values*
PE4L	Class 4 over CLNS	6.22.2.3	C4L: ER, DR, Discard	C4L: ER, DR, Discard

Note.— The choice of action (DR, Discard) is an implementation choice and may depend on the type of error encountered.

3.5.2.7.1.11.2 Actions on receipt of an invalid or undefined parameter in a CR TPDU

Index	*Event*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
RR1	A parameter not defined in ISO/IEC 8073 shall be ignored	13.2.3	M	M
RR2	An invalid value in the alternative protocol class parameter shall be treated as a protocol error	13.2.3	M	M

Index	*Event*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
RR3	An invalid value in the class and option parameter shall be treated as a protocol error	13.2.3	M	M
RR4	On receipt of the additional option selection parameter bits 8 to 7, and bits 6 to 1 if not meaningful for the proposed class, shall be ignored	13.3.4 g)	M	M
RR6	On receipt of the class option parameter bits 4 to 1 if not meaningful for the proposed class shall be ignored	13.3.3	M	M
RR7	What action is supported on receipt of a parameter defined in ISO 8073 (other than those covered above) and having an invalid value?	13.2.3	Ignore, Protocol error	Ignore, Protocol error

Note.— The choice of action (Ignore, Protocol error) is an implementation choice and may depend on the type of error encountered.

3.5.2.7.1.11.3 Actions on receipt of an invalid or undefined parameter in a TPDU other than a CR TPDU

Index	*Event*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
U11	A parameter not defined in ISO/IEC 8073 shall be treated as a protocol error	13.2.3	M	M
U12	A parameter which has an invalid value as defined in ISO/IEC 8073 shall be treated as a protocol error	13.2.3	M	M
U13 (class 4 only)	A TPDU received with a checksum which does not satisfy the defined formula shall be discarded	6.17.3	M	M

3.5.2.7.1.12 *Class 4 timers and protocol parameters*

Index	*Event*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
TA1	T1 (Local retransmission)	12.2.1.1.4	M	M
TA2	N (Maximum transmission)	12.2.1	M	M
TA3	IL (Local inactivity time)	12.2.1.1.7	M	M
TA4	W (Window update)	12.2.1	M	M

Index	*Event*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
TA5	L (Frozen reference time)	12.2.1.1.6	M	M

Index	*Event*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
ATN-TA1	R (Persistence)	12.2.1.1.5	O	O
ATN-TA2	MLR (NSDU lifetime)	12.2.1.1.1	O	O
ATN-TA3	MRL (NSDU lifetime)	12.2.1.1.1	O	O
ATN-TA4	ELR (Maximum transit delay)	12.2.1.1.2	O	O
ATN-TA5	ERL (Maximum transit delay)	12.2.1.1.2	O	O
ATN-TA6	AL (Acknowledgement time)	12.2.1.1.3	O	M
ATN-TA7	AR (Acknowledgement time)	12.2.1.1.3	O	M
ATN-TA8	IR (Remote inactivity time)	12.2.1.1.7	O	M

Note.— According to ISO, the following applies to an implementation under test (IUT):

Index	*Event*	*ISO/IEC 8073 references*	*ISO status*	*ATN support*
OT9	Does IUT support optional timer TS2 when operating in class 4?	6.22.2.3	O	O

3.5.2.7.1.13 *Extended 32-bit checksum*

Index	*Event*	*ATN reference*	*ATN support*
ETC1	Extended 32-bit checksum in CR TPDU	§3.5.4.2	ATN6:M
ETC2	Extended 32-bit checksum in CC TPDU	§3.5.4.3.2	ETC1:M
ETC3	ISO/IEC 8073 checksum parameter in CC TPDU	§3.5.4.3.2 b)	ETC1:X
ETC4	Confirm the use of a checksum mechanism in CC TPDU	§3.5.4.3.2 c)	ETC1:M
ETC5	Extended 32-bit checksum in all subsequent TPDUs	§3.5.4.3.4	(ETC1 and ETC2):M
ETC6	Encoding of extended 32-bit checksum	§3.5.2.4.3.1	ATN6:M
ETC7	Computation of extended 32-bit checksum	§3.5.4.5	ATN6:M
ETC8	Validation of extended 32-bit checksum	§3.5.4.6	ATN6:M

3.5.2.8 Dynamic local retransmission time adaptation

3.5.2.8.1 General

Note 1.— A critical element of any COTP implementation is the determination of an appropriate retransmission timeout interval. The retransmission timeout interval has important and conflicting effects on individual user throughput and overall network efficiency. To achieve optimal throughput, a short retransmission timeout interval may be used. However, if the timeout interval is too short, then TPDUs may be retransmitted unnecessarily, with the consequence of wasting network bandwidth and decreasing the useful throughput.

Note 2.— In the ATN internetwork, the round-trip time (RTT), i.e. the time interval between sending a packet and receiving an acknowledgement for it, is expected to change over time, as routes and network traffic load might change. For this reason the ATN COTP timeout and retransmission strategy relies on the dynamic measurement of the round-trip time. The ATN COTP is expected to re-estimate the RTT and compute a new timeout interval every time a new packet is acknowledged.

3.5.2.8.2 Round-trip time estimation

Note 1.— The round-trip time is the interval of time between the sending of a TPDU and the receipt of its acknowledgement. It implicitly measures both the internetwork transit delay, including time spent in intermediate systems, and any time spent at the receiver and sender processing the PDU and acknowledgement.

Note 2.— The round-trip time can be determined by the sending transport entity, by retaining the time of transmission of each CR, CC, and DT TPDU. When the associated acknowledgement is received, the difference between the current time and the time when the acknowledged packet has been sent provides one sample of the experienced round-trip time.

3.5.2.8.2.1 A transport entity shall measure the round-trip time elapsed between every first transmission of a CR, CC or DT TPDU and the receipt of the first corresponding acknowledgement.

Note.— Acknowledgement of a CR TPDU corresponds to the receipt of a CC TPDU. Acknowledgement of a CC TPDU corresponds to the receipt of an AK, DT, ED or EA TPDU. Acknowledgement of a DT TPDU corresponds to the receipt of an AK TPDU.

3.5.2.8.2.2 When a TPDU is received that acknowledges for the first time one or more TPDUs, then the round-trip time shall be measured by computing the difference between the time of transmission of the most recently sent TPDU among those being acknowledged and the time of reception of the acknowledgement.

3.5.2.8.2.3 If none of the TPDUs being acknowledged were retransmitted prior to the receipt of the acknowledgement, then the measured round-trip time shall be considered by the transport entity as a valid round-trip time sample.

3.5.2.8.2.4 If one or more retransmissions of one or more TPDUs being acknowledged occurred before the receipt of the acknowledgement, then the measured round-trip time shall be considered by the transport entity as an invalid round-trip time sample.

3.5.2.8.3 Retransmission time calculation

3.5.2.8.3.1 Every time a new valid round-trip time sample is obtained on a transport connection, the transport entity shall compute a new suitable value for the local retransmission time (T1).

3.5.2.8.3.2 The initial value of the local retransmission time ($T1_{init}$) should be computed as a function of an initial round trip time estimate ($SRTT_{init}$) and of its mean deviation (D_{init}), as follows:

$$SRTT_{init} = S_0$$

$$D_{init} = SRTT_{init}/4$$

$$T1_{init} = SRTT_{init} + 4 * D_{init} + A_R$$

where:

a) S_0 is the first valid round-trip time sample; and

b) A_R is the remote acknowledgement time value.

3.5.2.8.3.3 Any further value of the local retransmission time (T1) should be computed as a function of a “smoothed” round-trip time estimate (SRTT) and of its “smoothed” mean deviation D, as follows:

$$Err = S - SRTT_{prev}$$

$$SRTT_{new} = SRTT_{prev} + g * Err$$

$$D_{new} = D_{prev} + h * (ABS(Err) - D_{prev})$$

$$T1 = SRTT_{new} + 4 * D_{new} + A_R$$

where:

a) $SRTT_{prev}$ and $SRTT_{new}$ are the previous and new computed values of the “smoothed” round-trip time estimate. Initially, $SRTT_{prev}$ is set to $SRTT_{init}$.

b) D_{prev} and D_{new} are the previous and new computed values of the “smoothed” mean deviation. Initially, D_{prev} is set to D_{init}.

c) Err is the difference between the measured value just obtained (S) and the previous $SRTT_{prev}$.

d) The gains g and h are constants that control how rapidly the smoothed round-trip time and its smoothed mean deviation adapt to change. g is set to 1/8. h is set to 1/4.

e) ABS(Err) is the absolute value of Err.

f) T1 is the local retransmission time value.

g) A_R is the remote acknowledgement time value.

Note 1.— This algorithm is derived from the Jacobson’s algorithm and differs only by the addition of the remote acknowledgement time (A_R) in the formula used for the computation of the local retransmission time value. This change is in response to the unique requirements of the aeronautical environment which may require long acknowledgement times.

Note 2.— The SRTT, D and T1 variables are maintained on a per transport connection basis.

3.5.2.8.3.4 If an alternative algorithm for the computation of the local retransmission time (T1) is implemented over air-ground connections, then its performance shall be at least equivalent to the performance of the algorithm recommended above.

3.5.2.8.4 Retransmission time back-off procedure

3.5.2.8.4.1 Whenever a retransmission timeout occurs, the transport entity shall double the local retransmission time value before retransmitting the unacknowledged data.

Note.— This procedure is known as exponential back-off. Back-off is performed independently of the round-trip time estimation, since without an acknowledgement there is no new timing information to be fed into the Retransmission Time value calculation.

3.5.2.8.4.2 If as a result of this procedure the local retransmission time exceeds its maximum value (see ⁋3.5.2.8.5), then the local retransmission time shall be set to its maximum value.

3.5.2.8.4.3 Whenever an invalid round-trip time sample is obtained, the retransmission time value shall remain set to the value having resulted from the operation of the previous backoff procedure.

Note.— This rule is derived from a procedure known as the Karn's algorithm.

3.5.2.8.5 Initial, minimum and maximum local retransmission time value

3.5.2.8.5.1 The transport entity shall maintain the value of the local retransmission time within a bounded range.

3.5.2.8.5.2 The lower and upper bound of the local retransmission time shall be configurable.

3.5.2.8.5.3 When intended for operation over air-ground subnetworks, the lower and upper bound of the local retransmission time shall be set to the minimum and maximum T1 values, respectively, specified in Table ⁋3-7.

3.5.2.8.5.4 When intended for operation over air-ground subnetworks, the initial value of the local retransmission time shall be set to the nominal T1 value specified in Table ⁋3-7.

3.5.2.8.5.5 When intended for operation exclusively over ground-ground subnetworks, the initial value of the local retransmission time shall be greater than the maximum expected round-trip time.

3.5.3 Connectionless mode transport protocol operation

The connectionless transport service (CLTS) and connectionless transport protocol (CLTP) allow the exchange of unconfirmed datagrams between communicating transport service users. The connectionless transport service is not used by any of the current CNS/ATM applications specified in Doc 9880, Parts I and II, therefore this section is merely a placeholder for a possible future development.

3.5.4 Extended 32-bit checksum

3.5.4.1 General

3.5.4.1.1 When present in a TPDU, the extended 32-bit checksum parameter shall be validated using the algorithm specified in ⁋3.5.4.6.

3.5.4.1.2 If the validation fails, the TPDU shall be discarded without further processing.

3.5.4.2 Negotiating the use of extended 32-bit checksum in transport connections

3.5.4.2.1 When extended 32-bit checksums are supported and a low residual error rate is requested, the CR TPDU shall contain both an extended 32-bit checksum parameter computed as specified in §3.5.4.5 and the ISO/IEC 8073 checksum parameter. The option for the "non-use of checksum" shall not be proposed in the "additional option selection" parameter of the CR TPDU.

Note.— Including the extended 32-bit checksum parameter in a CR TPDU implies that use of extended 32-bit checksum is proposed.

3.5.4.2.2 The extended 32-bit checksum parameter value shall be calculated first and the resulting check digits inserted into the TPDU before the ISO/IEC 8073 checksum is calculated.

3.5.4.2.3 The value of the ISO/IEC 8073 checksum parameter shall be set to zero before the extended 32-bit checksum is computed.

3.5.4.2.4 When a medium residual error rate is requested, the CR TPDU shall contain the ISO/IEC 8073 checksum parameter; the extended 32-bit checksum parameter shall not be present. The option for the "non-use of checksum" shall not be proposed in the "additional option selection" parameter of the CR TPDU.

3.5.4.2.5 When a high residual error rate is requested, the extended 32-bit checksum parameter shall not be present. The option for the "non-use of checksum" shall be proposed in the "additional option selection" parameter of the CR TPDU.

3.5.4.3 Accepting the use of checksums

3.5.4.3.1 A CR TPDU that does not contain an extended 32-bit checksum parameter shall be processed in compliance with ISO/IEC 8073.

3.5.4.3.2 When a CR TPDU is received that includes the extended 32-bit checksum parameter, then the connection responder shall validate the received checksum as specified in §3.5.4.6 and, in order to signal acceptance of extended 32-bit checksum:

a) compute and include an extended 32-bit checksum parameter, as specified in §3.5.4.5, in the responding CC TPDU;

b) omit the ISO/IEC 8073 checksum parameter from the responding CC TPDU;

c) confirm the use of a checksum mechanism by setting the option bit for the "non-use of checksum" to zero in the "additional option selection" parameter of the responding CC TPDU.

Note.— This specification extends the semantic of the ISO/IEC 8073 option for the "Non-use of checksum" to mean "Non-use of any checksum mechanism". Setting this option to "No" means that the use of one of the checksum mechanisms is proposed or accepted respectively. Which checksum mechanism is proposed or accepted is determined by the presence or absence of the extended 32-bit checksum parameter within the CR or CC TPDU, respectively.

3.5.4.3.3 The ISO/IEC 8073 checksum shall be verified as correct before the extended 32-bit checksum is verified.

3.5.4.3.4 Once the use of extended 32-bit checksums is accepted, all other TPDUs exchanged on the same transport connection, in either direction, shall also include the extended 32-bit checksum parameter computed as specified in 3.5.4.5, and shall not include the ISO/IEC 8073 checksum parameter. Any TPDU received without the extended 32-bit checksum parameter or which includes an ISO/IEC 8073 checksum parameter shall be discarded.

3.5.4.3.5 If a TPDU other than a CR TPDU includes both an extended 32-bit checksum parameter and an ISO/IEC 8073 checksum parameter it shall be considered as a protocol error.

3.5.4.3.6 When the use of the extended 32-bit checksum is not acceptable, then the extended 32-bit checksum parameter shall not be included in the CC TPDU. Use of the ISO/IEC 8073 16-bit checksum shall be accepted if proposed.

Note 1.— There is no difference between rejecting the use of the extended 32-bit checksum and the response of an implementation that does not support extended 32-bit checksums.

Note 2.— It is generally expected that if the extended 32-bit checksum is proposed, then its use is necessary and it will be accepted. Rejection is very much an exceptional situation.

3.5.4.3.7 The extended 32-bit checksum parameter shall not be included in any subsequent TPDUs exchanged on the same transport connection if an extended 32-bit checksum parameter is not present in the CC TPDU.

3.5.4.4 Use in connectionless mode

3.5.4.4.1 When supported and when a low residual error rate is requested by the service user, the extended 32-bit checksum shall be computed as specified in 3.5.4.5 and included in the UD TPDU header as the value of the extended 32-bit checksum parameter. The ISO/IEC 8602 checksum parameter shall not be present.

Note.— The sender needs to know a priori that the intended recipient supports the extended 32-bit checksum; otherwise the UD TPDU will be discarded on receipt due to it containing an unrecognized parameter.

3.5.4.4.2 When a medium residual error rate is requested by the service user, then the ISO/IEC 8602 checksum shall be computed and included in the UD TPDU header.

3.5.4.4.3 When a high residual error rate is requested by the service user, then neither the extended 32-bit checksum parameter nor the ISO/IEC 8602 checksum parameter shall be present.

3.5.4.5 Extended 32-bit checksum computation

Note 1.— The style of Appendix B of ISO/IEC 8073 is followed in the definition of the extended 32-bit checksum algorithm.

Note 2.— This algorithm has been derived from: Fletcher, J. G., "An Arithmetic Checksum for Serial Transmissions", IEEE Transactions on Communications, Vol. COM-30, No. 1, January 1982, pp. 247-252.

3.5.4.5.1 Symbols

Note.— The following symbols are used:

a) C0, C1, C2, C3 are variables used by the algorithm;

b) i is the number (i.e. position) of an octet within the TPDU;

c) n is the number (i.e. position) of the first octet of the extended 32-bit checksum parameter;

d) L is the length of the complete TPDU including the "pseudo trailer"; and

e) Xj is the value of the jth octet of the extended 32-bit checksum parameter (in transmission order).

3.5.4.5.2 Arithmetic conventions

Addition shall be performed in one of the two following modes:

a) modulo 255; or

b) ones complement arithmetic in which if any of the variables has the value minus zero (i.e. 0xFFFF) it shall be regarded as though it were plus zero (i.e. 0).

3.5.4.5.3 Algorithm for generating the checksum parameter

3.5.4.5.3.1 The complete TPDU with the extended 32-bit checksum parameter value field set to zero shall be set up.

3.5.4.5.3.2 A "pseudo trailer" created from:

a) the length of the destination NSAP Address;

b) the destination NSAP Address;

c) the length of the source NSAP Address; and

d) the source NSAP Address;

and encoded identically to their encoding in the CLNP header, shall be appended to the TPDU.

Note 1.— This pseudo trailer is not part of the TPDU and is never transmitted to the destination end system.

Note 2.— A pseudo trailer rather than a pseudo header is used because the check digits have to be moved to the end of the TPDU by the receiver and hence a trailer will have to be constructed anyway.

3.5.4.5.3.3 The extended 32-bit checksum shall be created by the following algorithm:

1) initialize C0 , C1, C2 and C3 to zero;

2) process each octet in the combined TPDU and pseudo trailer sequentially from i = 1 to L by:

a) adding the value of the octet to C0; then

b) adding the value of C0 to C1, C1 to C2, and C2 to C3;

3) set the octets of the extended 32-bit checksum parameter as follows:

   a) X0 = - (C0 + C1 + C2 + C3);

   b) X1 = C1 + 2 * C2 + 3 * C3;

   c) X2 = - (C2 + 3 * C3); and

   d) X3 = C3;

4) discard the pseudo trailer octets.

3.5.4.6 Algorithm for checking the checksum parameter

3.5.4.6.1 The transport entity shall append to the received TPDU a “pseudo trailer” which is created from the source and destination NSAP addresses associated with the incoming TPDU and the value of the received extended 32-bit checksum parameter in the following order:

a) the length of the destination NSAP address;

b) the destination NSAP address;

c) the length of the source NSAP address;

d) the source NSAP address;

encoded identically to their encoding in the CLNP header

e) the octets of the extended 32-bit checksum parameter in the same order in which they appear in the checksum parameter.

3.5.4.6.2 The value of the extended 32-bit checksum parameter shall be set to zero.

3.5.4.6.3 If the received TPDU is a CR TPDU, then the value of the 16-bit checksum parameter shall be set to zero.

3.5.4.6.4 The extended 32-bit checksum shall be validated as follows:

1) initialize C0, C1, C2 and C3 to zero;

2) process each octet in the combined TPDU and pseudo trailer sequentially from i = 1 to L by:

   a) adding the value of the octet to C0; then

   b) adding the value of C0 to C1, C1 to C2, and C2 to C3;

3) discard the pseudo trailer;

4) if, when all the octets have been processed, one or more of the variables C0, C1, C2 or C3 do not have the value zero, then the checksum validation has failed.

3.6 INTERNETWORK SERVICE AND PROTOCOL SPECIFICATION

3.6.1 Introduction

Note 1.— The ATN Internet comprises a number of interconnected ATN routers and constituent subnetworks supporting data communication among host computers operating the ATN Internet protocols.

Note 2.— All ATN NPDUs (network protocol data units) are encapsulated within appropriate subnetwork protocol data units for transfer among ATN network entities using the connectionless ISO OSI network layer service provided by the ATN Internet. As the ATN Internet protocol is connectionless, any information required to process a particular NPDU is carried within the header of that network protocol data unit for processing by ATN routers and host computers.

3.6.1.1 Scope

Note 1.— This chapter provides requirements and recommendations pertaining to the use of the ISO/IEC 8473 by ATN end system and intermediate system network entities. This chapter is concerned with the use of ISO/IEC 8473 in the context of the internetworking protocol approach to the provision of CLNS as defined in ISO/IEC 8348. This chapter contains ATN-specific protocol implementations and is concerned with the interoperability of protocol implementations. It therefore provides appropriate compliance statements and APRLs for this purpose.

Note 2.— The ATN network layer connectionless-mode network service supports the transfer of a connectionless network service data unit (NSDU) from a source NSAP to a destination NSAP within the ATN network. Each such NSDU transfer is the result of a single invocation of the connectionless-mode network service encompassed within the ATN.

3.6.1.2 Applicability of requirements

All ATN intermediate system and end system network entities shall comply with the provisions contained in 3.6.2 and 3.6.3, in addition to all APRLs specified in 3.6.4.

3.6.2 ATN specific features

3.6.2.1 Purpose of ATN specific features

Note 1.— The ATN infrastructure, referred to as an Internet, comprises the interconnection of computers with gateways and routers via real subnetworks. This internetworking infrastructure allows for the incorporation of differing air-ground and ground-ground subnetworks servicing differing user groups, i.e. air traffic services (ATS), aeronautical operational control services (AOC) and others.

Note 2.— The CLNP (connectionless network protocol) protocol used to operate this internetworking infrastructure is based on ISO/IEC 8473 with ATN-specific additions to reflect the unique communications environment of the ATN.

Note 3.— The ATN specific functions listed in this chapter reflect responses to the additional functional needs of ATN network entities in order to support user requirements concerned with:

a) ensuring that information is conveyed about traffic type and routing policy requirements pertaining to user data in NPDUs;

b) ensuring that a priority scheme can be applied for management of end systems and intermediate systems output queues and buffers;

c) ensuring that specific policies and procedures are available to handle congestion avoidance and congestion control requirements within the ATN.

3.6.2.2 The security function

3.6.2.2.1 General

3.6.2.2.1.1 The SECURITY function of ISO/IEC 8473, as defined in this specification, shall be supported by ATN end system or intermediate system network entities receiving or transmitting inter-domain traffic other than traffic type as general communications.

3.6.2.2.1.2 ATN network entities shall therefore provide the globally unique security format for all created NPDUs.

3.6.2.2.1.3 The sole exception to this requirement is for general communications traffic where no security parameter information is required to be encoded in created NPDUs.

3.6.2.2.2 Encoding of the security parameter

3.6.2.2.2.1 The CLNP options security parameter shall be used in the ATN to convey information about the traffic type and routing policy requirements pertaining to the user data of the NPDU (other than general communications).

Note.— The CLNP options security parameter may also be used to convey a security classification.

3.6.2.2.2.2 The value component of the CLNP options security parameter (in the NPDU header) shall be encoded as follows:

a) the first octet shall always be encoded as **[1100 0000]** to indicate the globally unique security format;

b) the remaining octets shall contain the ATN security label encoded as the four fields illustrated in Figure 3-7 and defined below.

	Security Registration ID Length	Security Registration ID (variable)	Security Information Length	Security Information (optional)
Octet	0	1	n	n+1

Figure 3-7. The ATN security label

3.6.2.2.3 Security registration ID length

This field shall be one octet long and contain the length in octets of the security authority's security registration identifier.

Note.— The security registration ID identifies the authority that has specified the associated security policy.

3.6.2.2.4 Security registration ID

This field shall contain the following hexadecimal string which identifies the ATN security registration ID:

[06 04 2b 1b 00 00]

Note.— The ATN security registration ID value defined above is the encoding using ASN.1 basic encoding rules [ISO/IEC 8825-1] of the ATN security registration identifier defined as {1 3 27 0 0}. This ATN security registration identifier identifies the ATN security authority as an object in the ICAO object hierarchy. ICAO has been assigned an international code designator (ICD) decimal value [0027] in accordance with the dictates of ISO/IEC 6523. According to ISO/IEC 6523 and ISO/IEC 8824 this value identifies an arc of the identified organization of ISO. ICAO object identifiers designate an ICAO defined hierarchy starting with {1 3 27}. Under this arc, {0} has been designated as ATN, and the flat address space under ATN starts with object identifiers {0,1,2,3,4, ...}. Value {0} has been assigned as the traffic type and routing policy identifier.

3.6.2.2.5 Security information length

3.6.2.2.5.1 This field shall be one octet in length and shall define the length in octets of the security information.

3.6.2.2.5.2 If there is no security information, this field shall be set to zero.

3.6.2.2.6 Security information

3.6.2.2.6.1 *General*

3.6.2.2.6.1.1 When present, the security information field of the ATN security label shall be used to convey, as separate tag sets:

a) the traffic type and routing policy requirements, if any, applicable to the transfer of the user data through the ATN;

b) the security classification.

3.6.2.2.6.1.2 When no traffic type is identified then the general communications traffic type shall be assumed, with a routing policy requirement of “no preference”. When no security classification is specified then “unclassified” shall be assumed.

3.6.2.2.6.2 *Encoding of the security information field*

3.6.2.2.6.2.1 The security information field shall comprise zero, one or more security tag sets. A security tag with the same tag set name shall not occur more than once in the options security parameter of the CLNP NPDU.

	Tag Set Name Length	Tag Set Name	Tag Set Length	Security Tag
Octet	0	1	n	n+1

Figure 3-8. Security tag set format

3.6.2.2.6.2.2 Each security tag set shall consist of four fields, as illustrated in Figure 3-8 and shall be as defined in the following sections.

Note.— This format has been chosen to provide for an extensible type-length-value encoding method for security-related information placed in the CLNP header under rules specified by the ATN security authority.

3.6.2.2.6.3 *Security tag set name length*

The security tag set name length shall contain the length in octets of the tag set name field.

3.6.2.2.6.4 *Security tag set name*

The security tag set name shall be used to uniquely identify the tag set.

3.6.2.2.6.5 *Tag set length*

The tag set length field shall contain the length in octets of the security tag field.

3.6.2.2.6.6 *Security tag*

The security tag field shall be used to convey security-related information for which the syntax and semantics are identified by the preceding tag set name.

3.6.2.2.6.7 *Encoding of the tag set for traffic type and associated routing policies*

3.6.2.2.6.7.1 The tag set name shall be set to [0000 1111].

3.6.2.2.6.7.2 When present in the CLNP options security parameter, this tag set shall always be the first tag set to be encoded in the security information field of the ATN security label.

Note.— This tag set is used to identify the traffic type of the data, whether it is for ATC or airline communications, and, for operational communications, any routing policy requirements that apply.

3.6.2.2.6.7.3 The security tag shall indicate the routing policy requirements for the data contained in the same NPDU, according to Table 3-9.

Note.— See 3.2.7 for detailed information on the ATN security policy.

3.6.2.2.6.7.4 Those security tag values which are not defined in Table 3-9 shall be reserved for future use by this specification.

Table 3-9. Encoding of traffic type security tag

Traffic Type	*Category*	*Security Tag Value*	*Semantics*
ATN Operational Communications	Air Traffic Service Communications (ATSC)	000 00001	No Traffic Type Policy Preference.
		000 10000	Traffic preference for Class A ATSC route(s).
		000 10001	Traffic preference for Class B ATSC route(s).
		000 10010	Traffic preference for Class C ATSC route(s).
		000 10011	Traffic preference for Class D ATSC route(s).
		000 10100	Traffic preference for Class E ATSC route(s).
		000 10101	Traffic preference for Class F ATSC route(s).
		000 10110	Traffic preference for Class G ATSC route(s).
		000 10111	Traffic preference for Class H ATSC route(s).
	Aeronautical Operational Control (AOC)	001 00001	No traffic type policy preference
		001 00010	Route traffic only via gatelink
		001 00011	Route traffic only via VHF data link
		001 00100	Route traffic only via satellite data link
		001 00101	Route traffic only via HF data link
		001 00110	Route traffic only via Mode S data link
		001 00111	Route traffic using an ordered preference of gatelink first, then VHF data link
		001 01000	Route traffic using an ordered preference of gatelink first, then VHF data link, then satellite
		001 01001	Route traffic using an ordered preference of gatelink first, then VHF data link, then HF data link, then satellite data link
ATN Administrative Communications	No category defined	001 10000	No traffic type policy preference
General Communications	No category defined	N/A	*Note.— General communications traffic does not require encoding of security parameters within created NPDUs. Specification of a security tag value for such general communications is therefore not applicable.*
ATN Systems Management Communications	No category defined	011 00000	No traffic type policy preference

3.6.2.2.6.8 *Encoding of the tag set for security classification*

3.6.2.2.6.8.1 The tag set name shall be set to [0000 0011].

3.6.2.2.6.8.2 When present in the security parameter, this tag set shall always follow the tag set for traffic type and associated routing policies (see §3.6.2.2.6) if present, but otherwise shall be the first tag set to be encoded in the field.

Note.— The purpose of this field is to permit the later extension of the ATN to handle classified data.

3.6.2.2.6.8.3 The security tag shall indicate the security classification of the NPDU according to the following table:

3.6.2.2.6.8.4 Those security classification tag values which are not assigned in Table §3-10 shall be reserved for future use by this specification.

Table 3-10. Encoding of the security classification tag

Value	*Security Classification*
0000 0001	unclassified
0000 0010	restricted
0000 0011	confidential
0000 0100	secret
0000 0101	top secret
0000 0110 to 1111 1111	unassigned

3.6.2.3 Management of network priority

Note.— Network priority handling provisions are specified in §3.2.8.

3.6.2.4 Congestion management

Note 1.— The congestion management provisions in the network layer are intended to guarantee the notification to the transport layer of potential risks of congestion via the CE bit conveyed in the QoS maintenance parameter of an ISO/IEC 8473 NPDU. §3.5.2.5 defines the measures that the transport layer implements upon receipt of NPDUs with the CE bit set.

Note 2.— The above requirement is applicable to all types of ISO/IEC 8473 NPDUs.

3.6.2.4.1 Setting of the congestion experienced flag

3.6.2.4.1.1 The congestion experienced flag (CE-flag) in the QoS maintenance parameter in the options part of an NPDU header shall initially be set to zero by the originator of the NPDU.

3.6.2.4.1.2 When an NPDU is being forwarded by an ATN intermediate system, the intermediate system shall examine the depth of the output queue selected for that NPDU.

3.6.2.4.1.3 If the depth of the selected output queue exceeds a threshold α (see Table 3-11), the ATN intermediate system shall set the CE-flag in the NPDU header.

Note.— The above assumes a single output queue per network (CLNP) priority. If mixed priority queues are implemented, which is valid provided that priority order is always maintained, then the CE-flag is set only when the number of NPDUs on the queue of the same or a higher priority exceeds alpha.

3.6.2.4.1.4 Once the CE-flag is set, it shall not be reset by any ATN intermediate system traversed by the NPDU further along to the path towards the destination.

3.6.2.4.2 Forwarding congestion information to the receiving NS-user

3.6.2.4.2.1 For each sequence of NPDUs that together form an NSDU, the destination network entity shall keep two counters:

a) the first one, n-total, shall reflect the length of that sequence;

b) the second one, n-CE, shall reflect the number of those NPDUs of this sequence that had the CE-flag set on reception by the destination network entity.

Note.— Each NSDU is forwarded through the network as a sequence consisting of one or more NPDUs.

3.6.2.4.2.2 When the destination network entity passes an NSDU to the receiving NS-user, it shall convey the associated counters n-total and n-CE to the NS-user.

Note.— The conveyance of the congestion information associated with an NSDU to the NS-user is a local matter.

3.6.2.4.3 Required algorithm values

The value settings defined in Table 3-11 shall be implemented:

Table 3-11. Required values for α

Name	*Description*	*Required range*
α	Output queue threshold	1 packet

3.6.3 ATN specific requirements for ISO/IEC 8473

Note.— This section defines ATN specific requirements on the ISO/IEC 8473 protocol.

3.6.3.1 Segmentation function

3.6.3.1.1 ATN intermediate systems (ISs) shall support both the segmenting and the non-segmenting subsets of ISO/IEC 8473.

3.6.3.1.2 ATN end systems shall support the ISO/IEC 8473 segmenting subset.

Note.— Use of the non-segmenting subset of ISO/IEC 8473 for NPDUs whose packet size exceeds the maximum SNSDU size supported by an underlying subnetwork will result in the packet being discarded. Use of the non-segmenting ISO/IEC 8473 subset is most appropriate for situations where the SNSDU size of the subnetwork(s) used for NPDU transfer is well understood.

3.6.3.2 Security function

Note.— The ATN specific use of the ISO/IEC 8473 security function is specified in 3.6.2.2.

3.6.3.3 Echo request function

ATN end system and intermediate system network entities (NEs) should support the ECHO REQUEST function as invoked by network layer management.

Note.— The echo request function is invoked to obtain information on the reachability of specific network entities and the path characteristics between NEs through the operation of network layer routing functions.

3.6.3.4 Echo response function

3.6.3.4.1 ATN end systems and intermediate systems shall support the echo response function of ISO/IEC 8473.

Note.— The echo response function is performed by a network entity when it has received an echo request (ERQ) PDU that has reached its destination. When invoked, the echo response function causes an echo response (ERP) PDU to be created.

3.6.3.4.2 If the data part of the received ERQ PDU contains an ERP PDU header, then the options part of the ERP PDU to be sent shall be identical to (copied from) the options part of the ERP PDU header contained in the data part of the received ERQ PDU.

3.6.3.4.3 If the data part of the received ERQ PDU does not contain an ERP PDU header, then the security, priority, and QoS maintenance options of the ERP PDU shall be identical to the corresponding options in the header of the ERQ PDU, if present.

3.6.3.4.4 If the data part of the received ERQ PDU does not contain an ERP PDU header, and if the security option (respectively, the priority or QoS maintenance option) is not present in the received ERQ PDU header, then the security option (respectively, the priority or QoS maintenance option) shall not be included in the ERP PDU.

3.6.3.4.5 If the data part of the received ERQ PDU does not contain an ERP PDU header, and if the partial recording of route option is present in the received ERQ PDU header, then the partial recording of route option shall be specified in the ERP PDU, with the second octet of the parameter value field set to the value 3.

3.6.3.5 Network priority

Note.— The ATN specific use of the ISO/IEC 8473 priority is specified in 3.2.8.4.

3.6.4 APRLs

3.6.4.1 General

An implementation of the ISO/IEC 8473 protocol shall be used in an ATN system if and only if its PICS is in compliance with the APRL provided in this part of Doc 9880.

Note.— The CLNP requirements list is a statement of which capabilities and options of the protocol at minimum are required to be implemented for the ATN environment. The requirements list may be used by the protocol implementor as a checklist to conform to this standard; by the supplier and procurer to provide a detailed indication of the capabilities of an implementation; by the user to check the possibility of interworking between two different implementations; and by the protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance to the protocol.

3.6.4.2 Support of ATN-specific network layer features

Index	*Item*	*ATN reference*	*ATN support*
ATN CLNP1	Encoding and use of the security parameter	⁋3.6.2.2	M
ATN CLNP2	Management of network priority	⁋3.6.2.3, ⁋3.2.8.4	M
ATN CLNP4	Echo request function	⁋3.6.3.3	O
ATN CLNP5	Congestion management	⁋3.6.2.4	M
ATN CLNP6	Echo response function	⁋3.6.3.4.1	M
ATN CLNP7	Echo response parameter setting	⁋3.6.3.4.2, ⁋3.6.3.4.3, ⁋ 3.6.3.4.4	M

3.6.4.3 Major capabilities

Item	*Capability*	*ISO/IEC 8473 reference*	*Status*	*ATN support*
ES	End system		O.1	O.1
IS	Intermediate system		O.1	O.1
FL-r	<r> Full protocol	8473-1: 6	M	M
FL-s	<s> Full protocol	8473-1: 6	M	M
NSS-r	<r> Non-segmenting subset	8473-1: 5.2	M	M
NSS-s	<s> Non segmenting subset	8473-1: 5.2	IS:M ^IS:O	IS:M ^IS:O
IAS-r	<r> Inactive subset	8473-1: 5.2	ES:O	ES:O

Item	*Capability*	*ISO/IEC 8473 reference*	*Status*	*ATN support*
IAS-s	<s> Inactive subset	8473-1: 5.2	1 IAS-r:M 2 ^IAS-r:X	3 IAS-r:M 4 ^IAS-r:X
S802	SNDCF for ISO/IEC 8802	8473-2: 5.4	O.2	O
SCLL	SNDCF for CL link service	8473-4: 5.3.1	O.2	O
SCOL	SNDCF for CO link service	8473-4: 5.3.2	O.2	O
SX25	SNDCF for ISO/IEC 8208	8473-3: 5.4	O.2	O
ATN SNDCF	SNDCF for mobile subnetworks	ATN Ref: §3.7	N/A	5 ISMOB:M 6 ISGRD:O 7 ^IS:O

ISMOB: If ISO/IEC 8473 is used over mobile subnetworks, then ISMOB is true, else ISMOB is false.

ISGRD: If ISO/IEC 8473 is used over ground subnetworks, then ISGRD is true, else ISGRD is false.

O.1: The supported functions, NPDUs, associated parameters and timers required for end systems are provided in APRLs §3.6.4.4 through §3.6.4.11. The supported functions, NPDUs, associated parameters and timers required for intermediate systems are provided in APRLs §3.6.4.12 through §3.6.4.18.

O.2: APRLs for the SNDCF for use with ISO/IEC 8802-2 subnetworks are provided in §3.7.5.2 and §3.7.5.3. APRLs for the SNDCF for use with ISO/IEC 8208 subnetworks are provided in §3.7.5.4 through §3.7.5.7.

3.6.4.4 End systems – Supported functions

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
ePDUC	PDU composition	6.1	M	M
ePDUD	PDU decomposition	6.2	M	M
eHFA	Header format analysis	6.3	M	M
ePDUL-s	<s> PDU lifetime control	6.4	M	M
ePDUL-r	<r> PDU lifetime control	6.4	O	M
eRout	Route PDU	6.5	M	M
eForw	Forward PDU	6.6	M	M
eSegm	Segment PDU	6.7	M	M
eReas	Reassemble PDU	6.8	M	M
eDisc	Discard PDU	6.9	M	M

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
eErep	Error reporting	6.10	M	M
eEdec-s	<s> Header error detection	6.11	M	M
eEdec-r	<r> Header error detection	6.11	M	M
eSecu-s	<s> Security	6.13, ATN Ref: §3.6.2.2	O	M
eSecu-r	<r> Security	6.13, ATN Ref. §3.6.2.2	O	M
eCRR-s	<s> Complete route recording	6.15	O	OX
eCRR-r	<r> Complete route recording	6.15	O	O
ePRR-s	<s> Partial route recording	6.15	O	M
ePRR-r	<r> Partial route recording	6.15	O	M
eCSR	Complete source routing	6.14	O	OX
ePSR	Partial source routing	6.14	O	OX
ePri-s	<s> Priority	6.17, ATN Ref. §3.6.3.5	O	M
ePri-r	<r> Priority	6.17, ATN Ref. §3.6.3.5	O	M
eQOSM-s	<s> QOS maintenance	6.16	O	M
eQOSM-r	<r> QOS maintenance	6.16	O	M
eCong-s	<s> Congestion notification	6.18	eQOSM-s: M	eQOSM-s:M
eCong-r	<r> Congestion notification	6.18	O	M
ePadd-s	<s> Padding	6.12	O	OX
ePadd-r	<r> Padding	6.12	M	M
eEreq	Echo request	6.19, ATN Ref. §3.6.3.3	O	O
eErsp	Echo response	6.20, ATN Ref. §3.6.3.4	O	M
eSegS	Create segments smaller than necessary	6.8	O	O

Note.— The classification “OX” indicates optional to implement, precluded to use.

3.6.4.5 End systems – Supported NPDUs

Item	*NPDU*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
eDT-t	DT (full protocol) transmit	7.7	M	M
eDT-r	DT (full protocol) receive	7.7	M	M
eDTNS-t	DT (non-segment) transmit	7.7	NSS-s:M	NSS-s:M
eDTNS-r	DT (non-segment) receive	7.7	M	M
eER-t	ER transmit	7.9	M	M
eER-r	ER receive	7.9	M	M
eIN-t	Inactive PDU transmit	7.8	IAS-s:M	IAS-s:M
eIN-r	Inactive PDU receive	7.8	IAS-r:M	IAS-r:M
eERQ-t	ERQ transmit	7.10	eEreq:M	eEreq:M
eERQ-r	ERQ receive	7.10	M	M
eERP-t	ERP transmit	7.11	eErsp:M	eErsp:M
eERP-r	ERP receive	7.11	M	M

3.6.4.6 End systems – Supported DT parameters

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
edFxPt-s	<s> Fixed part	7.2	M	M
edFxPt-r	<r> Fixed part	7.2	M	M
edAddr-s	<s> Address	7.3	M	M
edAddr-r	<r> Address	7.3	M	M
edSeg-s	<s> Segmentation part	7.4	M	M
edSeg-r	<r> Segmentation part	7.4	M	M
edPadd-s	<s> Padding	7.5.2	ePadd-s:M	—
edPadd-r	<r> Padding	7.5.2	M	M
edSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
edSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
edCRR-s	<s> Complete route recording	7.5.5	eCRR-s:M	—
edCRR-r	<r> Complete route recording	7.5.5	eCRR-r:M	eCRR-r:M
edPRR-s	<s> Partial route recording	7.5.5	ePRR-s:M	M
edPRR-r	<r> Partial route recording	7.5.5	ePRR-r:M	M
edCSR-s	<s> Complete source routing	7.5.4	eCSR:M	—
edPSR-s	<s> Partial source routing	7.5.4	ePSR:M	—
edQOSM-s	<s> QOS maintenance	7.5.6	eQOSM-s or eCong-s:M	eQOSM-s:M
edQOSM-r	<r> QOS maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM-r or eCong-r:M
edPri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
edPri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
edData-s	<s> Data	7.6	M	M
edData-r	<r> Data	7.6	M	M
edUnSup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded and where appropriate an error report PDU generated?	6.21	M	M
edUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

3.6.4.7 End systems – Supported ER parameters

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
eeFxPt-s	<s> Fixed part	7.2	M	M
eeFxPt-r	<r> Fixed part	7.2	M	M

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
eeAddr-s	<s> Address	7.3	M	M
eeAddr-r	<r> Address	7.3	M	M
eePadd-s	<s> Padding	7.5.2	ePadd-s:M	—
eePadd-r	<r> Padding	7.5.2	M	M
eeSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
eeSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
eeCRR-s	<s> Complete route recording	7.5.5	eCRR-s:M	—
eeCRR-r	<r> Complete route recording	7.5.5	eCRR-r:M	eCRR-r:M
eePRR-s	<s> Partial route recording	7.5.5	ePRR-s:M	M
eePRR-r	<r> Partial route recording	7.5.5	ePRR-r:M	M
eeCSR-s	<s> Complete source routing	7.5.4	eCSR:M	—
eePSR-s	<s> Partial source routing	7.5.4	ePSR:M	—
eeQOSM-s	<s> QOS maintenance	7.5.6	eQOSM-s or eCong-s:M	eQOSM-s or eCong-s:M
eeQOSM-r	<r> QOS maintenance	7.5.6	eQOSM-r or eCong-r:M	eQOSM-r or eCong-r:M
eePri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
eePri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
eeDisc-s	<s> Reason for discard	7.9.5	M	M
eeDisc-r	<r> Reason for discard	7.9.5	M	M
eeData-s	<s> Data	7.9.6	M	M
eeData-r	<r> Data	7.9.6	M	M
eeUnSup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded and where appropriate an error report PDU generated?	6.21	M	M
eeUnSup3	Are parameters selecting unsupported Type 3 functions ignored?	6.21	M	M

3.6.4.8 End systems – Inactive DT parameters

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
eiNLPI-s	<s> Inactive network layer protocol identifier	7.8.2	IAS-s:M	IAS-s:M
eiNLPI-r	<r> Inactive network layer protocol Identifier	7.8.2	IAS-r:M	IAS-r:M
eiData-s	<s> Data	7.8.3	IAS-s:M	IAS-s:M
eiData-r	<r> Data	7.8.3	IAS-r:M	IAS-r:M

3.6.4.9 End systems – Supported ERQ parameters

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
eqFxPt-s	<s> Fixed part	7.2	M	M
eqFxPt-r	<r> Fixed part	7.2	M	M
eqAddr-s	<s> Address	7.3	M	M
eqAddr-r	<r> Address	7.3	M	M
eqSeg-s	<s> Segmentation part	7.4	M	M
eqSeg-r	<r> Segmentation part	7.4	M	M
eqPadd-s	<s> Padding	7.5.2	ePadd-s:M	—
eqPadd-r	<r> Padding	7.5.2	M	M
eqSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
eqSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
eqCRR-s	<s> Complete route recording	7.5.5	eCRR-s:M	—
eqCRR-r	<r> Complete route recording	7.5.5	eCRR-r:M	eCRR-r:M
eqPRR-s	<s> Partial route recording	7.5.5	ePRR-s:M	M
eqPRR-r	<r> Partial route recording	7.5.5	ePRR-r:M	M
eqCSR-s	<s> Complete source routing	7.5.4	eCSR:M	—
eqPSR-s	<s> Partial source routing	7.5.4	ePSR:M	—
eqQOSM-s	<s> QOS maintenance	7.5.6	eQOSM-s or eCong-s:M	eQOSM-s:M

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN support
eqQOSM-r	<r> QOS maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM-r or eCong-r:M
eqPri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
eqPri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
eqData-s	<s> Data	7.6	M	M
eqData-r	<r> Data	7.6	M	M
eqUnSup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded and where appropriate an error report PDU generated?	6.21	M	M
eqUnSup3	Are parameters selecting unsupported Type 3 functions ignored?	6.21	M	M

3.6.4.10 End systems – Supported ERP parameters

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN support
epFxPt-s	<s> Fixed part	7.2	M	M
epFxPt-r	<r> Fixed part	7.2	M	M
epAddr-s	<s> Address	7.3	M	M
epAddr-r	<r> Address	7.3	M	M
epSeg-s	<s> Segmentation part	7.4	M	M
epSeg-r	<r> Segmentation part	7.4	M	M
epPadd-s	<s> Padding	7.5.2	ePadd-s:M	—
epPadd-r	<r> Padding	7.5.2	M	M
epSecu-s	<s> Security	7.5.3, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	eSecu-s:M	eSecu-s:M
epSecu-r	<r> Security	7.5.3, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	eSecu-r:M	eSecu-r:M

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
epCRR-s	<s> Complete route recording	7.5.5	eCRR-s:M	—
epCRR-r	<r> Complete route recording	7.5.5	eCRR-r:M	eCRR-r:M
epPRR-s	<s> Partial route recording	7.5.5, ATN Ref: ⁋3.6.3.4.5	ePRR-s:M	M
epPRR-r	<r> Partial route recording	7.5.5, ATN Ref: ⁋3.6.3.4.5	ePRR-r:M	M
epCSR-s	<s> Complete source routing	7.5.4	eCSR:M	—
epPSR-s	<s> Partial source routing	7.5.4	ePSR:M	—
epQOSM-s	<s> QOS maintenance	7.5.6, ATN Ref: ⁋3.6.3.4.3, ⁋ 3.6.3.4.4	eQOSM-s or eCong-s:M	eQOSM-s:M
epQOSM-r	<r> QOS maintenance	7.5.6, ATN Ref: ⁋3.6.3.4.3, ⁋ 3.6.3.4.4	eQOSM-r or eCong-r :M	eQOSM-r or eCong-r:M
epPri-s	<s> Priority	7.5.7, ATN Ref: ⁋3.6.3.4.3, ⁋ 3.6.3.4.4	ePri-s:M	ePri-s:M
epPri-r	<r> Priority	7.5.7, ATN Ref: ⁋3.6.3.4.3, ⁋ 3.6.3.4.4	ePri-r:M	ePri-r:M
epData-s	<s> Data	7.6	M	M
epData-r	<r> Data	7.6	M	M
epUnSup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded and where appropriate an error report PDU generated?	6.21	M	M
epUnSup3	Are parameters selecting unsupported Type 3 functions ignored?	6.21	M	M

3.6.4.11 End systems – Timers

Item	*Timer*	*Ref*	*ISO status*	*ISO range*	*ATN support*	*Values supported*
ELifReas	Is reassembly timer <= received derived PDU lifetime?	6.8	M		M	
eReasTim	Reassembly timer	6.8	M	500ms to 127.5s	M	<= lifetime

3.6.4.12 Intermediate systems – Supported functions

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iPDUC	PDU composition	6.1	M	M
iPDUD	PDU decomposition	6.2	M	M
iHFA	Header format analysis	6.3	M	M
iPDUL	<s> PDU lifetime control	6.4	M	M
iRout	Route PDU	6.5	M	M
iForw	Forward PDU	6.6	M	M
iSegm	Segment PDU	6.7	iDSNS:M	iDSNS:M
iReas	Reassemble PDU	6.8	O	O
iDisc	Discard PDU	6.9	M	M
iErep	Error reporting	6.10	M	M
iEdec	<s> Header error detection	6.11	M	M
iSecu	<s>Security	6.13 ATN Ref: §3.6.2.2	O	M
iCRR	<s> Complete route recording	6.15	O	OX
iPRR	<s> Partial route recording	6.15	O	M
iCSR	Complete source routing	6.14	O	OX
iPSR	Partial source routing	6.14	O	OX
iPri	<s> Priority	6.17, ATN Ref: §3.6.3.5	O	M

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iQOSM	<s> QOS maintenance	6.16	O	M
iCong	<s> Congestion notification	6.18, ATN Ref: §3.6.2.4	O	M
iPadd	<s> Padding	6.12	M	M
iEreq	Echo request	6.19, ATN Ref: §3.6.3.3	O	O
iErsp	Echo response	6.20, ATN Ref: §3.6.3.4	O	M
iSegS	Create segments smaller than necessary	6.8	O	O
iDSNS	Simultaneous support of subnetworks with different SN-user data sizes	6.7	O	O

Note.— The classification "OX" indicates optional to implement, precluded to use.

3.6.4.12.1 Supported security parameters

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iSADSSEC	Source address specific security	7.5.3.1	iSecu:O.5	iSecu:O
iDADSSEC	Destination address specific security	7.5.3.2	iSecu:O.5	iSecu:O
iGUNSEC	Globally unique security	ATN Ref. §3.6.2.2	iSecu:O.5	iSecu:M

O.5: The security parameter within a single NPDU specifies a security format code indicating source address specific, destination address specific or globally unique security.

3.6.4.12.2 Quality of Service maintenance function

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iQOSNAVAIL	If requested QOS not available, deliver at different QOS	6.16	iQOSM:M	iQOSM:M
iQOSNOT	Notification of failure to meet requested QOS	6.16	iQOSM:O	iQOSM:O

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
	Which of the following formats of QOS are implemented?			
iSADDQOS	Source address specific QOS	7.5.6.1	iQOSM:O.3	iQOSM:O
iDADDQOS	Destination address specific QOS	7.5.6.2	iQOSM:O.3	iQOSM:O
iGUNQOS	Globally unique QOS	7.5.6.3	iQOSM:O.3	iQOSM:M
iSvTD	Sequencing versus transit delay	7.5.6.3	iGUNQOS:O.4	iGUNQOS:O.4
iCongE	Congestion experienced	7.5.6.3	iGUNQOS:O.4	iGUNQOS:M
iTDvCst	Transit delay versus cost	7.5.6.3	iGUNQOS:O.4	iGUNQOS:O.4
iREPvTD	Residual error probability versus transit delay	7.5.6.3	iGUNQOS:O.4	iGUNQOS:O.4
iREPvCst	Residual error probability versus cost	7.5.6.3	iGUNQOS:O.4	iGUNQOS:O.4

O.3: The Quality of Service maintenance parameter within a single NPDU specifies a QOS format code indicating source address specific, destination address specific or globally unique QOS.

O.4: If the QOS format code indicates that the globally unique QOS maintenance function is employed, then each bit in the associated parameter value may be set to indicate the order of intra and inter domain routing decisions based on QOS. The parameter values which apply to inter-domain routing are provided in Table 4 of ISO/IEC 10747.

3.6.4.13 Intermediate systems – Supported NPDUs

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iDT-t	DT (full protocol) transmit	7.7	M	M
iDT-r	DT (full protocol) receive	7.7	M	M
iDTNS-t	DT (non-segment) transmit	7.7	M	M
iDTNS-r	DT (non-segment) receive	7.7	M	M
iER-t	ER transmit	7.9	M	M
iER-r	ER receive	7.9	M	M
iERQ-t	ERQ transmit	7.10	iEreq:M	iEreq:M

Item	*Function*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iERQ-r	ERQ receive	7.10	M	M
iERP-t	ERP transmit	7.11	iErsp:M	iErsp:M
iERP-r	ERP receive	7.11	M	M

3.6.4.14 Intermediate systems – Supported DT parameters

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
idFxPt-s	<s> Fixed part	7.2	M	M
idFxPt-r	<r> Fixed part	7.2	M	M
idAddr-s	<s> Addresses	7.3	M	M
idAddr-r	<r> Addresses	7.3	M	M
idSeg-s	<s> Segmentation part	7.4	M	M
idSeg-r	<r> Segmentation part	7.4	M	M
idPadd-s	<s> Padding	7.5.2	M	M
idPadd-r	<r> Padding	7.5.2	M	M
idSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M
idSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
idCRR-s	<s> Complete route recording	7.5.5	iCRR:M	—
idCRR-r	<r> Complete route recording	7.5.5	iCRR:M	—
idPRR-s	<s> Partial route recording	7.5.5	M	M
idPRR-r	<r> Partial route recording	7.5.5	iPRR:M	M
idCSR-s	<s> Complete source routing	7.5.4	iCSR:M	—
idCSR-r	<r> Complete source routing	7.5.4	iCSR:M	—
idPSR-s	<s> Partial source routing	7.5.4	M	M
idPSR-r	<r> Partial source routing	7.5.4	iPSR:M	—
idQOSM-s	<s> QOS maintenance	7.5.6	M	M
idQOSM-r	<r> QOS maintenance	7.5.6	iQOSM or iCong:M	iQOSM or iCong:M

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN support
idPri-s	<s> Priority	7.5.7	M	M
idPri-r	<r> Priority	7.5.7	iPri:M	iPri:M
idData-s	<s> Data	7.6	M	M
idData-r	<r> Data	7.6	M	M
idUnSup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded and where appropriate an error report PDU generated?	6.19	M	M
idUnSup3	Are parameters selecting unsupported Type 3 functions ignored?	6.19	M	M

3.6.4.15 Intermediate systems – Supported ER parameters

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN support
ieFxPt-s	<s> Fixed part	7.2	M	M
ieFxPt-r	<r> Fixed part	7.2	M	M
ieAddr-s	<s> Address	7.3	M	M
ieAddr-r	<r> Address	7.3	M	M
iePadd-s	<s> Padding	7.5.2	M	M
iePadd-r	<r> Padding	7.5.2	M	M
ieSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M
ieSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
ieCRR-s	<s> Complete route recording	7.5.5	iCRR:M	—
ieCRR-r	<r> Complete route recording	7.5.5	iCRR:M	—
iePRR-s	<s> Partial route recording	7.5.5	M	M
iePRR-r	<r> Partial route recording	7.5.5	iPRR:M	M
ieCSR-s	<s> Complete source routing	7.5.4	iCSR:M	—
ieCSR-r	<r> Complete source routing	7.5.4	iCSR:M	—

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iePSR-s	<s> Partial source routing	7.5.4	M	M
iePSR-r	<r> Partial source routing	7.5.4	iPSR:M	—
ieQOSM-s	<s> QOS maintenance	7.5.6	M	M
ieQOSM-r	<r> QOS maintenance	7.5.6	iQOSM or iCong:M	iQOSM or iCong:M
iePri-s	<s> Priority	7.5.7	M	M
iePri-r	<r> Priority	7.5.7	iPri:M	iPri:M
ieDisc-s	<s> Reason for discard	7.9.5	M	M
ieDisc-r	<r> Reason for discard	7.9.5	M	M
ieData-s	<s> Data	7.6	M	M
ieData-r	<r> Data	7.6	M	M
ieUnsup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded?	6.21	M	M
ieUnsup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

3.6.4.16 Intermediate systems – Supported ERQ parameters

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iqFxPt-s	<s> Fixed part	7.2	M	M
iqFxPt-r	<r> Fixed part	7.2	M	M
iqAddr-s	<s> Addresses	7.3	M	M
iqAddr-r	<r> Addresses	7.3	M	M
iqSeg-s	<s> Segmentation part	7.4	M	M
iqSeg-r	<r> Segmentation part	7.4	M	M
iqPadd-s	<s> Padding	7.5.2	M	M
iqPadd-r	<r> Padding	7.5.2	M	M
iqSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN support
iqSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
iqCRR-s	<s> Complete route recording	7.5.5	iCRR:M	—
iqCRR-r	<r> Complete route recording	7.5.5	iCRR:M	—
iqPRR-s	<s> Partial route recording	7.5.5	M	M
iqPRR-r	<r> Partial route recording	7.5.5	iPRR:M	M
iqCSR-s	<s> Complete source routing	7.5.4	iCSR:M	—
iqCSR-r	<r> Complete source routing	7.5.4	iCSR:M	—
iqPSR-s	<s> Partial source routing	7.5.4	M	M
iqPSR-r	<r> Partial source routing	7.5.4	iPSR:M	—
iqQOSM-s	<s> QOS maintenance	7.5.6	M	M
iqQOSM-r	<r> QOS maintenance	7.5.6	iQOSM or iCong:M	iQOSM or ICong:M
iqPri-s	<s> Priority	7.5.7	M	M
iqPri-r	<r> Priority	7.5.7	iPri:M	iPri:M
iqData-s	<s> Data	7.6	M	M
iqData-r	<r> Data	7.6	M	M
iqUnSup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded and where appropriate an error report PDU generated?	6.19	M	M
iqUnSup3	Are parameters selecting unsupported Type 3 functions ignored?	6.19	M	M

3.6.4.17 Intermediate systems – Supported ERP parameters

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN support
ipFxPt-s	<s> Fixed part	7.2	M	M
ipFxPt-r	<r> Fixed part	7.2	M	M
ipAddr-s	<s> Addresses	7.3	M	M

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
ipAddr-r	<r> Addresses	7.3	M	M
ipSeg-s	<s> Segmentation part	7.4	M	M
ipSeg-r	<r> Segmentation part	7.4	M	M
ipPadd-s	<s> Padding	7.5.2	M	M
ipPadd-r	<r> Padding	7.5.2	M	M
ipSecu-s	<s> Security	7.5.3, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	iSecu:M	iSecu:M
ipSecu-r	<r> Security	7.5.3, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	iSecu:M	iSecu:M
ipCRR-s	<s> Complete route recording	7.5.5	iCRR:M	—
ipCRR-r	<r> Complete route recording	7.5.5	iCRR:M	—
ipPRR-s	<s> Partial route recording	7.5.5, ATN Ref: 3.6.3.4.5	M	M
ipPRR-r	<r> Partial route recording	7.5.5, ATN Ref: 3.6.3.4.5	iPRR:M	M
ipCSR-s	<s> Complete source routing	7.5.4	iCSR:M	—
ipCSR-r	<r> Complete source routing	7.5.4	iCSR:M	—
ipPSR-s	<s> Partial source routing	7.5.4	M	M
ipPSR-r	<r> Partial source routing	7.5.4	iPSR:M	-
ipQOSM-s	<s> QOS maintenance	7.5.6, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	M	M
ipQOSM-r	<r> QOS maintenance	7.5.6, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	iQOSM or iCong:M	iQOSM or iCong:M
ipPri-s	<s> Priority	7.5.7, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	M	M
ipPri-r	<r> Priority	7.5.7, ATN Ref: 3.6.3.4.3, 3.6.3.4.4	iPri:M	iPri:M

Item	*Parameter*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
ipData-s	<s> Data	7.6	M	M
ipData-r	<r> Data	7.6	M	M
ipUnsup2	Are received PDUs containing parameters selecting unsupported Type 2 functions discarded and where appropriate an error report PDU generated?	6.19	M	M
ipUnsup3	Are parameters selecting unsupported Type 3 functions ignored?	6.19	M	M

3.6.4.18 Intermediate systems – Timer and parameter values

Item	*Timer*	*ISO/IEC 8473-1 Reference*	*Status*	*ATN support*
iReasTim	Reassembly timer	6.8	iReas:M	iReas:M

3.7 SPECIFICATION OF SUBNETWORK DEPENDENT CONVERGENCE FUNCTIONS

3.7.1 Introduction

Note 1.— The purpose of a subnetwork dependent convergence function (SNDCF) is to provide the connectionless SN-service assumed by the ATN Internet protocols over real subnetworks.

Note 2.— The subnetwork service (SN-Service) provided by an SNDCF and as specified in this chapter is provided to the ISO/IEC 8473 Internetwork protocol and the ISO/IEC 9542 end system to intermediate system protocol entities.

Note 3.— The ATN Internetwork layer, including CLNP and the routing protocols that support it, assumes this common connectionless service to be provided by all subnetworks providing communications between ATN systems.

Note 4.— Figure 3-9 illustrates the relationships between the SNDCFs defined in this chapter, the SN-service that they provide to CLNP and ES-IS, and the underlying subnetworks.

Note 5.— There is no requirement to implement this service as a software interface.

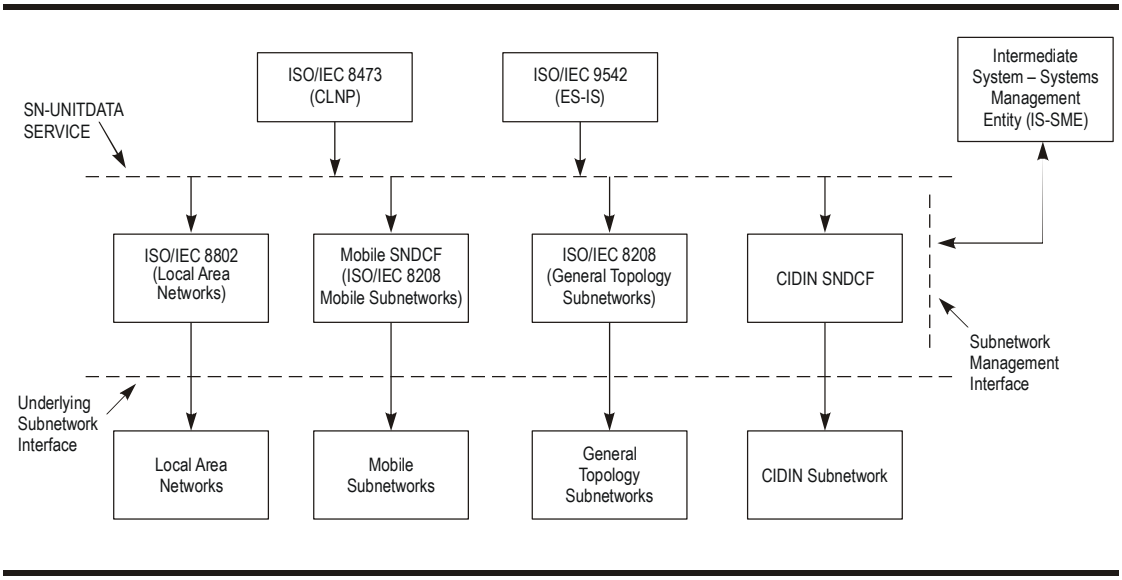


Figure 3-9. Relationship of SNDCFs to SN-Service and underlying subnetworks

3.7.2 Service provided by the SNDCF

Note 1.— This section specifies the assumed service provided internally by the SNDCF for the purpose of conveying network data PDUs between network entities.

Note 2.— The service to support SN-service-users is defined by the primitives in Table 3-12.

Table 3-12. SN-services and associated parameters

Parameter	*SN-UNITDATA request*	*SN-UNITDATA indication*
SN-Source-Address	Mandatory	Mandatory
SN-Destination-Address	Mandatory	Mandatory
SN-Priority	Optional	Optional
SN-Quality-of-Service	Optional	Optional
SNS-Userdata	Mandatory	Mandatory

3.7.2.1 Subnetwork service primitive parameters

Note.— The following sections specify the subnetwork service primitive parameters.

3.7.2.1.1 Subnetwork point of attachment (SNPA) addresses

Note.— The SN-source-address and SN-destination-address parameters specify the points of attachment to a public or private subnetwork(s). The SN-source-address and SN-destination-address addresses include information

denoting a particular underlying subnetwork, as well as addressing information for systems attached directly to that subnetwork. SNPA values for a particular subnetwork are those specified and administered by the authority responsible for administration of that subnetwork.

3.7.2.1.2 SN-priority

Note 1.— The SN-priority parameter indicates the relative importance of the associated SNS-userdata parameter and may influence the order in which the SNS-userdata are transferred via the real underlying subnetwork service.

Note 2.— SN-priority values are in the range zero to fourteen, with higher values indicating higher priorities.

Note 3.— If no SN-priority is indicated, the value zero is assumed to be the default.

Note 4.— Further requirements related to subnetwork priority are specified in 3.2.8.5.

3.7.2.1.3 Subnetwork Quality of Service (SNQoS)

Note 1.— The use of the SN-Quality-of-Service parameter is optional and depends on the needs of the SN-service-user.

Note 2.— Associated with each connectionless-mode transmission, certain measures of Quality of Service are requested when the SN-UNITDATA primitive action is initiated. These requested measures (or parameter values and options) are based on a priori knowledge of the service available from the subnetwork. Knowledge of the nature and type of service available is typically obtained prior to an invocation of the underlying connectionless-mode service and the information passed is a local matter.

3.7.2.1.4 Subnetwork service userdata

Note 1.— The SNS-userdata contains the ISO/IEC 8473 or ISO/IEC 9542 NPDU that has to be conveyed between adjacent network entities.

Note 2.— The SNS-userdata is an ordered multiple of octets and is transferred transparently between the subnetwork points of attachment specified in the SNS primitive.

3.7.3 SNDCF for ISO/IEC 8802-2 subnetworks

Note.— ISO/IEC 8802-2 subnetworks are subnetworks that provide the logical link control sublayer service defined by ISO/IEC 8802-2.

3.7.3.1 The SNDCF for use with ISO/IEC 8802-2 subnetworks shall be implemented according to ISO/IEC 8473-2.

3.7.3.2 APRLs

3.7.3.2.1 An implementation of the ISO/IEC 8802 SNDCF shall be used in ATN end systems and routers if and only if its PICS is in compliance with the APRLs given in 3.7.3.2.2 and 3.7.3.2.3.

3.7.3.2.2 Subnetwork dependent convergence functions SNDCF for use with ISO/IEC 8802-2 Subnetworks – Functions

Item	*Function*	*ISO/IEC 8473-2 Reference*	*Status*	*ATN support*
S802SNUD	Is subnetwork user data of at least 512 octets transferred transparently by the SNDCF ?	5.2	M	M
S802SNTD	Is transit delay determined by the SNDCF prior to the processing of user data ?	5.2	M	M

3.7.3.2.3 Subnetwork dependent convergence functions SNDCF for use with ISO/IEC 8802-2 Subnetworks – multi layer dependencies

Item	*Dependency*	*ISO/IEC 8473-2 Reference*	*ATN support*
S802SSg-r	<r> Maximum SN data unit size (RX)	5.2	>=512
S802SSg-s	<s> Maximum SN data unit size (TX)	5.2	>=512

3.7.4 SNDCF for ISO/IEC 8208 mobile subnetworks

3.7.4.1 General

3.7.4.1.1 Over ISO/IEC 8208 mobile subnetworks, the subnetwork service described in 3.7.2 shall be provided using the SNDCF for ISO/IEC 8208 mobile subnetworks as specified below.

Note 1.— The SNDCF specified below is only applicable when providing the SN-UNITDATA service to ISO/IEC 8473, ISO/IEC 9542, ISO/IEC 11577 and ISO/IEC 10589 network layer protocols. Unpredictable behavior may result if used to support other network layer entities.

Note 2.— This SNDCF supports the following data compression procedures:

- *Local reference (LREF) compression as specified in 3.7.4.3;*
- *Data stream mode compression as specified in 3.7.4.5.*

Note 3.— The Data stream mode compression uses the deflate algorithm which was originally specified in IETF RFC 1951.

Note 4.— Optional features of LREF compression provide for "local reference cancellation" and for "maintenance of the local reference directory". The mechanism for maintaining the local reference directory requires the support of the ISO/IEC 8208 fast select facility.

Note 5.—Optional features of data stream compression provide for "Negotiation of the use of pre-stored dictionaries" and for "Maintenance of the deflate history windows". These mechanisms require the support of the ISO/IEC 8208 fast select facility.

Note 6.— A subnetwork connection group is the set of virtual circuits simultaneously active between the same pair of DTEs, and which use the same subnetwork priority level, the same data compression mechanism(s) and the same optional features of LREF compression, if any.

Note 7.— When the LREF compression is used in the context of a subnetwork connection group, the same local reference directory (as defined in 3.7.4.3.1) is shared between all the virtual circuits of this subnetwork connection group.

Note 8.— If a subnetwork connection group already exists with the same remote DTE and the same compression mechanisms but with a different priority than the one used by the newly established virtual circuit, this circuit may not use the local reference directory of this group, as packets will not travel at the same speed on two circuits which have different priorities.

Note 9.— The supported data compression mechanisms and their options are negotiated when each virtual circuit used by the SNDCF is established. As a result of this negotiation, the virtual circuit is placed into a new subnetwork connection group or is inserted in an existing subnetwork connection group. Negotiated data compression mechanisms and optional features of LREF compression are applied on a subnetwork connection group basis. This means that the same compression mechanism(s) and the same LREF compression option(s) are used for all virtual circuits established in the context of the same subnetwork connection group. Optional features of data stream compression are applied on a virtual circuit basis. This means that virtual circuits established in the context of the same subnetwork connection group may use different data stream compression options (e.g. different pre-stored dictionaries).

3.7.4.1.2 All ATN intermediate systems using mobile ISO/IEC 8208 subnetworks for communication with other intermediate systems shall implement the LREF compression procedure.

3.7.4.1.3 Implementations using this SNDCF for air-ground communications should only implement the LREF optional facility for local reference cancellation when the lifetime of the virtual circuits is of the same order as the flight time.

3.7.4.2 Call setup

3.7.4.2.1 Calling DTE procedures

3.7.4.2.1.1 *General*

3.7.4.2.1.1.1 When it has been determined that a virtual circuit is to be made available, the calling SNDCF shall establish the virtual circuit using the procedures specified in ISO/IEC 8208, either:

a) dynamically, on receipt of a SN-UNITDATA request and when the SNDCF lacks a suitable virtual channel to the NPDU's destination supporting the required priority and QoS; or

b) by the explicit intervention of systems management, identifying the destination SNDCF's SNPA address, priority and QoS.

3.7.4.2.1.1.2 An ISO/IEC 8208 CALL REQUEST packet shall be sent to the DTE address specified as the SN-destination-address, with the following optional user facilities and CCITT-specified DTE facilities.

Note 1.— Normally, this is achieved by encoding the destination DTE address as the called address of the ISO/IEC 8208 call request packet. This is appropriate when the ATN router is directly connected to the air-ground subnetwork, or when it is connected to the air-ground subnetwork via another subnetwork and an interworking facility (ISO TR 10029). However, when the ATN router is connected to the air-ground subnetwork via another subnetwork and

an interworking facility is not available, one possible alternative approach is to address the ISO/IEC 8208 call request packet to the access point of the air-ground subnetwork (e.g. a GDLP) and convey the destination DTE Address in the called address extension facility of the ISO/IEC 8208 call request packet whereas the DTE addresses configured for the local access point of the air-ground subnetwork is encoded in the called address field of the ISO/IEC 8208 call request packet. It is then the responsibility of the air-ground subnetwork access facility to reformat the received ISO/IEC 8208 call request packet into a call request packet appropriate for transmission to the destination DTE address over the air-ground subnetwork.

Note 2.— Other optional user facilities and CCITT-specified DTE facilities may be required by subnetworks. The use of these facilities is a local matter.

3.7.4.2.1.1.3 The call request user data shall be formatted as specified in 3.7.4.2.1.5.

3.7.4.2.1.2 *The priority facility*

3.7.4.2.1.2.1 The mapping of ATN network layer priorities to ATN mobile subnetwork priorities shall be as defined in Annex 10, Volume III, Part 1, Chapter 3, Table 3-2 for those mobile subnetworks subject to ICAO Standards.

3.7.4.2.1.2.2 For mobile subnetworks not subject to ICAO Standards, the priority facility shall be used if the subnetwork provider supports prioritization of virtual circuits and specifies the mapping of network service to subnetwork service priorities.

3.7.4.2.1.2.3 The priority value passed in the SN-UNITDATA request or indicated by the System Manager shall be mapped to priority of data on a connection, as specified by the subnetwork provider.

3.7.4.2.1.2.4 If the priority to gain a connection and/or priority to keep a connection is conveyed within the ISO/IEC 8208 facility parameter field, these priorities shall be consistent with the priority of data on a connection and set according to the subnetwork provider's guidelines.

Note 1.— The SNDCF is assumed to know, a priori, if a given subnetwork supports prioritization of virtual circuits, the number of discrete priority levels supported and the relationship between the subnetwork priority and SNSDU priority.

Note 2.— The mapping between SNSDU priority and subnetwork priority is specified separately for each subnetwork type.

3.7.4.2.1.3 *Non-standard default packet size facility and flow control parameter negotiation facility*

Either the non-standard default packet size facility or the flow control parameter negotiation facility shall be used to request the maximum packet size supported by the subnetwork.

Note.— The selection of which facility to use is dependent on the facilities supported by the subnetwork.

3.7.4.2.1.4 *The fast select facility*

3.7.4.2.1.4.1 The fast select facility shall be used if supported by all subnetwork provider(s) in the DTE-DTE virtual path.

Note.— Airborne routers are assumed to have a priori knowledge of fast select support (or lack thereof) along the DTE-DTE virtual path based on each individual destination air-ground router's DTE address.

3.7.4.2.1.4.2 No restriction on response shall be indicated.

Note 1.— This permits the responding DTE to accept the call and to return up to 128 octets of user data.

Note 2.— If fast select is not supported, the compression procedures can only be negotiated by successive attempts to establish the virtual circuit requesting different combinations of compression procedures.

3.7.4.2.1.5 *Call request user data*

Note.— Call request user data is used to indicate which compression procedures are offered by the calling DTE. When the fast select facility is used, call accept user data is then used to indicate which compression procedures are accepted by the called DTE.

3.7.4.2.1.5.1 The call request user data format shall be as illustrated in Figure 3-10.

3.7.4.2.1.5.2 The first octet of the call user data (the subsequent protocol identifier (SPI)) shall be set to binary [1100 0001] to indicate that the virtual circuit is to be used to provide the underlying service by this SNDCF.

Note.— ISO TR 9577 provides the international register for SPI values. The value binary [1100 0001] has not been assigned by the ISO technical report and it is unlikely that it will be.

3.7.4.2.1.5.3 The second octet is the length indicator of the subsequent SNDCF parameter block, and its value shall be an unsigned binary number giving the number of octets in the SNDCF parameter block (from version number field up to and including (if present) the maximum number of directory entries field).

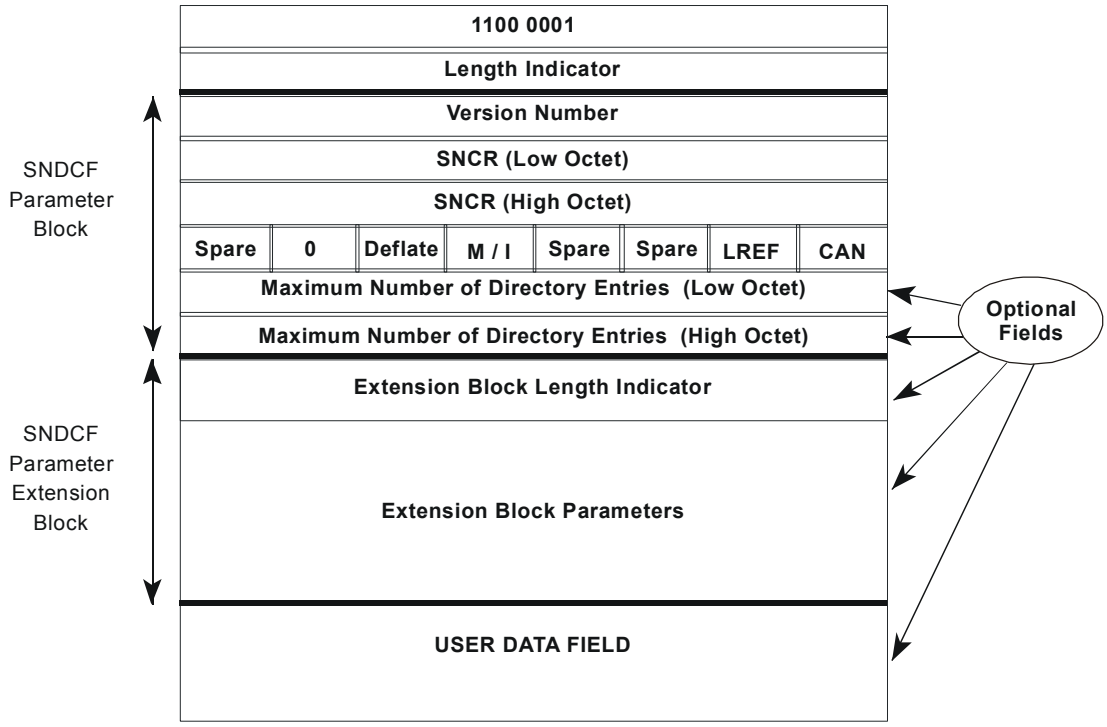


Figure 3-10. Format for call request user data

3.7.4.2.1.5.4 SNDCF parameter block

Note.— The SNDCF parameter block contains a fixed part and an optional part. The fixed part is 4 octets long and is always present; it contains the parameter's version number, subnetwork connection reference (SNCR), and compression techniques. The optional part is 1 or 2 octets long; it is present if the LREF compression algorithm is offered and is used to define the maximum directory size of the LREF directory.

3.7.4.2.1.5.4.1 The first octet of the SNDCF parameter block is the SNDCF version number and shall be set to [0000 0010], if the call request user data contains an SNDCF extension parameter block (see 3.7.4.2.1.5.4.13), and to [0000 0001] otherwise.

Note 1.— The value [0000 0001] indicates the first version of the SNDCF protocol. This version is compliant with the SNDCF provisions contained in previous editions of this specification.

Note 2.— The value [0000 0010] indicates the second version of the SNDCF protocol which has been added to the third edition of this specification.

3.7.4.2.1.5.4.1.1 When a subnetwork connection group with the called DTE already exists, then the SNDCF version number, which has been used to establish this subnetwork connection group, shall also be used when establishing any further virtual circuit within this group and the call request user data be formatted according to this SNDCF version number.

Note.— The use of the second version of the SNDCF protocol has to be avoided when it can be a priori known that the called DTE only supports a lower version of the protocol. Such a priori knowledge exists, for example, when the called DTE has previously rejected a call with a diagnostic code indicating "Version number not supported".

3.7.4.2.1.5.4.1.2 The version number of the SNDCF protocol used by the calling DTE when initiating a call request should be configurable.

3.7.4.2.1.5.4.2 The second and third octets of the SNDCF parameter block shall provide the low order and high order octet, respectively, of the subnetwork connection reference (SNCR).

3.7.4.2.1.5.4.3 The value encoded in this field shall be the lowest available SNCR value in the range from 0 up to one less than the number of virtual circuits needed at this call priority.

Note.— The use of the SNCR is specified in ISO/IEC 8473 for use in call collision resolution over ISO/IEC 8208 subnetworks.

3.7.4.2.1.5.4.4 The fourth octet of the SNDCF parameter block shall indicate the compression techniques offered by the calling DTE, according to Table 3-13 and Figure 3-10.

3.7.4.2.1.5.4.5 Those bits of Table 3-13 and Figure 3-10 which are marked as "Spare" are reserved for future use by this specification and shall always be set to zero.

3.7.4.2.1.5.4.6 LREF compression shall always be offered.

Note 1.— This specification mandates the use of the LREF compression algorithm. This may not be true in future editions of this specification. Hence procedures are specified to negotiate the use of the LREF compression on a per virtual circuit basis.

Table 3-13. Compression options offered parameter

Bit number	*Option*
bit 8	Spare
bit 7	*Note.— In earlier versions of this specification this bit was used to indicate the ICAO address compression algorithm (ACA). To ensure backwards compatibility with these versions an incoming call with bit 7 set to 1 will be rejected indicating the diagnostic value 135 (see Table 3-15).*
bit 6	Deflate
bit 5	Maintenance/initiation of local reference directory (M/I) option
bit 4	Spare
bit 3	Spare
bit 2	Local reference (LREF) option
bit 1	Local reference cancellation (CAN) option supported

Note 2.— The decision as regards which options to offer out of those supported is otherwise a local matter.

Note 3.— Multiple compression procedures may be offered.

3.7.4.2.1.5.4.7 Bit 1 of the fourth octet of the SNDCF parameter block shall only be set if bit 2 is also set.

3.7.4.2.1.5.4.8 Bit 5 (M/I bit) of the fourth octet of the SNDCF parameter block shall be set to one by the calling SNDCF when the calling SNDCF has identified a subnetwork connection group with the called DTE, with the requested subnetwork priority and with the same data compression mechanisms and the same optional features of LREF compression, to request that the newly established circuit shares the local reference directory associated with this group.

3.7.4.2.1.5.4.9 The request for local reference directory maintenance shall only be used when the call request uses the fast select facility and when bit 2 of the compression options parameter (Local reference compression) is set to one.

3.7.4.2.1.5.4.10 When the request for local reference directory maintenance is used, then the subnetwork connection reference (SNCR) of the call request packet shall be set to the lowest available SNCR value in the range from 0 up to one less than the number of virtual circuits needed at this call priority.

3.7.4.2.1.5.4.11 When the LREF compression algorithm is offered, i.e. if bit 2 in the fourth octet of the SNDCF parameter block is set, then the value of the fifth and sixth octets (Maximum directory entries) shall be an unsigned even binary number indicating the maximum number of directory entries supported for the local reference (minimum size 128).

3.7.4.2.1.5.4.12 Bit 2 of the fourth octet of the SNDCF parameter block shall be set to zero.

3.7.4.2.1.5.4.13 SNDCF parameter extension block

Note.— The optional SNDCF parameter extension block has a variable length and is used to convey parameters related to advanced compression features, such as use of pre-stored data stream compression dictionaries and maintenance of the deflate compression history window. Parameters defined in this extension block may appear in any order.

3.7.4.2.1.5.4.14 When the SNDCF parameter extension block is present, then the first octet of this block shall be the octet immediately following the SNDCF parameter block.

3.7.4.2.1.5.4.15 The first octet of the SNDCF parameter extension block is the length indicator of this block and shall indicate the number of octets in the SNDCF parameter extension block (including its length indicator field) as an unsigned binary number with a maximum value of 121.

3.7.4.2.1.5.4.16 Each parameter contained within the SNDCF parameter extension block shall be structured as illustrated in Figure 3-11.

Octets	*Semantics*
1	Parameter code
2	Parameter length indication
3 ... m	Parameter value

Figure 3-11. Format of parameters in the SNDCF parameter extension block

3.7.4.2.1.5.4.17 The parameter code field shall be coded in binary.

3.7.4.2.1.5.4.18 There shall be no more than one parameter with the same parameter code in the SNDCF parameter extension block.

3.7.4.2.1.5.4.19 The parameter length indication field shall indicate the number of octets of the parameter value field.

3.7.4.2.1.5.4.20 Dictionaries list parameter

3.7.4.2.1.5.4.20.1 When the use of pre-stored data stream compression dictionaries is supported, the SNDCF parameter extension block shall include a dictionaries list parameter if the following conditions are satisfied:

a) the deflate compression algorithm is offered, i.e. bit 6 in the fourth octet of the SNDCF parameter block is set; and

b) the call request uses the fast select facility.

3.7.4.2.1.5.4.20.2 The dictionaries list parameter shall be encoded as defined in 3.7.4.2.1.5.8.

3.7.4.2.1.5.4.21 Deflate maintenance parameter

3.7.4.2.1.5.4.21.1 When the option for the maintenance of the deflate history windows is supported, the SNDCF parameter extension block shall include a deflate maintenance parameter, if all of the following conditions are satisfied:

a) the deflate compression algorithm is offered, i.e. bit 6 in the fourth octet of the SNDCF parameter block is set;

b) a subnetwork connection group already exists with the same remote DTE, with the requested subnetwork priority and with the same data compression mechanisms and the same optional features of LREF compression;

c) the values of bit 2 (LREF option) and bit 5 (M/I option) in the fourth octet of the SNDCF parameter block are equal (i.e. both bits are set to 0 or both bits are set to 1);

d) the call request uses the fast select facility.

3.7.4.2.1.5.4.21.2 The deflate maintenance parameter shall be encoded as defined in 3.7.4.2.1.5.9.

3.7.4.2.1.5.5 When the call request user data contains an SNDCF parameter extension block, then the octet following the SNDCF parameter extension block shall be the first octet of the user data field, if present.

3.7.4.2.1.5.6 Otherwise, the octet following the SNDCF parameter block shall be the first octet of the user data field, if present.

3.7.4.2.1.5.7 The information in the user data field of the call request user data shall not be compressed. When the fast select facility is available, the user data field may be used to convey the ISO/IEC 9542 ISH PDU as part of the routing initiation sequence.

3.7.4.2.1.5.8 Encoding of the dictionaries list parameter

3.7.4.2.1.5.8.1 The dictionaries list parameter shall be structured as illustrated in Figure 3-11.

3.7.4.2.1.5.8.2 The parameter code field of the dictionaries list parameter shall be set to [0000 0001].

3.7.4.2.1.5.8.3 The parameter value field of the dictionaries list parameter shall consist of one or more dictionary tags, as defined in 3.7.4.2.1.5.8.7, identifying the latest supported version of the data stream compression dictionaries supported by the calling DTE.

3.7.4.2.1.5.8.4 A calling DTE shall only indicate support of a given version of a data stream compression dictionary if it also supports all previous versions of the same data stream compression dictionary.

3.7.4.2.1.5.8.5 Within the dictionaries list parameter value field, the dictionary tags shall appear in the order of preference of the calling DTE, whereby the first dictionary tag identifies the most preferred dictionary.

3.7.4.2.1.5.8.6 Within the dictionaries list parameter value field, there shall be no duplication of a dictionary tag.

3.7.4.2.1.5.8.7 Encoding of the dictionary tag

Note 1.— A dictionary tag uniquely identifies a data stream compression dictionary.

Note 2.— A data stream compression dictionary consists of an octetstring of frequently used symbols in the uplink direction and of an octetstring of frequently used symbols in the downlink direction. Each of these two octetstrings may be up to 32KB long.

3.7.4.2.1.5.8.7.1 A dictionary tag shall be two octets in length.

3.7.4.2.1.5.8.7.2 The two most significant bits of the first octet of a dictionary tag shall identify the registration authority of the data stream compression dictionary, as indicated in Table 3-14.

Table 3-14. Encoding of the first octet of a dictionary tag

Bit 8	*Bit 7*	*Registration authority*
0	0	ICAO
0	1	IATA
1	0	Reserved
1	1	Reserved

3.7.4.2.1.5.8.7.3 The six least significant bits of the first octet of a dictionary tag shall identify one data stream compression dictionary registered by the registration authority identified by the two most significant bits.

Note.— At present, no data stream compression dictionary has been registered by ICAO.

3.7.4.2.1.5.8.7.4 The second octet of a dictionary tag shall be an unsigned binary number in the range [01-FF] (hexadecimal) identifying the latest version of this data stream compression dictionary being supported by the ATN router.

3.7.4.2.1.5.9 Encoding of the deflate maintenance parameter

3.7.4.2.1.5.9.1 The deflate maintenance parameter shall be structured as illustrated in Figure 3-11.

3.7.4.2.1.5.9.2 The parameter code of the deflate maintenance parameter shall be set to [0000 0010].

3.7.4.2.1.5.9.3 The parameter length field of the deflate maintenance parameter shall be set to 4.

3.7.4.2.1.5.9.4 The parameter value field of the deflate maintenance parameter shall be a 4 octets-long unsigned binary number that is encoded least significant byte first, least significant bit first.

3.7.4.2.1.5.9.5 The parameter value field of the deflate maintenance parameter shall be set to the absolute value of the upper edge of the decompressor history window being maintained over this subnetwork connection group.

Note.— The absolute value of the upper edge of the decompressor history window is defined in 3.7.4.5.9.3.

3.7.4.2.1.5.10 Procedure associated with the use of the deflate maintenance parameter

When the maintenance of the deflate history window option is offered, the calling DTE shall duplicate the decompressor history window currently used for deflate compression over the last virtual circuit established in the context of the subnetwork connection group and register this copy as the initial decompressor history window to be used for deflate decompression over the virtual circuit being established.

Note.— A physically separate copy is required because the content of the history windows of the preceeding virtual circuit in that subnetwork connection group may still evolve while the new virtual circuit is being established.

3.7.4.2.1.6 *Receipt of "Call Confirm Packet"*

3.7.4.2.1.6.1 Fast select facility in use

3.7.4.2.1.6.1.1 When an ISO/IEC 8208 call confirm packet is received from the called DTE and the fast select facility is in use, then the calling DTE shall inspect the first octet of the received call confirm user data (see 3.7.4.2.2.4.3) in order to determine which of the offered compression procedures have been accepted and whether the call confirm user data contains an SNDCF parameter extension block.

3.7.4.2.1.6.1.2 If the called SNDCF has accepted the call indicating that an offered compression procedure is not supported, then the calling SNDCF shall maintain the virtual circuit and shall not apply this compression procedure.

3.7.4.2.1.6.1.3 If the M/I bit is set to zero in the first octet of the call confirm user data and if a deflate maintenance parameter is not present in the SNDCF parameter extension block, then a new subnetwork connection group shall be created and the newly established virtual circuit becomes the first member of that group.

3.7.4.2.1.6.1.4 If the M/I bit is set to one in the first octet of the call confirm user data and the M/I bit in the preceding call request had also been set to one, then the newly established virtual circuit shall be inserted into the subnetwork connection group identified when the call request was issued.

3.7.4.2.1.6.1.5 If the M/I bit is set to one in the first octet of the call confirm user data, and M/I bit had been set to zero in the preceding call request, then this is an error condition, and the call shall be cleared with an ISO/IEC 8208 cause code of zero, and a diagnostic code of 242 (Disconnection – incompatible information in user data).

3.7.4.2.1.6.1.6 If the PEXT bit is set to zero in the first octet of the call confirm user data and a SNDCF parameter extension block containing a dictionaries list parameter or a deflate maintenance parameter, respectively, was present in the associated call request user data, then the calling SNDCF shall assume that none of the proposed dictionaries has been accepted by the called SNDCF and/or that the called SNDCF has not accepted to maintain the deflate history windows, respectively.

3.7.4.2.1.6.1.7 If the PEXT bit is set to one in the first octet of the call confirm user data, then the call confirm user data contains an SNDCF parameter extension block and the calling SNDCF shall process this parameter extension block as specified in 3.7.4.2.1.6.1.11.

3.7.4.2.1.6.1.8 If the PEXT bit in the first octet of the received call confirm user data:

a) is set to one and the length of the call confirm user data is greater than the value of the first octet of the received SNDCF parameter extension block (i.e. length indicator) plus 1; or

b) is not set to one and the length of the Call Confirm User Data is greater than one;

then the received call confirm user data contains additional data, and the calling SNDCF shall inspect the first octet of the user data field (see Figure 3-12) whether it contains a recognized NPDU SPI.

Note.— The additional data, if any, is processed without performing any of the decompression mechanisms that may have been negotiated.

3.7.4.2.1.6.1.9 If the inspected octet contains a recognized NPDU SPI, then the calling SNDCF shall pass this octet and the remaining part of the received call confirm user data (i.e. the NPDU) in an SN-UNITDATA indication to the appropriate SN-service user, using the received SPI to identify the network layer protocol, and hence which SN-service user is responsible for handling this NPDU.

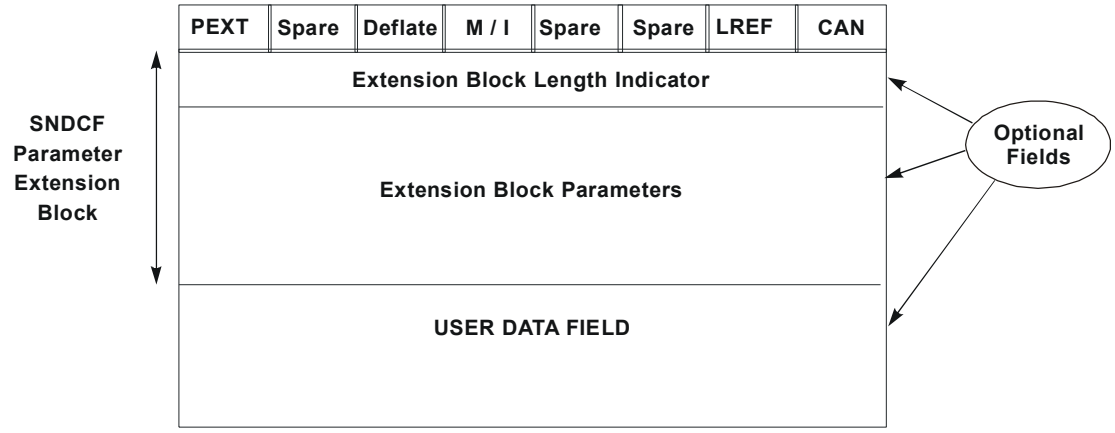


Figure 3-12. Format for call accept user data

3.7.4.2.1.6.1.10 If no such SN-service user exists or the inspected octet does not contain a recognized NPDU SPI, then the additional data in the call confirm user data shall be discarded.

3.7.4.2.1.6.1.11 Processing of SNDCF parameter extension block

3.7.4.2.1.6.1.11.1 If the SNDCF parameter extension block contains an unknown optional parameter, then this parameter shall be ignored but the received ISO/IEC 8208 call confirm packet not be discarded.

3.7.4.2.1.6.1.11.2 If a deflate maintenance parameter is present in the SNDCF parameter extension block, the following cases are error conditions:

a) the preceeding call request did not convey any deflate maintenance parameter;

b) bit 6 (i.e. deflate bit) of the first octet of the call confirm user data is not set;

c) the values of bit 2 (LREF option) and bit 5 (M/I option) of the first octet of the call confirm user data are not equal;

d) a dictionary selection parameter is also present in the SNDCF parameter extension block;

e) more than one deflate maintenance parameter is present in the SNDCF parameter extension block;

and shall be handled by clearing the call with an ISO/IEC 8208 cause code of zero, and a diagnostic Code of 242 (i.e. Disconnection – incompatible information in user data).

3.7.4.2.1.6.1.11.3 If the value of the deflate maintenance parameter is such that the position of the upper edge of the remote DTE decompressor window is indicated to be higher than the position of the upper edge of the local compressor window, then:

a) the calling DTE shall clear the virtual circuit with a cause code set to zero, and a diagnostic code set to 242 (i.e Disconnection – incompatible information in user data);

b) the calling DTE shall then re-attempt to establish the virtual circuit without proposing maintenance of the deflate history windows;

c) this error condition shall be reported to systems management.

Note.— Because of wrap around, implementors must treat the term "higher" with a certain degree of caution.

3.7.4.2.1.6.1.11.4 If a deflate maintenance parameter is present in the SNDCF parameter extension block and if none of the above error conditions is encountered, then the newly established virtual circuit shall be inserted into the subnetwork connection group identified when the call request was issued.

3.7.4.2.1.6.1.11.5 Then the calling DTE shall duplicate the compressor history window currently used for deflate compression over the last virtual circuit established in the context of the subnetwork connection group and register this copy as the initial compressor history window to be used for deflate compression over the virtual circuit being established.

3.7.4.2.1.6.1.11.6 Then the compressor history window that has been associated with the newly established virtual circuit shall be resynchronized with the decompressor history window of the remote DTE, by setting the compressor history window upper edge to the value of the remote decompressor window upper edge that is indicated by the value of the deflate maintenance parameter.

3.7.4.2.1.6.1.11.7 If, as a consequence of the above procedure, the lower edge of the compressor history window becomes greater than the new upper edge, then the lower edge shall be aligned with the new upper edge.

Note.— This may occur when the octet of history data pointed by the upper edge of the remote decompressor history window is outside the local compressor window. As a result of this procedure, the local compressor window is reset to a void state, and maintenance of the history window has failed. However, the lower and upper edges of the local compressor window are resynchronized with the upper edge of the remote decompressor window, and this will allow to re-attempt the maintenance of the deflate compression when a next virtual circuit is created in the context of this subnetwork connection group.

3.7.4.2.1.6.1.11.8 If a dictionary selection parameter is present in the SNDCF parameter extension block, the following cases are error conditions:

a) the preceding call request did not convey any dictionaries list parameter;

b) bit 6 (i.e. deflate option) of the first octet of the call confirm user data is not set;

c) a deflate maintenance parameter is also present in the SNDCF parameter extension block;

d) more than one dictionary selection parameter is present in the SNDCF parameter extension block;

e) the dictionary tag conveyed in the dictionary selection parameter does not identify the same version or an older version of one of the data stream compression dictionaries that have been proposed in the dictionaries list parameter conveyed in the preceding call request;

and shall be handled by clearing the call with an ISO/IEC 8208 cause code of zero, and a diagnostic code of 242 (Disconnection – incompatible information in user data).

3.7.4.2.1.6.1.11.9 If a dictionary selection parameter is present in the SNDCF parameter extension block and if none of the above error conditions is encountered, then the compressor and decompressor history windows of the newly established virtual circuit shall be initialized with the content of the dictionary that is identified by the dictionary selection parameter.

3.7.4.2.1.6.2 Fast select facility not in use

When an ISO/IEC 8208 call confirm packet is received from the called DTE and the fast select facility is not in use, then the calling DTE shall assume that all of the offered compression procedures have been accepted.

3.7.4.2.1.7 *Call rejection by the DCE or Called DTE*

3.7.4.2.1.7.1 General

3.7.4.2.1.7.1.1 When a DTE originated ISO/IEC 8208 call clearing packet is received with a diagnostic value indicating that the proposed LREF directory is too big (see Table 3-15), then the call should be re-attempted with the minimum directory size (see 3.7.4.3.1.3).

Note.— This is to ensure that the call is not rejected again due to the requested directory size being too big.

3.7.4.2.1.7.1.2 If the diagnostic indicates call collision resolution then no further attempt shall be made to re-establish the call.

3.7.4.2.1.7.1.3 When a DTE originated ISO/IEC 8208 call clearing packet is received with a diagnostic value indicating “Version number not supported” (see Table 3-15), then the call shall be re-attempted with a version number in the SNDCF parameter block of the call request user data (see 3.7.4.2.1.5.4.1) which is one less than previously used.

Note.— This failure condition may occur if the calling ATN router supports a later edition of this specification than the called ATN router.

3.7.4.2.1.7.2 Fast select facility requested

When a DCE or DTE originated ISO/IEC 8208 call clearing packet is received with a diagnostic indicating fast select not subscribed or fast select acceptance not subscribed, then the call shall be re-attempted but without requesting the fast select facility.

Note.— Some network service providers may indicate the non-availability of the fast select facility via other diagnostic codes.

3.7.4.2.1.7.3 Fast select facility not in use

Note.— In this case, when rejection by the called DTE indicates that the reject reason is due to an offered compression procedure not being supported, then the call is re-attempted without offering the rejected procedure. This is the only negotiation procedure possible when fast select is not available.

3.7.4.2.1.7.3.1 When a DTE originated ISO/IEC 8208 call clearing packet is received with a diagnostic indicating *LREF compression not supported* (see Table 3-15), the call shall be re-attempted without offering LREF compression.

3.7.4.2.1.7.3.2 When a DTE originated ISO/IEC 8208 call clearing packet is received with a diagnostic indicating *Local reference cancellation not supported* (see Table 3-15), the call shall be re-attempted without offering local reference cancellation.

Table 3-15. Diagnostic values for ATN call clearing

	Binary value	*Decimal value*	*Diagnostic code*
1	1111 1001	249	Connection rejection – unrecognized protocol identifier in user data
2	1000 0000	128	Version number not supported
3	1000 0001	129	Length field invalid
4	1000 0010	130	Call collision resolution
5	1000 0011	131	Proposed directory size too large
6	1000 0100	132	Local reference cancellation not supported
7	1000 0101	133	Received DTE refused, received NET refused or invalid NET selector
8	1000 0110	134	Invalid SNCR field
9	1000 0111	135	ACA compression not supported *Note.— Although the ACA is no longer supported by this specification, this diagnostic code is retained for backwards compatibility reasons. It is used to reject incoming calls from implementations compliant with previous versions of this specification, if they offer ACA without supporting the fast select facility.*
10	1000 1000	136	LREF compression not supported
11	1000 1111	143	Deflate compression not supported
12	1111 0000	240	System lack of resources
13	0000 0000	0	Cleared by system management
14	1001 0000	144	Idle timer expiration
15	1001 0001	145	Need to re-use the circuit
16	1001 0010	146	By local means (to be used for system local error)
17	1001 0011	147	Invalid SEL field value in received NET

3.7.4.2.1.7.3.3 When a DTE originated ISO/IEC 8208 call clearing packet is received with a diagnostic indicating *Deflate compression not supported* (see Table 3-15), the call shall be re-attempted without offering deflate compression.

3.7.4.2.2 Called DTE procedures

3.7.4.2.2.1 *Incoming call processing*

3.7.4.2.2.1.1 When an ISO/IEC 8208 incoming call packet is received, the called SNDCF first shall check for a call collision.

3.7.4.2.2.1.2 If the SNDCF has an outstanding call request to the same DTE address, specified as the calling DTE in this incoming call packet, and the call priority and SNCR are identical, then a call collision has occurred, and the call collision resolution procedures specified in ISO/IEC 8473-3 shall be invoked to resolve the call collision.

3.7.4.2.2.1.3 The called SNDCF shall then determine whether to accept the call.

3.7.4.2.2.1.4 The call shall be rejected if any of the following conditions are true:

a) the proposed ISO/IEC 8208 facility is not available;

b) the proposed priority is not supported;

c) the fast select facility was not selected in the incoming call packet and an offered compression algorithm is not supported;

d) the format of the call user data is invalid;

e) the version number is not supported;

f) the local reference compression is offered and the called SNDCF does not support the proposed directory size;

g) local policy does not permit communication with the calling DTE.

3.7.4.2.2.1.5 The call shall then be rejected using a call clearing packet, with the appropriate diagnostic code, as listed in Table 3-15.

3.7.4.2.2.1.6 If the call is to be accepted then the called SNDCF shall perform the ISO/IEC 8208 procedures associated with accepting a call.

3.7.4.2.2.2 *Call acceptance with the fast select facility in use*

3.7.4.2.2.2.1 The combination of compression techniques acceptable to the SNDCF, out of those offered by the calling SNDCF, shall be indicated by setting the appropriate bits in the first octet of the ISO/IEC 8208 call accept user data as shown in Figure 3-12.

3.7.4.2.2.2.2 If the M/I bit is set to one in the call request user data and,

a) there is one and only one existing subnetwork connection group with the calling DTE with the same data compression mechanisms and the same optional features of LREF compression as indicated in the call request user data, and the requested priority; and

b) it is acceptable to share the local reference directory associated with this subnetwork connection group with this virtual circuit;

then the virtual circuit shall be inserted in this subnetwork connection group and the M/I bit set to one in the call accept user data.

3.7.4.2.2.2.3 Otherwise, and if the virtual circuit is not inserted in a subnetwork connection group as a result of the procedure for the maintenance of the deflate history windows (see 3.7.4.2.2.2.8.3), a new subnetwork connection group shall be created, with this virtual circuit as the first member of the group and the M/I bit set to zero in the call accept user data.

Note.— By setting the M/I bit to zero, the responding SNDCF can refuse to maintain the local reference directory from the old virtual circuit to the new virtual circuit. This will result in an additional subnetwork connection group and, as long as one or more exists, in all further local reference directory maintenance requests to be rejected.

3.7.4.2.2.2.4 If there is additional user data beyond the SNDCF parameter block or the SNDCF parameter extension block respectively (see Figure 3-11) in the received incoming call packet and the first octet of this additional user data is a recognized NPDU SPI, then the remaining part of the received incoming call user data contains an NPDU, and the called SNDCF shall pass this NPDU in an SN-UNITDATA indication to the appropriate SN-service user.

3.7.4.2.2.2.5 The first octet of this NPDU (i.e. the SPI) shall be used by the called SNDCF in order to identify the network layer protocol and hence which SN-service user is responsible for handling this NPDU.

3.7.4.2.2.2.6 If no such SN-service user exists or the first octet of the additional user data does not contain a recognized NPDU SPI, then the additional user data shall be discarded.

3.7.4.2.2.2.7 If an SNDCF parameter extension block (see Figure 3-11) is present in the received incoming call packet, then it shall be processed by the called SNDCF as specified in 3.7.4.2.2.2.8.

3.7.4.2.2.2.8 Processing of received SNDCF parameter extension block

3.7.4.2.2.2.8.1 The called DTE shall ignore any unknown optional parameters conveyed in the SNDCF parameter extension block.

Note.— When rival compression options have been offered in the SNDCF parameter extension block, then the selection of one offered option over another is a local matter of the called DTE.

3.7.4.2.2.2.8.2 The order of preference of compression options should be configurable.

3.7.4.2.2.2.8.3 Processing of received deflate maintenance parameter

3.7.4.2.2.2.8.3.1 If a deflate maintenance parameter is present in the received SNDCF parameter extension block, then the deflate maintenance parameter shall be ignored if one or more of the following conditions are true:

a) the maintenance of the deflate history windows is not supported;

b) bit 6 (i.e. deflate option) of the fourth octet of the SNDCF parameter block is not set;

c) the values of bit 2 (LREF option) and bit 5 (M/I option) of the fourth octet of the SNDCF parameter block are not equal;

d) more than one deflate maintenance parameter is present in the SNDCF parameter extension block;

e) a dictionaries list parameter is also present in the SNDCF parameter extension block, and at least one of the proposed dictionaries is supported, and the use of pre-stored dictionaries is supported and prefered to the maintenance of the deflate history windows option;

f) no subnetwork connection group exists with the calling DTE at the requested priority and with the same data compression mechanisms and the same optional features of LREF compression as indicated in the fourth octet of the received SNDCF parameter block;

g) more than one of such subnetwork connection groups exist;

h) the value of the upper edge of the remote decompressor window indicated by the deflate maintenance parameter is higher than the upper edge of the local compressor window associated to the active virtual circuit in the subnetwork connection group;

i) the M/I bit is set to one in the call request user data, and it is not acceptable for the called DTE to share the local reference directory associated with this subnetwork connection group with the new virtual circuit to be established.

3.7.4.2.2.2.8.3.2 If a deflate maintenance parameter is present in the SNDCF parameter extension block and none of the above conditions is true, then the newly established virtual circuit shall be inserted into the subnetwork connection group.

3.7.4.2.2.2.8.3.3 Then, the called DTE shall duplicate the compressor and decompressor history windows currently used for deflate compression over the previous virtual circuit established in the context of the subnetwork connection group, and register this copy as the initial compressor and decompressor history windows to be used for deflate compression over the new virtual circuit.

Note.— A physically separate copy is required because the content of the history windows of the former virtual circuit in that subnetwork connection group may evolve while the new virtual circuit is being established.

3.7.4.2.2.2.8.3.4 The compressor history window that has been associated with the new virtual circuit shall be resynchronized with the decompressor history window of the remote DTE, by setting the local compressor history window upper edge to the value of the remote decompressor window upper edge that is indicated by the value of the deflate maintenance parameter.

3.7.4.2.2.2.8.3.5 If, as a consequence of the above procedure, the lower edge of the local compressor history window becomes greater than the new upper edge, then the lower edge shall be aligned with the new upper edge.

Note.— This may occur when the octet of history data pointed by the upper edge of the remote decompressor history window is ouside the local compressor window. As a result of this procedure, the local compressor window is reset to a void state, and maintenance of the history window has failed. However, the lower and upper edge of the local compressor window is resynchronized with the upper edge of the remote decompressor window, and this will allow to re-attempt the maintenance of the deflate compression when a next virtual circuit is created in the context of this subnetwork connection group.

3.7.4.2.2.2.8.3.6 The called DTE shall then insert a deflate maintenance parameter in the SNDCF parameter extension block of the call accept user data.

3.7.4.2.2.2.8.3.7 The deflate maintenance parameter shall be encoded as defined in ⁋3.7.4.2.1.5.9.

3.7.4.2.2.2.8.3.8 The parameter value field of the deflate maintenance parameter shall be set to the absolute value of the upper edge of the local decompressor history window being maintained over this subnetwork connection group.

Note.— The absolute value of the upper edge of the decompressor history window is defined in ⁋3.7.4.5.9.3.

3.7.4.2.2.2.8.3.9 No more than one deflate maintenance parameter shall be inserted in the SNDCF parameter extension block of the call accept user data.

3.7.4.2.2.2.8.4 Processing of a dictionaries list parameter

3.7.4.2.2.2.8.4.1 If a dictionaries list parameter is present in the received SNDCF parameter extension block, then the dictionaries list parameter shall be ignored if one or more of the following conditions are true:

a) the use of pre-stored deflate compression dictionaries is not supported;

b) bit 6 (i.e. deflate option) of the fourth octet of the SNDCF parameter block is not set;

c) more than one dictionaries list parameter is present in the SNDCF parameter extension block;

d) a deflate maintenance parameter is also present in the SNDCF parameter extension block, and the maintenance of the deflate history windows option is supported and prefered over the use of pre-stored dictionaries;

e) none of the data stream compression dictionaries proposed in the value field of the dictionaries list parameter, either at the proposed version or any earlier version, is supported.

3.7.4.2.2.2.8.4.2 If a dictionaries list parameter is present in the SNDCF parameter extension block and none of the above conditions is true, then the called DTE shall select one of the proposed dictionaries at the highest mutually supported version and initialize the compressor and decompressor history windows of the newly established virtual circuit with the content of that dictionary.

3.7.4.2.2.2.8.4.3 The called DTE shall then insert a dictionary selection parameter in the SNDCF parameter extension block of the call accept user data.

3.7.4.2.2.2.8.4.4 The dictionary selection parameter shall be encoded as defined in 3.7.4.2.2.4.7.

3.7.4.2.2.2.8.4.5 The parameter value field of the deflate selection parameter shall be set to the value of the dictionary tag corresponding to the dictionary that has been selected.

3.7.4.2.2.3 *Call acceptance without the fast select facility in use*

If fast select is not in use then a call shall only be accepted if all offered compression procedures and facilities are acceptable, and the proposed LREF directory size can be supported.

Note.— Call rejection is specified above in 3.7.4.2.2.1.4.

3.7.4.2.2.4 *Call accept user data*

Note.— User data can only be present in the call accept packet if the fast select facility is available and has been selected in the call request.

3.7.4.2.2.4.1 When fast select is available and has been selected in the call request, then a call accept user data shall be present in the call accept packet.

3.7.4.2.2.4.2 The call accept user data format shall be as illustrated in Figure 3-12.

3.7.4.2.2.4.3 The first octet of the call accept user data shall identify the compression procedure(s) accepted by the called DTE and shall signal the presence of an SNDCF parameter extension block, if any, in the call accept user data.

Note.— With the exception of the most significant bit (i.e. PEXT bit) and the adjacent spare bit, the bit fields of this octet have the same semantics as the ones used for the fourth octet of the SNDCF parameter block of the received call request user data (see Table 3-13).

3.7.4.2.2.4.4 The most significant bit (i.e. PEXT bit) of the first octet of the call accept user data shall be set to one if the call accept user data contains an SNDCF parameter extension block (see Figure 3-12) and if the value of the first octet of the SNDCF parameter block (i.e. version number) of the received call request user data is greater than 1.

Note.— The second condition above ensures backwards compatibility with ATN implementations which have signalled in the received call request packet to support Version 1 of the SNDCF protocol.

3.7.4.2.2.4.5 SNDCF parameter extension block

Note.— The optional SNDCF parameter extension block is used to convey to the calling SNDCF parameters related to the compression techniques which have been accepted by the called SNDCF.

3.7.4.2.2.4.5.1 If present, the SNDCF parameter extension block shall start at the second octet of the call accept user data.

3.7.4.2.2.4.5.2 The first octet of the SNDCF parameter extension block is the length indicator of this block, and its value shall indicate the number of octets of the SNDCF parameter extension block (including the length indicator field) as an unsigned binary number.

3.7.4.2.2.4.5.3 Each parameter contained within the SNDCF parameter extension block shall be structured as illustrated in Figure 3-11 and as specified in 3.7.4.2.1.5.4.17 through 3.7.4.2.1.5.4.19.

3.7.4.2.2.4.6 In case that the call accept packet will be used to convey an NPDU, the octet following the SNDCF parameter extension block, if such a block is present, or the second octet of the call accept user data respectively, if such a block is not present, shall be the first octet of this NPDU.

Note 1.— An ISO/IEC 9542 ISH PDU may be conveyed as part of the routing initiation procedure.

Note 2.— Since the negotiated compression procedures apply to the data transfer phase (see 3.7.4.2.3.1), the optional NPDU in the call accept user data, if present, is sent uncompressed.

3.7.4.2.2.4.7 Encoding of the dictionary selection parameter

3.7.4.2.2.4.7.1 The dictionary selection parameter shall be structured as illustrated in Figure 3-11.

3.7.4.2.2.4.7.2 The parameter code of the dictionary selection parameter shall be set to [0000 0011].

3.7.4.2.2.4.7.3 The parameter length field of the dictionary selection parameter shall be set to 2.

3.7.4.2.2.4.7.4 The parameter value field of the dictionaries selection parameter shall consist of one and only one dictionary tag as defined in 3.7.4.2.1.5.8.7, identifying the data stream compression dictionary selected by the called DTE.

3.7.4.2.3 Data transfer phase

3.7.4.2.3.1 During the data transfer phase of a virtual circuit established by this SNDCF, the compression procedures accepted by the called DTE shall be applied to each NPDU transferred over the virtual circuit.

Note.— NPDUs are queued for transfer as a result of an SN-UNITDATA.request. Received NPDUs are passed to the SN-service user by an SN-UNITDATA.indication.

3.7.4.2.3.2 The order in which concurrently applied compression procedures and ISO/IEC 8208 segmentation are applied shall be as follows:

a) if the LREF compression algorithm is used, it shall be applied to the ISO/IEC 8473 PDU first;

b) if the deflate compression algorithm is used, it shall be applied after LREF compression and before M-bit segmentation;

c) finally, if the ISO/IEC 8208 M-bit sequencing procedures are required due to the size of the PDU, then these shall be applied.

3.7.4.2.3.3 This sequence shall be inverted on the receiving end as follows:

a) if M-bit segmentation has been applied, then reassembly of the NPDU from the received ISO/IEC 8208 data packets shall be done first;

b) if the deflate compression algorithm is used the corresponding decompression algorithm shall be applied after M-bit segmentation and before LREF compression;

c) finally if the LREF compression is used, the LREF decompression algorithm shall then be applied.

3.7.4.2.4 Call clearing

3.7.4.2.4.1 The SNDCF shall clear a virtual circuit:

a) when system management requests call clearing; or

b) on the expiration of a timeout period following the transmission or receipt of SN-UNITDATA; or

c) if the resources are required by another virtual circuit with a higher priority.

3.7.4.2.4.2 Items b) or c) above shall only apply to those virtual circuits that have been established following an SN-UNITDATA.request.

3.7.4.2.4.3 When it has been determined that a virtual circuit is to be cleared, the SNDCF shall invoke the ISO/IEC 8208 functions associated with call clearing.

3.7.4.2.4.4 All packets subsequently received other than a clear confirm or a clear indication shall be ignored.

3.7.4.2.4.5 The same actions shall apply to the receipt of a clear indication.

3.7.4.2.4.6 The clearing cause octet in the ISO/IEC-8208 cause/diagnostic field shall be set to [1000 0000].

3.7.4.2.4.7 The reason for clearing the call shall be placed in the diagnostic field using the appropriate diagnostic values according to Table 3-15.

Note.— If a virtual connection is cleared due to a network problem, the SNDCF may attempt to re-establish the connection before the associated forwarding information is removed from network layer routing tables. The selective re-establishment of X.25 connections may be based on the originating clearing cause and diagnostic codes.

3.7.4.3 Local reference compression procedures

3.7.4.3.1 Local directory initialization

3.7.4.3.1.1 Both calling and called SNDCFs shall create a local directory to be associated with each newly established subnetwork connection group.

3.7.4.3.1.2 This directory shall consist of entries numbered from zero to a maximum of 32 767, each entry consisting of:

a) a pair of NSAP addresses, known as the inward and outward NSAP addresses respectively;

b) the ISO/IEC 8473 protocol version number;

c) the value of the security options parameter which may be empty.

3.7.4.3.1.3 The directory shall be initially empty. The mobile SNDCF shall support a minimum directory size of 128 entries.

3.7.4.3.2 Action following an SN-UNITDATA request

3.7.4.3.2.1 *General*

3.7.4.3.2.1.1 On receipt of a SN-UNITDATA request the SNDCF shall identify an appropriate virtual circuit to the subnetwork user associated with the SN-destination-address, and which satisfies the PDU priority and security requirements, and queue the accompanying PDU (i.e. the user data associated with the SN-UNITDATA request) for transfer over that virtual circuit.

3.7.4.3.2.1.2 If there is no virtual circuit which satisfies the PDU priority and security requirement, then the SNDCF shall try to establish a virtual circuit with the requested PDU security and priority.

3.7.4.3.2.1.3 If a suitable virtual circuit can be established, then the PDU shall be queued for transfer over the newly established virtual circuit. If no such virtual circuit can be established, then if an existing virtual circuit associated with the SN-destination-address provides an adequate level of security and priority, the PDU shall be queued for transfer over the existing virtual circuit.

3.7.4.3.2.1.4 Otherwise, the PDU shall be discarded.

Note 1.— The opening of an additional virtual circuit for this purpose may be inappropriate in certain cases. For example, opening an additional virtual circuit via a single frequency VDL subnetwork or via the Mode S subnetwork will not necessarily result in increased capacity.

Note 2.— The maintenance of the minimum QoS level includes ensuring that the number of local references that are required to support the number of data streams multiplexed over a given virtual circuit does not exceed the number available.

3.7.4.3.2.1.5 If no virtual circuit exists to the SN-destination-address, and the circuit is not classified as dynamically assigned by the ISO/IEC 10589 (IS-IS) routing protocol or under a static routing regime, then the SN-UNITDATA shall be discarded, with an error report sent to a system manager.

Note.— Virtual circuits between intermediate systems and between intermediate systems and end systems are initially established by procedures associated with the specific routing procedures employed. If no such virtual circuit has been established, or may be established under the routing procedures, then no route exists and hence it is an error if an attempt is made to send a PDU over such a route.

3.7.4.3.2.2 *Identification of network layer protocol*

3.7.4.3.2.2.1 Prior to transmission of an SN-UNITDATA SN-userdata parameter over a virtual circuit, the SNDCF shall inspect the initial octet of the SN-userdata parameter (initial protocol identifier (IPI)) to identify the network layer protocol contained within the SN-UNITDATA request.

3.7.4.3.2.2.2 If the IPI contains binary [1000 0001] indicating ISO/IEC 8473, then the procedures in 3.7.4.3.2.3 shall be performed.

3.7.4.3.2.2.3 If the IPI contains binary [1000 0010] indicating ISO/IEC 9542 (ES-IS), binary [1000 0011] indicating ISO/IEC 10589 (IS-IS), or binary [0100 0101] indicating ISO/IEC 11577 (NLSP), then the packet shall be sent unchanged over the virtual circuit, using the M-bit segmentation mechanism, if the packet is larger than the maximum length of user data permitted for the virtual circuit.

3.7.4.3.2.2.4 If the IPI contains any other value, the SN-UNITDATA request shall be discarded, and an error sent to a system manager.

Note.— The IPI designating the ISO/IEC 11577 has been included in the set of allowed IPIs in order to preserve the possiblity for use of this protocol in the future. However, at the time of publication of this specification, no ATN security protocol architecture has been defined. Thus, this inclusion of the NLSP IPI in the allowed IPI set does not indicate that NLSP will be incorporated into the future ATN security architecture.

3.7.4.3.2.3 *Identification of option parameter and local directory look-up*

3.7.4.3.2.3.1 The ISO/IEC 8473 NPDU header contained in the SN-userdata shall then be inspected. If one of the following is true:

a) the ISO/IEC 8473 NPDU is an echo request (ERQ) or echo response (ERP) NPDU;

b) parameters other than the security, priority or QoS maintenance parameters are present in the options part of the NPDU header;

c) the QoS maintenance parameter is anything other than the globally unique format;

d) the priority option is present with a value greater than 14;

then the SN-userdata shall be sent unchanged over the virtual circuit using M-bit segmentation procedures as appropriate.

3.7.4.3.2.3.2 Otherwise, the local directory associated with the virtual circuit shall then be interrogated to determine if an entry exists such that:

a) the inward NSAP address is equal to the PDU's source NSAP address;

b) the outward NSAP address is equal to the PDU's destination NSAP address;

c) a security parameter is present with the same value as that contained in the PDU header, if present, and otherwise absent;

d) the same ISO/IEC 8473 version number as is present in the PDU header.

3.7.4.3.2.3.3 If an entry is found, then the NPDU shall be sent in the compressed form constructed according to 3.7.4.3.3, using the local directory entry number as the local reference.

3.7.4.3.2.3.4 If no entry is found, then a new directory entry shall be created and the SN-userdata shall be modified as specified in 3.7.4.3.2.4.

3.7.4.3.2.4 *Establishing a new local reference*

3.7.4.3.2.4.1 A new directory entry shall be created containing the NPDU source NSAP address as the inward NSAP address, and the NPDU destination NSAP address as the outward NSAP address.

3.7.4.3.2.4.2 The value of the protocol version number, and the security parameter, if present, shall also be placed in this entry.

3.7.4.3.2.4.3 The entry number shall have the lowest possible entry number that has not previously been used for the local directory associated with this virtual circuit, and shall be in the range [0..63] or [128..16 447] if the SNDCF is the initiator of the first virtual circuit in a subnetwork connection group, or [64..127] or [16 448..32 767], if the SNDCF is the responder for such a virtual circuit.

3.7.4.3.2.4.4 When a directory size greater than 128 but less than 32 767 has been negotiated, then the highest local reference that the initiator may allocate shall be:

127 + (n -128) / 2

and the highest local reference that the responder may allocate shall be:

16 447 + (n -128) / 2

where "n" is the agreed maximum directory size.

3.7.4.3.2.4.5 If a directory full condition occurs then, as a local matter, either the PDU shall be sent unmodified over the virtual circuit or the virtual circuit shall be reset.

Note.— A user generated network reset results in the total clearing of the directory which then permits the assignment of an unused local reference.

3.7.4.3.2.4.6 When this SNDCF is used for air-ground communication or when the local reference cancellation option is available for use, then the PDU should be sent unmodified over the virtual circuit.

3.7.4.3.2.4.7 The PDU, which may be either a DT PDU or an ER PDU, shall have an additional options field added to the PDU header.

3.7.4.3.2.4.8 This option parameter shall have local significance only (i.e. is only of interest to the sending and receiving SNDCFs), and is called the local reference.

3.7.4.3.2.4.9 This local reference option parameter shall be included as the first parameter in the option part of the DT or ER PDU header.

3.7.4.3.2.4.10 This option shall be specified as follows:

Parameter code:	[0000 0101]
Parameter length:	variable
Parameter value:	the entry number of the local directory entry created above and expressed as an unsigned integer.

Note 1.— The entry number is therefore assigned as a so-called local reference.

Note 2.— The unsigned integer is encoded most significant byte first, in compliance with ISO/IEC 8473-1.

3.7.4.3.2.4.11 The checksum, length indicator, and segment length fields of the PDU header shall be modified to reflect the insertion of the new options field and any changes to the length of the source and destination address.

3.7.4.3.2.4.12 The total length, if present, shall be left unmodified.

3.7.4.3.2.5 *Reference cancellation option*

3.7.4.3.2.5.1 When the optional local reference cancellation facility is implemented, and both SNDCFs using a virtual circuit have indicated that they support this facility, then the SNDCF shall monitor the number of local references on each virtual circuit which it has both assigned and are in use.

3.7.4.3.2.5.2 When the number of such local references on a given virtual circuit exceeds a system manager specified threshold, then the local reference cancellation procedures specified in ⁋3.7.4.3.6 shall be invoked, in order to ensure that the number of unused local references in the range in which the SNDCF is permitted to assign local references, is at least equal to a system manager specified target.

3.7.4.3.2.6 *Transfer of the modified ISO/IEC 8473 PDU*

The modified ISO/IEC 8473 NPDU (i.e. the NPDU with the added local reference option) shall be inserted in the user data field of an ISO/IEC 8208 data packet and shall be sent over the virtual circuit, using the ISO/IEC 8208 M-bit segmentation procedure, if appropriate.

3.7.4.3.3 Compression of SN-Userdata

3.7.4.3.3.1 *General*

3.7.4.3.3.1.1 An initial DT NPDU shall be compressed according to the procedures specified in ⁋3.7.4.3.3.2.

3.7.4.3.3.1.2 A derived DT NPDU shall be compressed according to the procedures specified in ⁋3.7.4.3.3.3.

3.7.4.3.3.1.3 An ER NPDU shall be compressed according to the procedures specified in ⁋3.7.4.3.3.3.17.

3.7.4.3.3.2 *Initial DT PDU compression*

3.7.4.3.3.2.1 General

Note.— An initial DT PDU is an ISO/IEC 8473 DT PDU that either contains no segmentation part in its PDU header or contains a segmentation part with a segment offset value that equals zero and the segment length is equal to the total length.

3.7.4.3.3.2.1.1 The original initial DT PDU shall be compressed into the compressed initial data PDU as shown in Figure 3-13.

3.7.4.3.3.2.1.2 The fields of the compressed initial data PDU shall be set as follows.

3.7.4.3.3.2.2 Type field

The PDU type field value shall be set according to the values of the original Initial DT PDU ER, SP and more segments (MS) flags as defined in Table 3-16.

Table 3-16. Initial DT PDU type codes

PDU type values	*CLNP NPDU ER value*	*CLNP NPDU SP value*	*CLNP NPDU MS value*
0 0 0 0	0	0	0
0 0 0 1	0	1	0
0 0 1 0	1	0	0
0 0 1 1	1	1	0

3.7.4.3.3.2.3 PDU priority field

The PDU priority field value shall be set to the lowest four bits of the original PDU priority parameter value field, if the priority option is present, and set to zero otherwise.

3.7.4.3.3.2.4 PDU lifetime field

The PDU lifetime field value shall be set to the eight bits of the original NPDU lifetime field.

3.7.4.3.3.2.5 P bit field

The P field value shall be set to one if the original uncompressed PDU contained the priority option. This field shall be set to zero otherwise.

3.7.4.3.3.2.6 Q bit field

3.7.4.3.3.2.6.1 The Q field value shall be set to one if the original uncompressed PDU contained the QoS maintenance option.

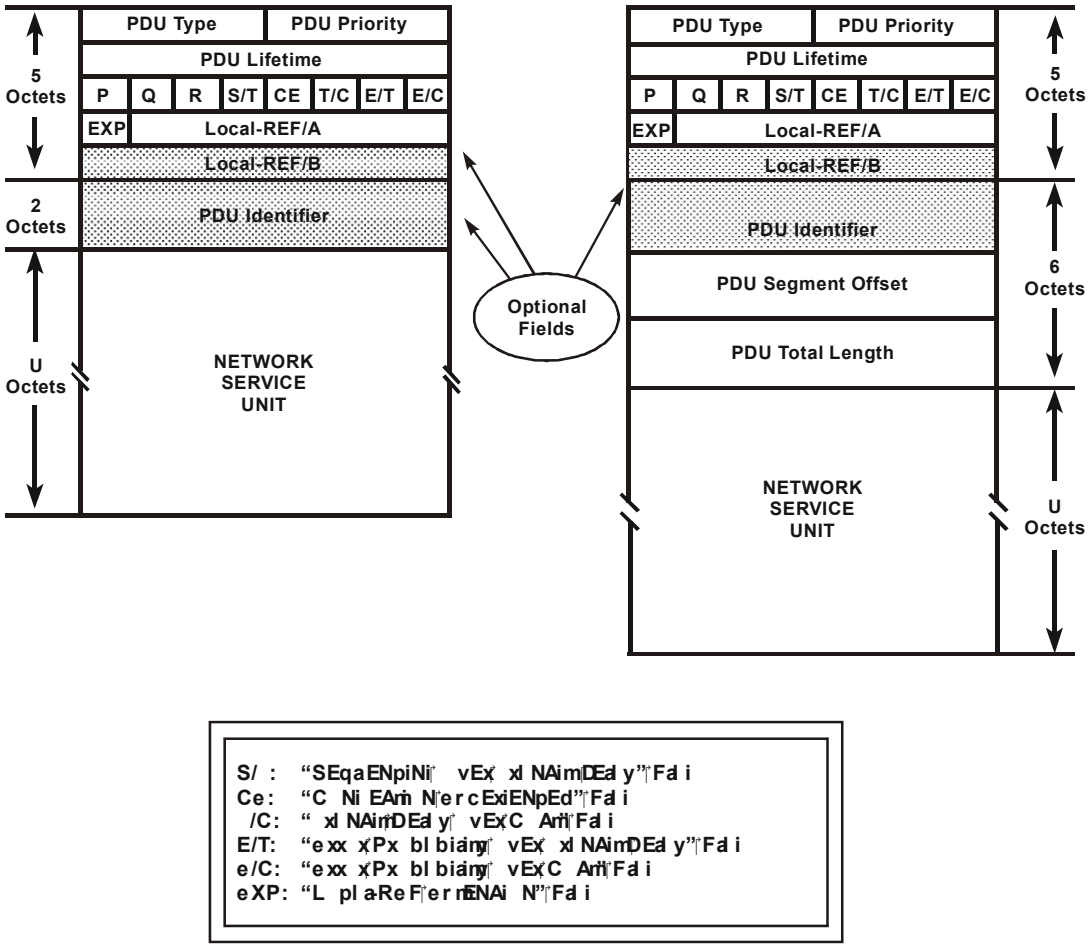


Figure 3-13. Compressed initial and derived formats

3.7.4.3.3.2.6.2 This field shall be set to zero otherwise.

3.7.4.3.3.2.7 R bit field

3.7.4.3.3.2.7.1 The R field value shall be set to one if the original uncompressed PDU contains a non-zero checksum.

3.7.4.3.3.2.7.2 This field shall be set to zero otherwise.

3.7.4.3.3.2.8 S/T, CE , T/C, E/T, and E/C fields

3.7.4.3.3.2.8.1 The values of these fields shall be set to bits 5 through 1 of the QoS parameter value option field of the original PDU, if the Quality of Service maintenance option is present.

3.7.4.3.3.2.8.2 The S/T field shall be set to the value of bit 5 of the Quality of Service maintenance parameter value field, if present (i.e. sequencing vs. transit delay) and set to zero otherwise.

3.7.4.3.3.2.8.3 The CE field shall be set to the value of bit 4 in the Quality of Service maintenance parameter value field.

3.7.4.3.3.2.8.4 The T/C field shall be set to the value of bit 3 in the Quality of Service maintenance parameter value field.

3.7.4.3.3.2.8.5 The E/T field shall be set to the value of bit 2 in the Quality of Service maintenance parameter value field.

3.7.4.3.3.2.8.6 The E/C field shall be set to the value of bit 1 in the Quality of Service maintenance parameter value field.

3.7.4.3.3.2.9 EXP, Local-REF/A and Local-REF/B fields

3.7.4.3.3.2.9.1 If the value of the local reference determined according to the procedure specified in 3.7.4.3.2.4 is less than 128, then the EXP field shall be set to zero.

3.7.4.3.3.2.9.2 In this case, only the Local-REF/A field shall be present in the PDU.

3.7.4.3.3.2.9.3 The Local-REF/A field value shall be set to the value of the local reference encoded as an unsigned integer.

3.7.4.3.3.2.9.4 If the value of the local reference is greater than or equal to 128, the EXP field shall be set to one, and both Local-REF/A and Local-REF/B fields shall be present in the PDU.

3.7.4.3.3.2.9.5 The local reference shall be encoded as a 15 bit unsigned integer, with the least significant eight bits placed in the Local-REF/B field, and the most significant seven bits placed in the Local-REF/A field.

3.7.4.3.3.2.10 PDU identifier

3.7.4.3.3.2.10.1 If the initial DT PDU allows segmentation (SP flag is set to one), then the PDU identifier field shall be included in the compressed initial data PDU.

3.7.4.3.3.2.10.2 The PDU identifier field shall contain the data unit identifier as provided in the segmentation part of the initial DT PDU.

3.7.4.3.3.2.10.3 If the initial DT PDU does not allow segmentation (SP flag is set to zero), then this field shall not be included in the compressed initial data PDU.

3.7.4.3.3.2.11 PDU segment offset

This field shall not be present in the compressed data PDU for an initial DT PDU.

Note.— The segment offset of an initial DT PDU is always zero and is a priori known by the receiving SNDCF.

3.7.4.3.3.2.12 PDU total length

This field shall not be present in the compressed data PDU for an initial DT PDU.

Note.— The total length field value of an initial DT PDU is the length of the entire PDU in octets. This value is identical to the value of the segment length field for an initial DT PDU, and both values may be recalculated by the receiving SNDCF.

3.7.4.3.3.2.13 Network service data unit field

This field shall contain the data part of the original initial DT PDU.

3.7.4.3.3.3 *Derived DT PDU compression*

3.7.4.3.3.3.1 General

3.7.4.3.3.3.1.1 The original derived DT PDU shall be compressed into the compressed derived data PDU as shown in Figure 3-13.

3.7.4.3.3.3.1.2 The fields of the compressed derived data PDU shall be set as defined in the following sections.

3.7.4.3.3.3.2 Type field

3.7.4.3.3.3.2.1 The PDU type field value shall be set according to the values of the original NPDU ER, SP and MS flags as defined in Table 3-17.

Table 3-17. Derived PDU type codes

PDU type values	*CLNP NPDU ER value*	*CLNP NPDU SP value*	*CLNP NPDU MS value*
0 1 1 0	0	1	0
0 1 1 1	0	1	1
1 0 0 1	1	1	0
1 0 1 0	1	1	1

3.7.4.3.3.3.3 PDU priority field

This field shall be set as defined in 3.7.4.3.3.2.3.

3.7.4.3.3.3.4 PDU lifetime field

This field shall be set as defined in 3.7.4.3.3.2.4.

3.7.4.3.3.3.5 P bit field

This field shall be set as defined in 3.7.4.3.3.2.5.

3.7.4.3.3.3.6 Q bit field

This field shall be set as defined in 3.7.4.3.3.2.6.

3.7.4.3.3.3.7 S/T, CE , T/C, E/T, and E/C fields

These fields shall be set as defined in §3.7.4.3.3.2.8.

3.7.4.3.3.3.8 EXP, Local-REF/A and Local-REF/B fields

These fields shall be set as defined in §3.7.4.3.3.2.9.

3.7.4.3.3.3.9 PDU identifier field

The PDU identifier field value shall be set to the data unit identifier contained in the segmentation part of the original derived DT PDU header.

3.7.4.3.3.3.10 PDU segment offset field

The PDU segment offset field value shall be set to the segment offset value contained in the segmentation part of the original derived DT PDU header.

3.7.4.3.3.3.11 PDU total length field

The PDU total length field value shall be set to the value of the total length field contained in the segmentation part of the original derived DT PDU.

3.7.4.3.3.3.12 Error report PDU compression

3.7.4.3.3.3.12.1 General

3.7.4.3.3.3.12.1.1 The original ER PDU shall be compressed into the compressed error report PDU as shown in Figure §3-14.

3.7.4.3.3.3.12.1.2 The fields of the compressed error report PDU shall be set as defined in the following sections.

3.7.4.3.3.3.13 PDU type field

The PDU type field value shall be set to [1101].

3.7.4.3.3.3.14 PDU priority field

This field shall be set as defined in §3.7.4.3.3.2.3.

3.7.4.3.3.3.15 PDU lifetime field

This field shall be set as defined in §3.7.4.3.3.2.4.

3.7.4.3.3.3.16 P bit field

This field shall be as defined in §3.7.4.3.3.2.5.

3.7.4.3.3.3.17 Q bit field

This field shall be set as defined in §3.7.4.3.3.2.6.

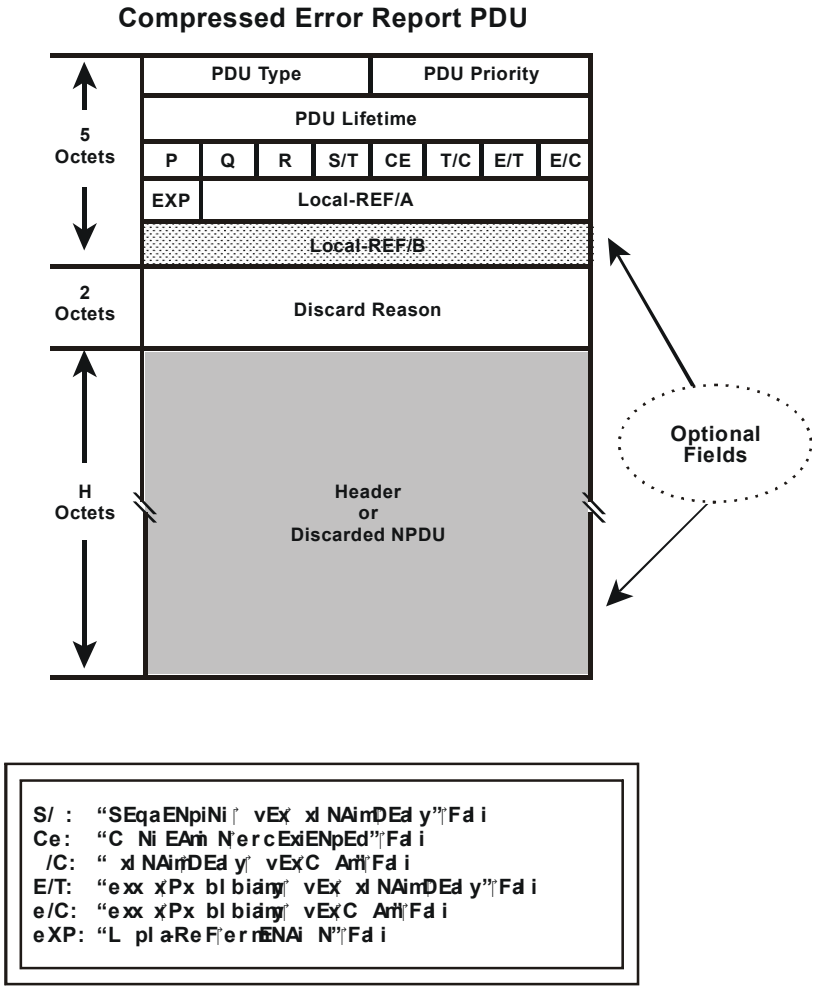


Figure 3-14. Compressed error report PDU

3.7.4.3.3.3.18 S/T, CE , T/C, E/T and E/C fields

These fields shall be set as defined in 3.7.4.3.3.2.8.

3.7.4.3.3.3.19 EXP, Local-REF/A, Local-REF/B fields

These fields shall be set as defined in 3.7.4.3.3.2.9.

3.7.4.3.3.3.20 Discard reason field

This field shall be set to the value of the reason for discard parameter value field contained in the original NPDU header.

3.7.4.3.3.3.21 Header of discarded NPDU field

This field shall contain the value of the error report data part if provided in the original error report PDU.

3.7.4.3.3.3.22 Transfer of compressed ISO/IEC 8473 PDUs

The compressed ISO/IEC 8473 NPDU (i.e. compressed initial data PDU, compressed derived data PDU, or compressed error report PDU) shall be inserted in the user data field of an ISO/IEC 8208 data packet and shall be sent over the virtual circuit, using the ISO/IEC 8208 M-bit segmentation procedure if appropriate.

3.7.4.3.4 Processing of packets received from the subnetwork service provider

Note.— The following sections specify the processing of packets received from the subnetwork service provider.

3.7.4.3.4.1 *Initial processing of NPDU*

3.7.4.3.4.1.1 On receipt of an incoming packet received from a virtual circuit, the SNDCF shall inspect the first octet to determine the network layer protocol ID or the compressed PDU type (see Table 3-18).

a) If this value is set to **[1000 0001]** indicating that the NPDU is an ISO/IEC 8473 NPDU with an uncompressed header, then the NPDU shall be processed according to 3.7.4.3.4.2.2.

b) If the first octet indicates either ISO/IEC 9542 (ES-IS), ISO/IEC 11577 (NLSP) or ISO/IEC 10589 (IS-IS), the SNDCF shall generate an SN-UNITDATA.indication with the NPDU as its SN-userdata parameter, and the SN-source-address and SN-destination-address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received.

c) If the value of the first four bits of the first octet is in the range binary **[0000]** to binary **[0011]** then the PDU is a compressed ISO/IEC 8473 initial DT PDU which shall be decompressed using the procedures specified in 3.7.4.3.4.3.

d) If the value of the first four bits of the first octet is in the range binary **[0110]** to binary **[1010]** (excluding 1000) then the PDU is a compressed ISO/IEC 8473 derived PDU, which shall be decompressed using the procedures specified in 3.7.4.3.4.3.

e) If the value of the first four bits of the first octet is binary **[1101]** then the PDU is a compressed ISO/IEC 8473 error PDU, which shall be decompressed using the procedures specified in 3.7.4.3.4.4.

f) If the value of the first four bits of the first octet is binary **[1110]** then the PDU is an SNDCF error report, which shall be processed according to the procedures of 3.7.4.3.4.5, and no SN-UNITDATA.indication generated.

g) If the value of the first four bits of the first octet is binary **[0100]** or binary **[0101],** then the PDU is respectively, a local reference cancellation request or response, which shall be processed according to the procedures of 3.7.4.3.6 and no SN-UNITDATA.indication generated.

3.7.4.3.4.1.2 In all other cases, the PDU shall be discarded and an SNDCF error report generated (see 3.7.4.3.5).

3.7.4.3.4.2 *Incoming ISO/IEC 8473 PDU with uncompressed header*

3.7.4.3.4.2.1 General

If the received NPDU is an ISO/IEC 8473 NPDU then the options part shall be inspected for the options field containing the local reference.

Table 3-18. Mapping between compressed PDU type fields and uncompressed PDU types

Compressed PDU type field	Uncompressed PDU type
[0000] - [0011]	Compressed initial DT PDU
[0110] - [0111] [1001] - [1010]	Compressed derived DT PDU
[1101]	Compressed error report PDU
[1110]	SNDCF error report
[0100]	Cancellation request PDU
[0101]	Cancellation accept PDU

3.7.4.3.4.2.2 Processing of unmodified ISO/IEC 8473 PDUs

If the local reference option is not present, then the SNDCF shall generate a SN-UNITDATA indication with the NPDU as its SN-userdata, and the SN-source-address and SN-destination-address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received.

3.7.4.3.4.2.3 Processing of modified ISO/IEC 8473 PDUs

3.7.4.3.4.2.3.1 If the local reference option is present, it shall be removed, and the checksum and PDU header length indication and segment length shall be modified to reflect this removal.

3.7.4.3.4.2.3.2 If a local reference options field is present, then the local directory associated with the virtual circuit over which the PDU was received shall be inspected for the presence of the corresponding entry.

3.7.4.3.4.2.3.3 If no such entry is present, and the value of the local reference is in the range within which the remote SNDCF is permitted to create local directory entries, then the entry shall be created, and:

a) the value of the inward NSAP address set to the PDU's destination NSAP address;

b) the value of the outward NSAP address set to the NSAP's source NSAP address; and

c) the values of the version number and security parameter, set to the corresponding values in the PDU header.

3.7.4.3.4.2.3.4 An SNDCF error report (see 3.7.4.3.5) shall be generated if the value of the local reference is not within the range within which the remote SNDCF is permitted to create local directory entries or is greater than the maximum negotiated when the call was established.

3.7.4.3.4.2.3.5 Otherwise, the local directory entry shall be compared with the received PDU. If:

a) the inward NSAP address does not match the destination NSAP address; or

b) the outward NSAP address does not match the source NSAP address; or

c) the version number does not match the version number present in the directory entry; or

d) the value of the security options parameter does not match the value in the directory, or is not correspondingly absent; then

an SNDCF error report shall be generated and returned over the same virtual circuit as the PDU was received.

3.7.4.3.4.2.3.6 The SNDCF shall then generate a SN-UNITDATA.indication with the NPDU as its SN-userdata, and the SN-source-address and SN-destination-address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received.

3.7.4.3.4.3 *Incoming compressed data PDU*

3.7.4.3.4.3.1 General

3.7.4.3.4.3.1.1 If the most significant four bits of the first octet of a received PDU (i.e. the PDU type field) are in the range [0000] to [0011] binary, excluding [1000], then the packet is a compressed ISO/IEC 8473 initial DT NPDU.

3.7.4.3.4.3.1.2 If the PDU type field of a received compressed PDU is in the range [0110] to [1010] binary, then the PDU is a compressed ISO/IEC 8473 derived DT NPDU.

3.7.4.3.4.3.1.3 Upon receipt, the SNDCF shall examine and validate the Local-REF in the compressed PDU.

3.7.4.3.4.3.1.4 The value of the local reference shall be extracted from the compressed header and the corresponding entry in the local directory located.

3.7.4.3.4.3.1.5 If no entry exists corresponding to the Local-REF present in the PDU, then an SNDCF error report shall be generated and returned over the same virtual circuit as the PDU was received, and the PDU shall be discarded.

3.7.4.3.4.3.1.6 If the Local-REF is valid, the original uncompressed NPDU shall be recreated by the procedures defined in 3.7.4.3.4.3.2 through 3.7.4.3.4.3.6.

3.7.4.3.4.3.1.7 The SNDCF then shall generate a SN-UNITDATA.indication with the SN-source address and SN-destination address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received, and the SN-userdata shall be set to the uncompressed DT NPDU.

3.7.4.3.4.3.2 Fixed part

Note 1.— The fixed part of the NPDU header consists of the network layer protocol identifier, length indicator, version/protocol identifier extension, PDU lifetime, SP flag, MS flag, E/R flag, type, segment length and checksum fields as defined in ISO/IEC 8473.

Note 2.— If the EXP field is set to zero, the local reference is the seven bit integer value of the Local-REF/A field. If the EXP field is set to one, the local reference value consists of the fifteen bit unsigned integer as stored with the least significant eight bits placed in the Local-REF/B field, and the most significant seven bits placed in the Local-REF/A field.

3.7.4.3.4.3.2.1 Network layer protocol identifier

This field shall be set to binary [1000 0001] to identify this network layer protocol as ISO/IEC 8473.

3.7.4.3.4.3.2.2 Length indicator

This field shall be set to the length of the uncompressed NPDU header in octets.

3.7.4.3.4.3.2.3 Version/protocol identifier extension

The version/protocol identifier extension field shall be set to the values provided in the corresponding entry of the local directory.

3.7.4.3.4.3.2.4 PDU lifetime

The eight bits of the PDU lifetime field shall be set to the eight bits of the PDU lifetime field of the compressed data PDU.

3.7.4.3.4.3.2.5 Segmentation permitted, more segments, error report flags

3.7.4.3.4.3.2.5.1 The values of these flags shall be derived from the value of the Protocol ID field and type field of the compressed data PDU.

3.7.4.3.4.3.2.5.2 These flag values shall be determined according to Table ⁋3-16 for an initial data PDU and Table ⁋3-17 for a derived data PDU.

3.7.4.3.4.3.2.6 Type code

This field shall be set to binary [11100] to indicate a DT PDU.

3.7.4.3.4.3.2.7 Segment length

3.7.4.3.4.3.2.7.1 This field shall indicate the entire length in octets of the PDU, including both header and data.

3.7.4.3.4.3.2.7.2 The value of this field shall be computed by the SNDCF.

3.7.4.3.4.3.2.7.3 For an initial DT NPDU, the value of this field shall be identical to the value of the total length field located in the segmentation part of the header.

3.7.4.3.4.3.2.8 PDU checksum

3.7.4.3.4.3.2.8.1 The value of this field shall be set to zero if the R bit in the compressed header is zero.

3.7.4.3.4.3.2.8.2 Otherwise, a checksum field shall be recomputed.

Note.— For the DT PDU, this includes the segmentation and options part (if present). For the error report PDU, this includes the reason for discard field as well.

3.7.4.3.4.3.3 Address part

Note.— The address part consists of the destination address length indicator, destination address, source address length indicator and source address as defined in ISO/IEC 8473.

3.7.4.3.4.3.3.1 Destination and source address length indicators and addresses

3.7.4.3.4.3.3.1.1 The source and destination NSAP addresses shall be set to the values provided in the corresponding entry of the local directory for the local reference number calculated.

3.7.4.3.4.3.3.1.2 The source NSAP address shall be set to the value of the outward NSAP address, and the destination NSAP address set to the value of the inward NSAP address.

3.7.4.3.4.3.3.1.3 The length fields shall contain the length of each address in octets.

3.7.4.3.4.3.4 Segmentation part

3.7.4.3.4.3.4.1 General

3.7.4.3.4.3.4.1.1 If the ISO/IEC 8473 SP field is set to one, then the segmentation part shall be generated.

3.7.4.3.4.3.4.1.2 The segmentation part shall consist of the data unit identifier, segment offset, and total length field as defined in ISO/IEC 8473.

3.7.4.3.4.3.4.2 Data unit identifier

This field shall contain the value of the PDU identifier field as provided in the compressed DT PDU.

3.7.4.3.4.3.4.3 Segment offset

3.7.4.3.4.3.4.3.1 For an initial DT PDU, this field shall be set to zero.

3.7.4.3.4.3.4.3.2 For a derived DT PDU, this field shall be set to the PDU segment offset field as provided in the compressed DT PDU.

3.7.4.3.4.3.4.4 PDU total length

3.7.4.3.4.3.4.4.1 For a derived DT PDU, this field shall contain the value of the PDU total length field as provided in the compressed DT PDU.

3.7.4.3.4.3.4.4.2 For an initial PDU, the entire length of the PDU in octets shall be calculated by the SNDCF and stored in this field.

3.7.4.3.4.3.5 Options part

3.7.4.3.4.3.5.1 General

3.7.4.3.4.3.5.1.1 If the Q bit field is set to one, the globally unique QoS option shall be recreated according to 3.7.4.3.4.3.5.3.

3.7.4.3.4.3.5.1.2 If the security option is present in the local reference directory entry, the security option shall be recreated according to 3.7.4.3.4.3.5.4.

3.7.4.3.4.3.5.1.3 If the P bit field is set to one, the priority option shall be recreated according to 3.7.4.3.4.3.5.2.

3.7.4.3.4.3.5.2 Priority

3.7.4.3.4.3.5.2.1 For the priority option, the parameter code shall be set to binary [1100 1101] and the parameter length set to one octet.

3.7.4.3.4.3.5.2.2 The four most significant bits of the parameter value shall be set to zero, and the four least significant bits set to the PDU priority field as provided in the compressed DT PDU.

3.7.4.3.4.3.5.3 Quality of Service maintenance

3.7.4.3.4.3.5.3.1 For the Quality of Service maintenance option, the parameter code shall be set to binary [1100 0011], the parameter length set to one octet.

3.7.4.3.4.3.5.3.2 The high order two bits of the parameter value shall be set to binary [11] to indicate globally unique, bit 6 shall be set to zero, and bits 5 through one set to the S/T, CE , T/C, E/T and E/C fields, respectively, as provided in the compressed data PDU.

3.7.4.3.4.3.5.4 Security

This field shall be set to the value of the security parameter contained in the corresponding local reference directory entry.

3.7.4.3.4.3.6 Data part

The data part shall be copied from the compressed data PDU data part.

3.7.4.3.4.4 Incoming compressed error report PDU

3.7.4.3.4.4.1 General

The original uncompressed header shall be recreated as defined in the following sections.

Note.— If the four most significant bits of the first octet (the PDU type field) of a received packet are [1101] then the packet is a compressed ISO/IEC 8473 ER NPDU.

3.7.4.3.4.4.2 Fixed part

The fixed part of the ER PDU shall be composed in the same manner as defined in 3.7.4.3.4.3.2 except for the type code which shall be set to binary [00001] to indicate an ER PDU, and for the SP and MS flags which shall be set to zeros.

3.7.4.3.4.4.3 Address part

The address part of the ER PDU shall be composed in the same manner as defined in 3.7.4.3.4.3.3.

3.7.4.3.4.4.4 Options part

The options part of the ER PDU shall be composed in the same manner as defined in 3.7.4.3.4.3.5 for an initial DT PDU.

3.7.4.3.4.4.5 Reason for discard

To compose this field, the parameter code shall be set to binary [1100 0001], the parameter length set to two octets, and the parameter value set to the discard reason field as provided in the compressed error report PDU.

3.7.4.3.4.4.6 Error report data part

If the compressed error report PDU contains the header of discarded NPDU field, then the error report data part shall be set to the value of the header of discarded NPDU field.

3.7.4.3.4.5 Incoming SNDCF error report

3.7.4.3.4.5.1 On receipt of an SNDCF error report with reason “compressed NPDU with unrecognized local reference”, the directory entry corresponding to the local reference returned in the SNDCF error report shall be reset to the unused state.

3.7.4.3.4.5.2 On receipt of an SNDCF error report with reason other than “compressed NPDU with unrecognized local reference” (see Table 3-19), the virtual circuit shall be reset (see 3.7.4.3.7) and the local reference directory associated with the virtual circuit shall be cleared to its initial state.

Note.— If the virtual circuit on which the error has been reported belongs to a connection group which shares the same LREF directory, there is no need to reset the remaining virtual circuits of that group.

3.7.4.3.4.5.3 The error should be notified to systems management.

Note.— If the four most significant bits of the first octet (the PDU type field) of an incoming packet are set to [1110], then a SNDCF error report has been received (see 3.7.4.3.5).

3.7.4.3.5 SNDCF error report

3.7.4.3.5.1 The SNDCF error report is a packet format unique to the Mobile SNDCF and shall be used to report errors in the use of local references as specified below.

3.7.4.3.5.2 The SNDCF error report PDU shall be constructed as follows:

a) the most significant four bits (PDU Type) of the first octet are set to binary 1110, while the least significant four bits are set to 0000.

b) the second octet is a discard reason encoded as an unsigned integer, with the following reason codes defined in the Table 3-19:

c) the local reference contained in the PDU for which the error is being reported is placed in the remaining octet(s) of the SNDCF error report PDU header, unless the reason is local reference cancellation error, when the SNDCF error report shall consist of three octets only, and the third octet shall contain the cancellation reference of the invalid cancellation request PDU.

3.7.4.3.5.3 The data portion of the SNDCF error report shall be used to return a copy of the PDU in error, similar to the ISO/IEC 8473 error report PDU.

3.7.4.3.5.4 The error report PDU shall be sent as an ISO/IEC 8208 DATA packet(s) and, if needed, segmented using the M-bit procedures.

3.7.4.3.6 Local reference cancellation option

3.7.4.3.6.1 *General*

Note.— When the implementation of this option has been agreed by both SNDCFs using a virtual circuit during the call setup procedures, then the following procedures may be used to selectively cancel one or more local references, i.e. make them available for re-use. An SNDCF may only request the cancellation of local references which are within the range in which it is permitted to assign local references.

Table 3-19. SNDCF error report diagnostic codes

Code	*Reason*
[0000 0000]	Compressed NPDU with unrecognized local reference
[0000 0001]	Creation of directory entry outside of sender's permitted range
[0000 0010]	Directory entry exists
[0000 0011]	Local reference greater than maximum value accepted
[0000 0100]	Data unit identifier missing when SP=1
[0000 0101]	Reserved
[0000 0111]	Compressed ISO/IEC 8473 PDU with unrecognized type
[0000 1000]	Local reference cancellation error

3.7.4.3.6.1.1 When an SNDCF invokes the procedures for local reference cancellation it shall format a cancellation request PDU, as specified below, and send the PDU to the other SNDCF over the virtual circuit to which it applies.

3.7.4.3.6.1.2 A cancellation request PDU shall be retransmitted periodically until it is acknowledged by a cancellation accept PDU, or an SNDCF error report PDU is received indicating an error in the request.

3.7.4.3.6.1.3 When a cancellation accept PDU is received, the corresponding directory entries shall be cleared, and the local references therefore become available for re-use.

3.7.4.3.6.1.4 When an SNDCF receives a cancellation request PDU, it shall first check to ensure that the local references identified in the PDU are within the range in which the sending SNDCF is permitted to assign local references.

3.7.4.3.6.1.5 If any one of them is not, then an SNDCF error report shall be returned, and the request ignored.

3.7.4.3.6.1.6 Otherwise, the directory entries corresponding to the indicated local references shall be cleared, and a cancellation accept PDU formatted and returned, in order to accept cancellation of these local references.

3.7.4.3.6.2 *The cancellation request PDU*

3.7.4.3.6.2.1 The PDU format shall be as illustrated in Figure 3-15. The first octet shall be set to [0100 0000]. The remainder of the PDU shall consist of:

a) a cancellation reference expressed as a one octet unsigned integer, and which uniquely identifies this cancellation request within the context of the virtual circuit;

Note.— In most cases uniqueness will be assured if the reference is implemented as a sequence number starting at zero and incremented by one (modulo 256), each time a cancellation request is sent.

b) a length octet (L1) given as an unsigned integer (0 to 255), which indicates the length in octets of the set of individual local references to cancel;

c) one or more local references expressed as one or two octets each, as appropriate, and encoded in successive octets, with the total number of octets containing such local references given by L1;

d) a length octet (L2) given as an unsigned integer (0 to 255), which indicates the length in octets of the set of inclusive local reference ranges to cancel;

e) one or more pairs of local reference ranges expressed as one or two octets each, as appropriate, and encoded in successive octets, with the total number of octets containing such local references given by L2.

3.7.4.3.6.2.2 In each of the above cases, if the value of a local reference is less than 128, then bit eight of the first octet in which it is encoded shall be set to zero, and the remaining seven bits set to the value of the local reference encoded as an unsigned integer.

3.7.4.3.6.2.3 The extended local reference octet shall not be present.

3.7.4.3.6.2.4 Otherwise, bit eight shall be set to one, and the remaining seven bits and the next octet set to the value of the local reference encoded as a 15 bit unsigned integer, with the least significant eight bits placed in the extended local reference octet, and the most significant seven bits placed in the first octet.

Note.— This format allows for the local references to be cancelled, to be expressed as either a set of individual references, or a set of inclusive ranges of individual references, or both.

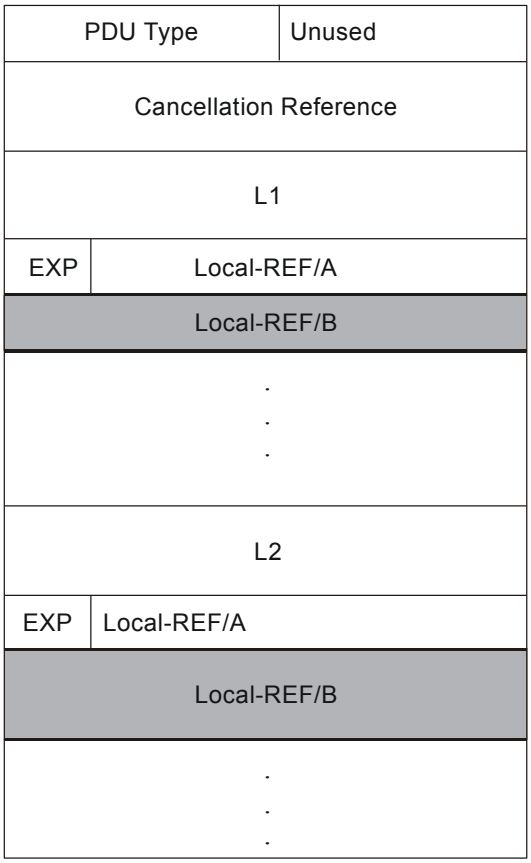


Figure 3-15. Cancellation request PDU

3.7.4.3.6.3 *The cancellation accept PDU*

3.7.4.3.6.3.1 The PDU format shall be as illustrated in Figure 3-16.

PDU type	Unused
Cancellation reference	

Figure 3-16. Cancellation accept PDU

3.7.4.3.6.3.2 The first octet shall be set to binary [0101 0000], and the second octet set to the cancellation reference of the cancellation request which is being accepted.

3.7.4.3.7 Call reset provisions

3.7.4.3.7.1 If at any time, a reset indication is received indicating a DCE originated reset, then this shall be confirmed and all other procedures associated with the call reset performed.

Note.— There is otherwise no impact on this SNDCF.

3.7.4.3.7.2 If the reset indication indicates a DTE user originated reset then, additionally, the directory associated with the virtual circuit shall be cleared to its initial state.

3.7.4.3.8 Call clearing and LREF procedures

When a virtual circuit has been terminated and the corresponding subnetwork connection group is now empty, then the local reference directory associated with this group shall be discarded.

3.7.4.4 Stream mode compression using deflate

Note 1.— The deflate algorithm was originally specified in IETF RFC 1951 and through example "C" code available from the algorithm's authors.

Note 2.— The deflate algorithm is a combination of two public domain and well-known data compression algorithms. These are the LZ77 algorithm (Lempel-Ziv 1977) and Huffman Codes. LZ77 removes redundancy in the data stream by replacing reoccurring strings by backward references to previous occurrences of such strings. Huffman Codes are variable length symbols that are used to compress strings of fixed length symbols. The Huffman Codes are chosen such that frequently occurring symbols are replaced by shorter bitstrings whilst rarely occurring symbols are replaced by longer bitstrings. They are also chosen such that no code is the prefix of another code in the same set of Huffman Codes. In deflate, the uncompressed data is first compressed using LZ77 and the result of this compression stage is further compressed using a set of standard Huffman Codes in order to compress both the literal value of strings for which no backward reference can be given, and the backward references themselves.

Note 3.— Deflate further optimizes the data compression by monitoring the stream of uncompressed data and dynamically generating a set of more optimal Huffman Codes. These can be communicated to the receiver at any time and used to improve the compression ratio.

Note 4.— The deflate specification also permits the compressor, when it detects an uncompressible string, to send that string as plain text.

Note 5.— The deflate algorithm has significant memory requirements when providing high compression efficiency. This extensive memory demand per compressed data stream may limit the number of virtual circuits which can be simultaneously supported by a given ATN router implementation over an air-ground adjacency. Consequently, ATN operators may choose to not support data stream compression when the demand for simultaneous air-ground connections exceeds the available memory resources.

3.7.4.4.1 Service description

Note.— The deflate encoder operates on NPDUs submitted via the SN-Service and after compression by the LREF function if used. The deflate decoder operates on data packets received from the subnetwork service provided by ISO/IEC 8208. The decoded NPDUs may then be further decompressed by the LREF compression procedures, if in use, or passed to the SN-service user. The positioning of the deflate encoder and decoder is illustrated in Figure 3-17.

When the use of the deflate algorithm has been proposed in the call request user data and either implicitly accepted by call acceptance in the absence of the fast select procedures, or explicitly accepted in the call accept when fast select is in use, then user data on all subsequent data packets shall be encoded using this algorithm.

Note.— ISO/IEC 8208 packets other than data packets may also contain user data. The above requirement excludes the encoding of user data on control packets as they may be delivered out of sequence.

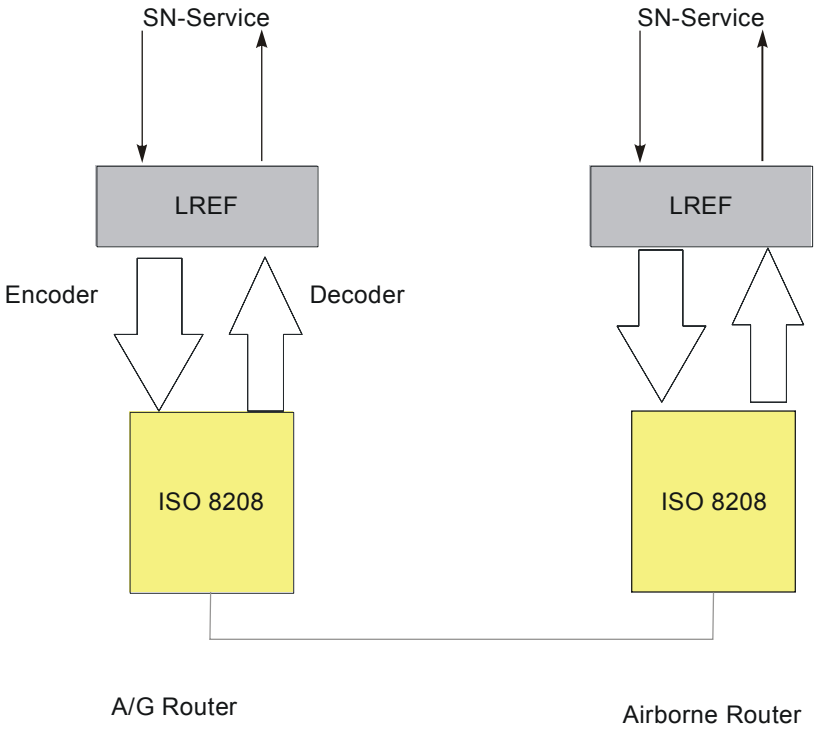


Figure 3-17. Relationship of the deflate encoder and decoder to ISO/IEC 8208 and LREF functions

3.7.4.4.2 Encoded packet format

3.7.4.4.2.1 Each NPDU shall be encoded into the compressed representation shown in Figure 3-18.

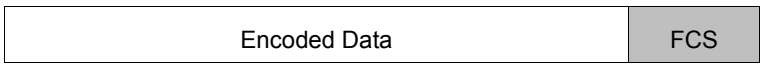


Figure 3-18. Compressed packet format

3.7.4.4.2.2 The compressed packet format shall comprise:

a) the encoded data; and

b) a two-octet frame check sum (FCS).

Note.— The length of the encoded data need not be explicitly specified as the encoded block is delimited by ISO/IEC 8208.

3.7.4.4.2.3 The sender shall ensure that the encoded representation of an NPDU is complete, i.e. that the receiver can recover the original NPDU without requiring information contained in any subsequent packets.

Note.— In IETF RFC 1951, an encoded data stream may comprise an arbitrary number of compressed blocks. This is also true for this specification. The purpose of the deflate data blocks is to delimit the scope of uncompressed data strings, strings compressed using the standard set of Huffman Codes, and those compressed using dynamically determined Huffman Codes. The compressor may decide to change between either one of these strategies at any time and not just at an NPDU boundary.

3.7.4.4.2.4 The encoded representation of the NPDUs shall be a data stream that is subdivided into a number of bit-aligned blocks of arbitrary length.

3.7.4.4.2.5 Each such block shall be in the format shown in Figure 3-19.

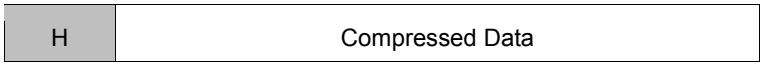


Figure 3-19. Format of deflate data blocks

3.7.4.4.2.6 Each deflate data block shall comprise:

a) a 3-bit header (H); and

b) a stream of self-delimited compressed data.

3.7.4.4.2.7 The first bit of the 3-bit header (i.e. the first bit transmitted) shall always be set to zero.

Note.— In IETF RFC 1951, setting the first bit to one indicates that it is the last block in an encoded data stream. This semantic is not required by this specification, as the end of a subnetwork connection fulfils this requirement.

3.7.4.4.2.8 The remaining two bits of the header shall be used to indicate the compression type according to Table 3-20.

Table 3-20. Compression type identifiers (bits shown in transmission order)

Encoding	*Compression type*
00	no compression
01	compressed with fixed Huffman codes
10	compressed with dynamically determined Huffman Codes
11	reserved

3.7.4.4.2.9 When a compressed data block is not wholly transmitted as the final compressed data block of the encoded data (see Figure 3-17) resulting from NPDU compression, the remaining part of that compressed data block shall be transmitted as the first part of the encoded data resulting from the compression of the next NPDU.

Note 1.— This means that compressed packets (other than the first one sent as part of a compressed data stream) do not necessarily start with a compressed data block header.

Note 2.— This behaviour is compatible with the use of the Z_PARTIAL_FLUSH option of the industry standard zlib software package. If this option is used to flush a deflate compressor, then an empty compressed data block is used to flush out compressed data. Part of this empty compressed data block typically terminates the "encoded data" and the remainder of the empty compressed data block will start the next transmission.

Note 3.— The FCS applies to the uncompressed NPDU data and is unaffected by this behaviour.

Note 4.— The required behaviour does not conflict with 3.7.4.5.2.3 as long as the compressed data block that partly terminates one transmission and starts the next transmission does not include any compressed data resulting from the compression of an NPDU.

3.7.4.4.3 Uncompressed deflate data blocks

3.7.4.4.3.1 When the encoder determines that no benefit can be derived by data compression of a given string, then that string shall be sent uncompressed.

3.7.4.4.3.2 The 3-bit header shall be right-padded with zeroes to the next octet boundary, and the remainder of the encoded data shall be formatted as shown in Figure 3-20.

Figure 3-20. Format of uncompressed deflate data blocks

3.7.4.4.3.3 An uncompressed deflate data block shall comprise:

a) an unsigned 16-bit length indicator (LEN), giving the number of octets of literal data in the block;

b) the ones complement of the 16-bit length indicator (NLEN);

c) the literal data.

3.7.4.4.3.4 The two length fields (LEN and NLEN) shall be encoded and sent least significant octet first.

3.7.4.4.3.5 The literal data shall be encoded in the same byte order as encountered in the uncompressed data stream.

Note 1.— The procedures by which the encoder determines that there is no benefit in compressing an NPDU are outside of the scope of this specification.

Note 2.— Even though the string is not compressed, this does not prevent the data in this block being referenced as part of the data stream by a subsequent LZ77-encoded NPDU.

3.7.4.4.4 Compressed deflate data blocks using fixed Huffman Codes

3.7.4.4.4.1 *General*

Note.— Encoded data blocks in the deflate format consist of sequences of symbols drawn from three conceptually distinct alphabets: either literal bytes, the alphabet of byte values (0..255), or <length, backward distance> pairs, where the length is drawn from (3..258) and the distance is drawn from (1..32 768). The literal and length alphabets are merged into a single alphabet (0..285), where values 0..255 represent literal bytes, and values 257..285 represent length codes (possibly in conjunction with extra bits following the symbol code). The value 256 indicates end-of-block and the block is hence self-delimiting without requiring an explicit length indicator.

3.7.4.4.4.1.1 A compressed NPDU shall be sent as a bit stream of bit-aligned symbols (the Huffman Codes representing literal values or length distance pairs), starting with the first bit transmitted after the 3-bit header.

3.7.4.4.4.1.2 The Huffman Codes used to encode the literal/length code in the LZ77 compressed data stream shall be as specified in Table 3-21.

Note.— Although Table 3-21 includes values 286 and 287, these are not used by the compression algorithm and are included only for completeness of the set of valid Huffman Codes.

Table 3-21. Huffman Codes used for deflate

Value	*Code length (Bits)*	*Huffman Code*
0 - 143	8	00110000 through 10111111
144 - 255	9	110010000 through 111111111
256 - 279	7	0000000 through 0010111
280 - 287	8	11000000 through 11000111

3.7.4.4.4.1.3 Huffman encoded values 0 to 255 inclusive shall represent literal values, i.e. the single octet values of a literal string.

Note.— The term "Huffman encoded value" is used to identify a symbol value that is represented by a Huffman Code taken from Table 3-21. For example, the "Huffman encoded value 145" is encoded as a 9-bit bit string "110010001".

3.7.4.4.4.1.4 The Huffman encoded value of 256 shall be used to indicate end-of-block and shall be appended at the end of each intermediate compressed deflate data block.

3.7.4.4.4.1.5 The Huffman Codes shall be encoded (packed) into the compressed data block, most significant bit first.

3.7.4.4.4.2 *Length/distance codes*

3.7.4.4.4.2.1 Length codes

3.7.4.4.4.2.1.1 Huffman-encoded values in the range 257 to 285 shall represent a length code and shall always be followed by an associated distance code.

3.7.4.4.4.2.1.2 Each length code shall represent a particular string length, as specified in Table 3-22.

3.7.4.4.4.2.2 Extra bits for length codes

3.7.4.4.4.2.2.1 Where a non-zero extra bit is specified for a given code, then a range of length values is represented by the length indicator, and the encoded representation of the length indicator shall be followed by exactly that number of additional bits.

3.7.4.4.4.2.2.2 The extra bits shall be interpreted as an integer stored with the most significant bit first.

Note.— For example, bits 1110 represent the value 14.

3.7.4.4.4.2.2.3 The value of the extra bits shall be added to the first length value in the range identified by such length code in order to determine the actual string length.

Note 1.— For example, length code 277 is followed by four extra bits. If these are 1110 then the actual string length indicated is 81.

Note 2.— Extra bits are not encoded as Huffman Codes.

Table 3-22. String length code values

Code	*Extra bits*	*Length(s)*	*Code*	*Extra bits*	*Lengths*	*Code*	*Extra bits*	*Length(s)*
257	0	3	267	1	15,16	277	4	67-82
258	0	4	268	1	17,18	278	4	83-98
259	0	5	269	2	19-22	279	4	99-114
260	0	6	270	2	23-26	280	4	115-130
261	0	7	271	2	27-30	281	5	131-162
262	0	8	272	2	31-34	282	5	163-194
263	0	9	273	3	35-42	283	5	195-226
264	0	10	274	3	43-50	284	5	227-257
265	1	11,12	275	3	51-58	285	0	258
266	1	13,14	276	3	59-66			

3.7.4.4.4.2.3 Distance codes

3.7.4.4.4.2.3.1 Each length code in the encoded data stream shall be followed by a Huffman-encoded distance code according to Table 3-23.

3.7.4.4.4.2.3.2 In this block format, the Huffman Codes for the distance codes shall be the 5-bit value of the distance code completed with leading zero-bits.

Note.— As this implies, the distance codes are assumed to each have the same probability of occurrence and hence there is no possibility of compression using Huffman Codes.

3.7.4.4.4.2.4 Extra bits for distance codes

3.7.4.4.4.2.4.1 Where a non-zero extra bit is specified for a given distance code, then a range of distances is represented by the distance code, and the encoded representation of the length indicator shall be followed by exactly that number of additional bits.

3.7.4.4.4.2.4.2 The extra bits shall be interpreted as an integer stored with the most significant bit first.

Note.— For example, bits 1110 represent the value 14.

3.7.4.4.4.2.4.3 The value of the extra bits shall be added to the first distance value in the range identified by such a distance code in order to determine the actual string length.

3.7.4.4.4.2.5 Semantic

3.7.4.4.4.2.5.1 The semantic of the distance value shall be the string (of length given by the length indicator) in the previously received data, at exactly the number of octets given by the distance value from the current position.

Note 1.— For example, the most recently received octet has a distance of one from the current position.

Note 2.— It is therefore possible under this specification to refer to a previously occurring string within the previous 32KB of data transmitted.

3.7.4.4.4.2.5.2 A backward reference shall not refer to a string on any other subnetwork connection or transmitted before a network reset has been performed.

Note 1.— A string reference may refer to a string in a previous block; i.e. the backward distance may cross one or more block boundaries. However a distance cannot refer past the beginning of the subnetwork connection, or since the most recent network service reset due to the fact that the receiving user may not have received those blocks transmitted immediately prior to a reset.

Note 2.— The referenced string may overlap the current position; for example, if the last 2 bytes decoded have values X and Y, a string reference with <length = 5, distance = 2> adds X,Y,X,Y,X to the output stream.

Table 3-23. Distance codes

Code	*Extra bits*	*Distance*	*Code*	*Extra bits*	*Distance*	*Code*	*Extra bits*	*Distance*
0	0	1	10	4	33-48	20	9	1025-1536
1	0	2	11	4	49-64	21	9	1537-2048
2	0	3	12	5	65-96	22	10	2049-3072
3	0	4	13	5	97-128	23	10	3073-4096
4	1	5,6	14	6	129-192	24	11	4097-6144
5	1	7,8	15	6	193-256	25	11	6145-8192
6	2	9-12	16	7	257-384	26	12	8193-12288
7	2	13-16	17	7	385-512	27	12	12289-16384
8	3	17-24	18	8	513-768	28	13	16385-24576
9	3	25-32	19	8	769-1024	29	13	24577-32768

3.7.4.5.5 Compressed deflate data blocks using dynamically determined Huffman Codes

3.7.4.5.5.1 *General*

Note 1.— The fixed set of Huffman Codes represent an initial "guess" as to the entropy of the original data stream and hence what are the optimal Huffman Codes. However, it is likely that analysis of an actual data stream will reveal a more appropriate set. This specification allows for this by providing a means to communicate a set of dynamically determined Huffman Code tables from compressor to decompressor and to identify the scope of applicability for those codes. This is achieved through the deflate data block format specified in this section. The data block includes a new set of Huffman Code tables at the beginning of the block and the remainder of the block comprises a compressed LZ77 data stream, compressed using these Huffman Code tables.

Note 2.— In order to avoid the overhead of exchanging the actual Huffman Code tables, the Huffman Codes are required to comply with a set of rules that permits a Huffman Code table to be generated from knowledge of the code lengths and the encoded alphabet only. As the alphabet is known by the decompressor a priori, only the code lengths have to be communicated.

Note 3.— A further level of compression is achieved by encoding the lists of code lengths as Huffman Codes. The Huffman Codes for the code lengths are themselves communicated at the start of this deflate data block format, by communicating their code lengths only.

Note 4.— The mechanism by which the compressor decides to make use of dynamically determined Huffman Codes is outside of the scope of this specification.

3.7.4.5.5.1.1 The Huffman Codes used for each alphabet in the deflate format shall obey the following rules:

a) all codes of a given bit length have lexicographically consecutive values, in the same order as the symbols they represent; and

b) shorter codes lexicographically precede longer codes.

3.7.4.5.5.1.2 The sequences of code length shall themselves be compressed using a Huffman Code and the alphabet for code lengths specified in Table 3-24.

Table 3-24. Alphabet for code lengths

Code	*Semantic*
0 .. 15	Represent code length of 0 to 15
16	Copy the previous code length 3 to 6 times; the next 2 bits indicate the repeat length (0 = 3, ... 3 = 6)
17	Repeat a code length of 0 for 3 to 10 times; the next 3 bits indicate the repeat length
18	Repeat a code length of 0 for 11 to 138 times; the next 7 bits indicate the repeat length

Note.— For example, codes 8, 16(+ binary 11), 16(+ binary 10) will expand to 12 code length of 8.

3.7.4.5.5.1.3 A code length of 0 shall indicate that the corresponding symbol in the literal/length or distance alphabet will not occur in the block and does not participate in the Huffman Code construction algorithm.

3.7.4.5.5.2 *Block format*

The format of a deflate data block using dynamically determined Huffman Codes shall comprise the following bit-aligned fields starting immediately after the 3-bit header, and encoded consecutively:

a) The 5-bit HLIT field, set to (number of literal/length codes - 257);

Note.— The number of literal/length codes is in the range 257 to 286.

b) The 5-bit HDIST field, set to (number of distance codes - 1);

Note.— The number of distance codes is in the range 1 to 32.

c) The 4-bit HCLEN field, set to (number of code length codes - 4);

Note.— The number of code length codes is in the range 4 to 19.

d) (HCLEN + 4) x 3 bits: code lengths for the code length alphabet given in Table 3-24, in the order: 16, 17, 18, 0, 8, 7, 9, 6, 10, 5, 11, 4, 12, 3, 13, 2, 14, 1, 15;

Note.— The code lengths are interpreted as 3-bit integers (0-7); as above, a code length of 0 means the corresponding symbol (literal/length or distance code length) is not used.

e) (HLIT + 257) code lengths for the literal/length alphabet, encoded using the code length Huffman Code

f) (HDIST + 1) code lengths for the distance alphabet, encoded using the code length Huffman Code

g) The actual compressed data of the block, encoded using the literal/length and distance Huffman Codes defined in the first part of this block

h) The literal/length symbol 256 (end of data), encoded using the literal/length Huffman Code.

Note.— The code-length repeat codes can cross from HLIT + 257 to the HDIST + 1 code lengths. In other words, all code lengths form a single sequence of HLIT + HDIST + 258 values.

3.7.4.5.5.3 *Decoding of dynamically determined Huffman Codes*

Note.— The following algorithm generates the Huffman Codes from the encoded bit-length codes as integers, intended to be read from most- to least-significant bit. A version of this algorithm expressed in "C" code may be found in IETF RFC 1951.

Dynamically determined Huffman Codes shall be decoded as follows:

1) Count the number of codes for each code length.

2) Find the numerical value of the first code for each code length, by applying the rule that no Huffman Code in the same table can be the prefix of another. For the smallest code length this is zero. For each subsequent code length, this is determined by identifying the next unallocated code for the preceding code length (by adding the number of codes to the first code) and then representing the result as a binary number, and right-padding the number with zero-bits so that the number has the same number of bits as required by the code length.

3) Assign numerical values to all codes, using consecutive values for all codes of the same length with the base values determined at step 2. Codes that are never used (which have a bit length of zero) must not be assigned a value.

Note.— For example, consider the alphabet ABCDEFGH with code lengths defined to be (3,3,3,3,3,2,4,4). Applying the above algorithm would generate the following Huffman Codes for each member of the alphabet:

Symbol	*Length*	*Code*
A	3	010
B	3	011
C	3	100
D	3	101
E	3	110
F	2	00
G	4	1110
H	4	1111

3.7.4.5.6 Frame checksum (FCS)

3.7.4.5.6.1 A two-octet, octet-aligned, frame checksum shall be appended to the end of each encoded packet.

3.7.4.5.6.2 The frame checksum shall be computed according to the same procedures as specified in ISO/IEC 8073 for computation of the transport protocol class 4 checksum.

3.7.4.5.6.3 The two octets of the frame checksum shall be the two partial sums C0 and C1 as specified in ISO/IEC 8073 Annex D.

3.7.4.5.6.4 The value of C0 shall be the first octet of the frame checksum parameter and the value of C1 shall be the second octet.

3.7.4.5.6.5 The checksum shall be computed on the NPDU prior to application of the deflate data compression procedure, i.e. it is a checksum on the uncompressed NPDU.

Note.— The frame checksum may be used by the decompression procedure to verify correct decompression of the NPDU.

3.7.4.5.7 Compression procedure

3.7.4.5.7.1 *General*

3.7.4.5.7.1.1 Each NPDU received from the SN-service user, possibly after compression by the LREF algorithm, shall be encoded into a single compressed data block in the format given by Figure 3-18 and specified in section 3.7.4.5.2.

3.7.4.5.7.1.2 The resulting data block shall be a complete encoded representation of the NPDU.

3.7.4.5.7.1.3 An implementation should use the full 32KB range of distance values permitted by the compressed data format.

Note 1.— This permits an implementation of the compressor to autonomously limit the size of the backwards window used to compress data in order to optimize the use of memory resources. However, the result will be a poorer compression ratio. On the other hand, the decompressor must always be able to accept any valid distance value, i.e. must maintain a 32KB buffer.

Note 2.— The actual procedure by which an implementation locates matches for strings in previously sent data, or even the length of the strings it looks for, is out of the scope of this specification.

3.7.4.5.7.2 *NPDU encoding*

3.7.4.5.7.2.1 The NPDU shall be encoded in the same sequence in which it would have been transmitted if it had not been compressed.

3.7.4.5.7.2.2 Octet sequences for which no preceding match is found shall be encoded as literal values using their corresponding Huffman Codes (i.e. Huffman Codes representing values in the range 0…255).

3.7.4.5.7.2.3 Octet sequences for which a match has been found within the last 32KB of encoded data shall be encoded as length/distance pairs.

3.7.4.5.7.2.4 The length of the octet string shall be encoded first, where necessary followed by the appropriate extra bits needed to fully define the length value.

3.7.4.5.7.2.5 The distance to the duplicate string shall similarly be encoded using the Huffman Code specified in Table 3-22 for the required distance, where necessary also followed by the appropriate extra bits needed to fully define the distance.

3.7.4.5.7.2.6 The Huffman Codes used shall be defined by the type of deflate data block (i.e. using the set of fixed Huffman Codes or a dynamically determined set).

3.7.4.5.7.2.7 NPDUs shall be compressed and passed to the ISO/IEC 8208 subnetwork in exactly the same order that they were given to the deflate compression function by the SN-service user.

3.7.4.5.7.2.8 When all octets in the NPDU have been encoded, the bit stream shall be padded with zero-bits until the next octet boundary is reached.

3.7.4.5.7.2.9 The frame checksum (FCS) shall then be appended to the compressed block.

Note.— The FCS is encoded as its binary value. It is not subject to Huffman encoding.

3.7.4.5.8 Decompression procedures

3.7.4.5.8.1 *General*

3.7.4.5.8.1.1 NPDUs shall be decompressed in exactly the same order that they have been received from the ISO/IEC 8208 subnetwork.

3.7.4.5.8.1.2 Each data packet received from an ISO/IEC 8208 subnetwork shall be assumed to be in the format given by Figure 3-18, and thus comprises one or more deflate data blocks.

3.7.4.5.8.2 *Compressed deflate data block*

3.7.4.5.8.2.1 Each compressed deflate data block shall be interpreted as a sequence of Huffman-encoded symbols.

3.7.4.5.8.2.2 Huffman-encoded values in the range 0…255 shall be taken as literal octet values and appended to the NPDU that is being decompressed in the order that they are found.

3.7.4.5.8.2.3 The Huffman-encoded value 256 shall be taken as end-of-block indication and not appended to the NPDU that is decompressed.

3.7.4.5.8.2.4 Huffman-encoded values in the range 257...285 shall be taken as length indicators and as introducing a length/distance pair.

3.7.4.5.8.2.5 The length and distance values shall be decoded, and the referenced string shall be appended to NPDU that is being decompressed.

3.7.4.5.8.3 *Uncompressed deflate data block*

Octets from uncompressed deflate data blocks shall be appended to the NPDU in the order in which they are encoded.

3.7.4.5.8.4 *FCS verification*

3.7.4.5.8.4.1 The frame checksum for the uncompressed NPDU shall be the last two octets of the received packet and shall be verified for all received NPDUs.

3.7.4.5.8.4.2 If this verification check fails, then the NPDU shall be discarded and a network reset initiated on the ISO/IEC 8208 subnetwork connection.

Note.— This network reset will be indicated to the receiving peer entity as a DTE-originated reset.

3.7.4.5.8.4.3 In this case, the call reset procedures specified in 3.7.4.4.9 shall be performed.

3.7.4.5.8.4.4 The error should be notified to system management.

3.7.4.5.9 Call reset provisions

3.7.4.5.9.1 If, at any time, a reset indication is received indicating a DCE-originated reset, then this shall be confirmed and all other procedures associated with the call reset performed.

3.7.4.5.9.2 If, at any time, the virtual circuit is reset by the local or remote DTE with the cause field indicating a DTE-originated reset, then the deflate compressor and decompressor history windows and the absolute value of the upper edge of these windows shall be re-initialized to the state which existed when the last virtual circuit without maintenance of the deflate history windows was established in this subnetwork connection group.

3.7.4.5.9.3 In particular, if the last virtual circuit established without maintenance of the deflate history windows in this subnetwork connection group was also established:

a) without the use of a pre-stored data stream dictionary, then the compressor and decompressor history windows of the current virtual circuit shall be reset to a void state and the absolute value of the upper edge of these windows shall be reset to 0;

b) with the use of a pre-stored data stream dictionary, then the compressor and decompressor history windows of the current virtual circuit shall be re-initialized with the content of that dictionary, and the absolute value of the upper edge of these windows shall be re-initialized to the size of the dictionary data copied into the history windows.

Note 1.— The absolute value of the upper edge of the decompressor (resp. compressor) history window designates the absolute offset of the last received (resp. sent) octet in the sequence of octets that were stored in the decompressor (resp. compressor) history window since its initialization or its last re-initialization in the context of the subnetwork connection group.

Note 2.— The re-initialization of the compressor and decompressor history windows occurs in the following cases:

a) when the virtual circuit currently active in the context of the subnetwork connection group is reset with a reason code indicating DTE-originated reset;

b) when a new virtual circuit is established in the context of the subnetwork connection group without the option for the maintenance of the deflate history windows.

Note 3.— At initialization or re-initialization time of the compressor and decompressor history windows, if no pre-stored data stream is used, then the upper edges of the compressor and decompressor history windows are initialized to zero. However, if a pre-stored data stream dictionary is used, then the upper edges of the compressor and decompressor history windows are initialized to the size of the dictionary data copied into the compressor and decompressor history windows.

Note 4.— When the deflate history windows are maintained over subsequent virtual circuits of the same subnetwork connection group, then the upper edges of the decompressor and compressor history windows are not reset to 0 or to the size of a pre-stored dictionary; they are simply re-synchronized with the upper edges of the decompressor and compressor history windows of the remote DTE.

Note 5.— Corruption of a data stream compression dictionary may cause a permanent communication failure.

3.7.5 ATN mobile SNDCF protocol requirements list

3.7.5.1 An implementation of the ATN mobile SNDCF shall be used in ATN airborne and air-ground routers if and only if its PICS is in compliance with the APRLs given in ⁋3.7.5.8.

3.7.5.2 ATN requirements for mobile SNDCFs

3.7.5.2.1 Major capabilities

Item	*Capability*	*ATN reference*	*ATN support*
mcNego	Negotiation of compression algorithm	⁋3.7.4.2	M
mcLocRef	Local reference header compression	⁋3.7.4.3	M
mcCan	Local reference cancellation	⁋3.7.4.3.6	O
mcM/I	Local reference directory maintenance	⁋3.7.4.3	Snvdl:M ^Snvdl:O
mcVer2	Version 2 of ISO/IEC 8208 mobile SNDCF	⁋3.7.4.2	M
mcDict	Negotiation of use of pre-stored dictionaries	⁋3.7.4.2.1, ⁋3.7.4.2.2	mcVer2:O ^mcVer2:-
mcDefMaint	Negotiation of maintenance of deflate history windows	⁋3.7.4.2.1, ⁋3.7.4.2.2	mcVer2:O ^mcVer2:-
mcDeflate	Deflate compression	⁋3.7.4.5	O

Note.— Snvdl is true when the VDL SNDCF is implemented.

3.7.5.2.2 Call setup and clearing procedures

Item	*Function*	*ATN reference*	*ATN support*
clInit	Call initiator	⁋3.7.4.2	O.1
clRspd	Call responder	⁋3.7.4.2	O.1
csDynam	Dynamic call setup	⁋3.7.4.2.1.1.1	clInit:O.2
csSys	Call setup by systems management	⁋3.7.4.2.1.1	clInit:O.2
csDef	Use of non-standard default packet size	⁋3.7.4.2.1.3	clInit:O.3
csNeg	Use of flow control parameter negotiation	⁋3.7.4.2.1.3	clInit:O.3
csFast	Use of fast select	⁋3.7.4.2.1.4	M
csM/I	Local reference directory maintenance request/acceptance	⁋3.7.4.2.1.5.4.9 ⁋3.7.4.2.2.2.3	^csFast: - mcM/I:M

Item	*Function*	*ATN reference*	*ATN support*
csOther	Use of other optional user facilities and CCITT-specified DTE facilities	⁅3.7.4.2.1.1.3	O
csCol	Call collision resolution	⁅3.7.4.2.2.1.2	clInit:M
csAcp	Call acceptance procedures	⁅3.7.4.2.1.6	clRspd:M
csRej	Call rejection procedures	⁅3.7.4.2.1.7	clRspd:M
csOrd	Order of compression procedures	⁅3.7.4.2.3.2	M
csDiag	Use of call rejection diagnostic codes	⁅3.7.4.2.1.7.3	clInit:M
csClear	Call clearing procedures	⁅3.7.4.2.4	M

Note.— Fast select only required if supported by subnetwork.

3.7.5.2.3 Negotiation of compression algorithm

Item	*Function*	*ATN reference*	*ATN support*
caMaxd	Indication of the maximum of directories entries in the call user data	⁅3.7.4.2.1.5.4.11	mcNego:O
caDict	Request/acceptance of use of pre-stored dictionaries	⁅3.7.4.2.1.5.4.20, ⁅3.7.4.2.1.6.1.10, ⁅3.7.4.2.2.2.9.4	mcDict:M ^mcDict:-
caDefMaint	Request/acceptance of maintenance of deflate history windows	⁅3.7.4.2.1.5.4.21, ⁅3.7.4.2.1.6.1.10, ⁅3.7.4.2.2.2.9.3	mcDefMaint:M ^mcDefMaint:-

3.7.5.2.4 Local reference header compression

Item	*Function*	*ATN reference*	*ATN support*
lrVC	Opening additional virtual circuits	⁅3.7.4.3.2.1.2	M
lrDirSize	Local directory with more than 128 entries	⁅3.7.4.3.1	O
lrProt	Identification of network layer protocol	⁅3.7.4.3.2.2	M
lrMod	Processing of SN-UnitData requests	⁅3.7.4.3.2	M
lrEst	Establishment of new local reference	⁅3.7.4.3.2.4	M
lrTransfer	Transfer of modified ISO 8473 PDU	⁅3.7.4.3.2.6	M
lrInitial	Initial DT PDU compression	⁅3.7.4.3.3.2	M
lrDerived	Derived DT PDU compression	⁅3.7.4.3.3.3	M

Item	*Function*	*ATN reference*	*ATN support*
lrError-s	Generation of error PDU compression	⁋3.7.4.3.3.3	M
lrDiscard	Compression of discarded PDU encapsulated within error PDU	⁋3.7.4.3.3.3.17	lrError-s:M
lrCompTr	Transfer of compressed PDUs	⁋3.7.4.3.3.3.19	M
lrReceived	Processing of received PDUs	⁋3.7.4.3.4	M
lrUncomp-r	Processing of received uncompressed PDUs	⁋3.7.4.3.4.2	M
LrReset	Purging directories entries on Reset	⁋3.7.4.3.7	mcLocRef:M
lrUnMod-r	Processing of received unmodified PDUs	⁋3.7.4.3.4.2.2	M
lrComp-r	Processing of received compressed data PDUs	⁋3.7.4.3.4.3	M
lrError-r	Processing of received compressed error PDUs	⁋3.7.4.3.4.4	M
lrSNDCFerr-s	Generation of SNDCF error report	⁋3.7.4.3.5	M
lrSNDCFerr-r	Processing of received SNDCF error report	⁋3.7.4.3.4.5	M

3.7.5.2.5 Local reference cancellation

Item	*Function*	*ATN reference*	*ATN support*
lrcMgmt	Management of local references	⁋3.7.4.3.2.5	mcCan:M
lrcRequest-s	Generation of cancellation request PDU	⁋3.7.4.3.6	mcCan:M
lrcRequest-r	Processing of incoming cancellation request PDU	⁋3.7.4.3.6	mcCan:M
lrcReliable	Reliable transfer of cancellation request	⁋3.7.4.3.6	mcCan:M
lrcAccept-s	Generation of cancellation accept PDU	⁋3.7.4.3.6	mcCan:M
lrcAccept-r	Processing of incoming cancellation accept PDU	⁋3.7.4.3.6	mcCan:M

3.7.5.2.6 PDU formats

3.7.5.2.6.1 *Call request user data*

Item	*Description*	*ATN reference*	*ATN support*
crLen	Length indicator	⁋3.7.4.2.1.5.3	M
crVersion	Version indicator	⁋3.7.4.2.1.5.4.1	M
crSNCR	Subnetwork connection reference (SNCR)	⁋3.7.4.2.1.5.4.2	M

Item	*Description*	*ATN reference*	*ATN support*
crComp	Offered compression techniques	⌈3.7.4.2.1.5.4.4	M
crDir	Maximum directory size *Note.—Dynamically, this field is only generated if local reference compression is offered.*	⌈3.7.4.2.1.5.4.11	M
crExtBlock	SNDCF parameter extension block	⌈3.7.4.2.1.5.4.13	mcVer2:M
crDictList	Dictionaries list parameter	⌈3.7.4.2.1.5.4.20	mcDict:M ^mcDict:-
crDefMaint	Deflate maintenance parameter	⌈3.7.4.2.1.5.4.21	mcDefMaint:M ^mcDefMaint:-
crAdd-s	Additional user data on send	⌈3.7.4.2.1.5.5	O
crAdd-r	Additional user data on receive	⌈3.7.4.2.1.5.5	O
MaxDir	Maximum number of directory entries supported	⌈3.7.4.2.1.5.4.11	≥128

3.7.5.2.6.2 *Call accept user data*

Item	*Description*	*ATN reference*	*ATN support*
caComp	Offered compression techniques	⌈3.7.4.2.2.4.3	mcNego:M
caAdd-s	Additional user data on send	⌈3.7.4.2.2.4.6	mcNego:O
caAdd-r	Additional user data on receive	⌈3.7.4.2.2.4.6	mcNego:O
caExtBlock	SNDCF parameter extension block	⌈3.7.4.2.2.4.5	mcVer2:M
caDictSel	Dictionaries selection parameter	⌈3.7.4.2.2.4.7	mcDict:M ^mcDict:-
caDefMaint	Deflate maintenance parameter	⌈3.7.4.2.1.5.4.21	mcDefMaint:M ^mcDefMaint:-

3.7.5.2.6.3 *Modified ISO/IEC 8473 NPDU*

Item	*Description*	*ATN reference*	*ATN support*
npLocRef-s	Local Reference Option field	⌈3.7.4.3.2.3	M

3.7.5.2.6.4 *Compressed initial PDU*

Item	*Description*	*ATN reference*	*ATN support*
inType	PDU Type	⌈3.7.4.3.3.2.2	M

Item	*Description*	*ATN reference*	*ATN support*
inPri	Priority	§3.7.4.3.3.2.3	M
inLifetime	Lifetime	§3.7.4.3.3.2.4	M
inFlags	Flag Bits	§3.7.4.3.3.2.5 to §3.7.4.3.3.2.9	M
inLocRef	Local reference (1 octet)	§3.7.4.3.3.2.9	M
inLocRef2	Local reference (2 octet)	§3.7.4.3.3.2.9	lrDirSize:M ^lrDirSize:X
inPDUId	PDU identifier	§3.7.4.3.3.2.10	M
inNSDU	User data	Figure §3-13	M

3.7.5.2.6.5 *Compressed derived PDU*

Item	*Description*	*ATN reference*	*ATN support*
drType	PDU type	§3.7.4.3.3.3.2	M
drPri	Priority	§3.7.4.3.3.3.3	M
drLifetime	Lifetime	§3.7.4.3.3.3.4	M
drFlags	Flag bits	§3.7.4.3.3.3.5 to §3.7.4.3.3.3.9	M
drLocRef	Local reference (1 octet)	§3.7.4.3.3.2.8	M
drLocRef2	Local reference (2 octet)	§3.7.4.3.3.2.8	lrDirSize:M ^lrDirSize:X
drPDUId	PDU identifier	§3.7.4.3.3.3.11	M
drSegOff	Segment offset	§3.7.4.3.3.3.13	M
drTotalLen	Total length	§3.7.4.3.3.3.15	M
drNSDU	User data	Figure §3-13	M

3.7.5.2.6.6 *Compressed error PDU*

Item	*Description*	*ATN reference*	*ATN support*
erType	PDU type	§3.7.4.3.3.3.21	M
erPri	Priority	§3.7.4.3.3.3.23	M
erLifetime	Lifetime	§3.7.4.3.3.3.25	M

Item	*Description*	*ATN reference*	*ATN support*
erFlags	Flag bits	§3.7.4.3.3.3.27 to §3.7.4.3.3.3.33	M
erLocRef	Local reference (1 octet)	§3.7.4.3.3.2.8	M
erLocRef2	Local reference (2 octet)	§3.7.4.3.3.2.8	lrDirSize:M ^lrDirSize:X
erReason	Discard reason	§3.7.4.3.3.3.34	M
erNSDU	Compressed header of discarded PDU	§3.7.4.3.3.3.17	M

3.7.5.2.6.7 *SNDCF error report PDU*

Item	*Description*	*ATN reference*	*ATN support*
sfType	PDU type	§3.7.4.3.5	M
sfReason	Discard reason	§3.7.4.3.5	M
sfLocRef	Local reference	§3.7.4.3.5	M
sfLocRef2	Local reference (2 octet)	§3.7.4.3.3.2.9	lrDirSize:M ^lrDirSize:X

3.7.5.2.6.8 *Cancellation request*

Item	*Description*	*ATN reference*	*ATN support*
cqType	PDU type	§3.7.4.3.6	mcCan:M
cqRef	Cancellation reference	§3.7.4.3.6	mcCan:M
cqLocRef	Local reference	§3.7.4.3.6	mcCan:M
cqLocRef2	Local reference (2 octet)	§3.7.4.3.3.2.9	mcCan:M

3.7.5.2.6.9 *Cancellation accept*

Item	*Description*	*ATN reference*	*ATN support*
ccType	PDU type	§3.7.4.3.6	mcCan:M
ccRef	Cancellation reference	§3.7.4.3.6	mcCan:M

3.7.6 SNDCF for IPv4 and IPv6 subnetworks

3.7.6.1 Model of operations

Note.— This section provides a description of the model of operations for the IP SNDCF.

3.7.6.1.1 The model of operations for the IP SNDCF shall be as illustrated in Figure 3-21.

3.7.6.1.2 The SNDCF shall provide an interface between CLNP and IP.

Note 1.— Other SNDCFs may provide access to other network interfaces and services, while other communications protocols may also make use of the IP network service (e.g. TCP). Architecturally, the SNDCF is the same for both IPv4 and IPv6.

Note 2.— The IP SNDCF is also used by the ES-IS protocol ([4]) when this protocol is run over an IP Network.

Note 3.— CLNP ([2]) is not intended to be an exclusive user of the IP network service, nor is it restricted to use only the network service provided by IP. The IP header does not replace the CLNP header. The CLNP header and user data are transferred as the data portion of an IP datagram.

Note 4.— Such datagrams may be fragmented during transit in the IP subnetwork. Generally, this is undesirable as it imposes additional overhead. When ATN systems are deployed, network managers are advised to take into account the maximum MTU size of any IP subnetworks that may be part of an end-to-end path when determining the maximum TPDU size to be negotiated.

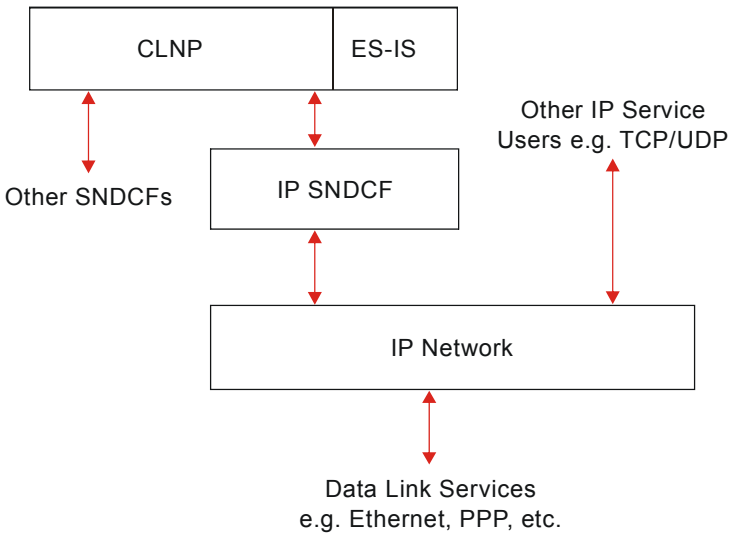


Figure 3-21. SNDCF for IP networks

3.7.6.2 References

Note.— This section provides references to the underlying standards that drive the design of the IP SNDCF.

1	IETF RFC 1791	September 1981	Internet protocol – DARPA Internet programme protocol specification
2	ISO/IEC 8473-1	1994	Information technology – Protocol for providing the connectionless-mode network service: protocol specification.
3	IETF RFC 3232	January 2002	Assigned Numbers: RFC 1700 is replaced by an on-line database
4	ISO/IEC 9542	1988	Information processing systems – Telecommunications and information exchange between systems – End system to intermediate system routing exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO/IEC 8473).
5	IETF RFC 1070	February 1989	Use of the Internet as a subnetwork for experimentation with the OSI network layer
6	ISO/IEC TR 9577	1993	Information technology - telecommunications and information exchange between systems - protocol identification in the network layer
7	IETF RFC 792	September 1981	Internet control message protocol (ICMP)
8	IETF RFC 3260	April 2002	New terminology and clarifications for Diffserv
9	IETF RFC 2460	December 1998	Internet protocol, Version 6 (IPV6) specification
10	IETF RFC 2463	December 1998	Internet control message protocol (ICMPv6) for the Internet protocol Version 6 (IPv6) specification
11	IETF RFC 796	September 1981	ADDRESS MAPPINGS Note.— This document is updated by [17].
12	IETF RFC 3513	April 2003	IP Version 6 addressing architecture
13	IETF RFC 2474	December 1998	Definition of the differentiated services field (DS Field) in the IPv4 and IPv6 headers Note.— This document is updated by [8] and [14].

14	IETF RFC 3168	September 2001	The addition of explicit congestion notification (ECN) to IP
15	IETF RFC 1812	June 1995	Requirements for IP Version 4 routers
16	IETF RFC 2309	April 1998	Recommendations on queue management and congestion avoidance in the Internet
17	IETF RFC 1519	September 1993	Classless inter-domain routing (CIDR): an address assignment and aggregation strategy

3.7.6.3 Provision of the SN-UNITDATA.request service element

3.7.6.3.1 Service element parameters

3.7.6.3.1.1 For IPv4, the SN-source-address and SN-destination-address parameters shall be 32-bit IP addresses.

Note.— Extra information concerning the IPv4 addressing architecture may be found in [11] and [17].

3.7.6.3.1.2 For IPv6, the SN-source-address and SN-destination-address parameters shall be 16-octet IP addresses.

Note.— Extra information concerning the IPv6 addressing architecture may be found in [12].

3.7.6.3.1.3 As a local matter, the SN-source-address shall either be:

a) used to indicate the SNPA from which the encapsulated PDU is to be sent: or

b) set to a null value.

Note.— The CLNP routing decision process will determine the SNPA from which the PDU is to be sent and the destination SNPA it is to be sent to. In many implementations, the source SNPA will be implicit in the selection of a particular instance of the IP SNDCF and hence, in such cases, this parameter is superfluous and may be set to a null value.

3.7.6.3.1.4 As a local matter, the SN-Quality-of-Service subparameters, if present, other than priority shall either be ignored by the IP SNDCF, or used to determine the differential service requirements for the encapsulating IP packet header.

3.7.6.3.1.5 The priority subparameter of the SN-Quality-of-Service service parameter shall be used to determine the value of the differentiated service field indicated in the encapsulating IP packet header as described in the procedures below.

3.7.6.3.1.6 The SN-Userdata shall be an unconstrained octet-string (e.g. an encoded CLNP PDU including the CLNP header and user data).

Note.— The user of the SN-UNITDATA.Request service is not constrained to CLNP and other users may include the ES-IS protocol and the IS-IS protocol.

3.7.6.3.2 Procedures

3.7.6.3.2.1 *IPv4 subnetworks*

3.7.6.3.2.1.1 When the IP SNDCF SN-UNITDATA.Request service element is invoked, an IPv4 datagram shall be constructed with the SN-userdata as the data portion of the datagram (the payload).

3.7.6.3.2.1.2 The IP datagram header shall be constructed according to [1] and as follows:

Note.— In most implementations, the IP packet will be constructed by the underlying IP service and not by the SNDCF. The SNDCF is normally responsible only for providing the parameters used for constructing the header.

a) the protocol shall be set to decimal 80 (as specified in [3] and formerly by [5] for ISO-IP);

b) the source address shall be the IP address assigned to the interface from which the packet is sent;

c) the destination address shall be the SN-destination-address;

d) the time to live shall be set to a locally specified value, which shall be configurable;

e) the three topmost bits of the differentiated service code point (DSCP, former precedence subfield) of the type of service (TOS) field shall be set depending on the value of the priority subparameter of the SN-Quality-of-Service service parameter, as in Table 3-25:

Table 3-25. CLNP priority to IP precedence mapping

IP precedence	*CLNP priority*
000 – Routine	0, 1, 2, 3, 4, 5
001 – Priority	6, 7
010 – Immediate	8, 9
011 – Flash	10
100 – Flash override	11, 12, 13
101 – CRITIC/ECP	14
110 – Internetwork control	N/A
111 – Network control	N/A

Note.— [15] indicates that user level packets with priority of 6 or 7 may be downgraded or discarded as these priorities are reserved for router to router communications.

f) as a local matter, the remaining differentiated service bits shall be set to correspond to the SN-Quality-of-Service parameter or to a locally specified default value;

Note.— This way of handling TOS maps to [13] by implementing the default and class-selector codepoints.

g) the last two bits of the TOS field (i.e. bits 6 and 7 according to [1]), shall be set to zero.

Note.— See section 22 of [14] for a discussion on the history of the IPv4 TOS bits. As indicated in [8], current practices assign the TOS bits 6 and 7 to the ECN. Setting these bits to zero is deemed necessary to indicate that ECN is not supported.

3.7.6.3.2.1.3 The resulting IP datagram shall be forwarded to its addressed destination on the IP network.

3.7.6.3.2.2 *IPv6 subnetworks*

3.7.6.3.2.2.1 When the IP SNDCF SN-UNITDATA.Request service element is invoked, an IPv6 header shall be constructed with the SN-userdata as the payload of the complete datagram.

3.7.6.3.2.2.2 The IP datagram header shall be constructed according to [9] and as follows:

Note.— In most implementations, the IP packet will be constructed by the underlying IP service and not by the SNDCF. The SNDCF is normally responsible only for providing the parameters used for constructing the header.

a) the next header field shall be set to decimal 80 (as specified in [3] for ISO-IP) unless extension headers are present, when the next header field of the final header shall be set to decimal 80.

Note.— The use of extension headers (e.g. for source routing) is a local matter.

b) the source address shall be the IP address assigned to the interface from which the packet is sent;

c) the destination address shall be the SN-Destination-Address;

d) the hop limit shall be set to a locally specified value, which shall be configurable;

e) the flow label shall be set to zeroes;

f) the traffic class shall be set according to [13]. The value of the first six bits (the DSCP) shall be set to the value xxx000, where the bits “xxx” are set depending on the value of the priority subparameter of the SN-Quality-of-Service service parameter and according to Table 3-25 (i.e. they are set to the value of the precedence bits in Table 3-25);

g) the last two bits of the traffic class shall be set to zero.

Note.— Setting the ECN bits to zero indicates that ECN is not supported. However, this may result in ATN data being randomly dropped by the “RED” algorithm for active queue management [16]. Network managers will need to investigate operation of the RED algorithm and may have to modify it in order to meet ATN service requirements.

3.7.6.4 SN-UNITDATA.Indication service element

3.7.6.4.1 IPv4 subnetworks

3.7.6.4.1.1 The system shall be configured such that IP packets with a protocol id of 80 are passed to the IP SNDCF.

Note.— As a consequence, an IPv4 datagram received by and addressed to an interface on the local system and with a protocol header field set to decimal 80 will be passed to the IPv4 SNDCF by the IP network service provider.

3.7.6.4.1.2 All IP datagrams passed to the IPv4 SNDCF by the IP network service provider shall result in an

SN-UNITDATA.Indication, constructed as follows:

a) the SN-Source-Address shall be set to the value of the source address field of the IP datagram header;

b) the SN-Destination-Address shall be set to the value of the destination address field of the IP datagram header;

c) the SN-Userdata shall be the data portion of the IP datagram;

d) no SN-Quality-of-service parameter shall be present.

Note.— Following standard practice, the first octet of the SN-Userdata is assumed to be the network protocol identifier as specified by [6] and is used to determine whether this is a CLNP packet, an ES-IS packet, etc. The received packet is then processed accordingly by the appropriate network layer protocol.

3.7.6.4.2 IPv6 subnetworks

3.7.6.4.2.1 The system shall be configured such that IP packets with a next header byte for the payload set to 80 are passed to the IP SNDCF.

Note.— As a consequence, an IPv6 datagram received by and addressed to an interface on the local system and with a next header field in either the IPv6 header or an extension header set to decimal 80 will be passed to the IPv6 SNDCF by the IP network service provider.

3.7.6.4.2.2 All IP datagrams passed to the IPv6 SNDCF by the IP network service provider shall result in an SN-UNITDATA.Indication, constructed as follows:

a) the SN-Source-Address shall be set to the value of the source address field of the IP datagram header;

b) the SN-Destination-Address shall be set to the value of the destination address field of the IP datagram header;

c) the SN-Unitdata shall be the payload of the IP datagram;

d) no SN-Quality-of-service parameter shall be present.

Note.— Following standard practice, the first octet of the SN-Userdata is assumed to be the network protocol identifier as specified by [6] and is used to determine whether this is a CLNP packet, an ES-IS packet, etc. The received packet is then processed accordingly by the appropriate network layer protocol.

3.7.6.5 ICMP message handling

Note 1.— ICMP messages may be received by the IP SNDCF as a result of an error in the routing or delivery of previously sent packets. However, the receipt of an ICMP message for each and every such error cannot be guaranteed. Inter-organizational security policies may also prohibit the transfer of some or all ICMP messages between organizations. Nevertheless, appropriate handling of ICMP messages received by intermediate systems may improve their responsiveness.

Note 2.— Except when explicitly stated, the text below applies indifferently to ICMPv4 messages ([7]) and

ICMPv6 messages ([10]).

3.7.6.5.1.1 If a “destination unreachable” or “time exceeded” ICMP message is received by the IP SNDCF, this should be reported to a layer management function indicating the destination IP address for which the problem is reported, so that appropriate action may be taken.

Note.— Appropriate action includes, but is not restricted to, enabling an alternative adjacency.

3.7.6.5.1.2 An ICMP message indicating a “parameter problem” may indicate a software or configuration error, and this should be notified to layer management so that the error is noted and fixed by a network manager.

Note 1.— All other ICMP messages received by the IP SNDCF may be ignored.

Note 2.— ICMPv4 source quench messages are ignored as there is no obvious mechanism for passing this information back to the original sender. ATN messages are also assumed to be at a higher priority than other message types, in which case ignoring a source quench is a reasonable reflection of this fact. The IP network is itself not usually able to respect message priority.

Note 3.— ICMP echo requests are normally handled by the underlying system.

3.7.6.6 Resilient operation

3.7.6.6.1 When it has more than one interface to an IP network, an ATN system implementing the IP SNDCF shall rely upon the configuration, topology and management of an underlying IP subnetwork, including IP functions implemented by the ATN system itself, in order to support resilient operation.

Note 1.— An IP Internet can be configured and deployed with redundant data links and routers in order to meet the target requirements for availability, reliability and continuity of service. Honouring the “Type of Service” request and, in particular, the packet priority can also be used to maintain ATN service levels during drop of the IP subnetwork Quality of Service (i.e. the subnetwork encounters some failures). However, the IP addressing mechanism does not readily support multi-homed end systems. For such reasons, an ATN system that supports the IP SNDCF and has availability, reliability and continuity of service that cannot be met with a single interface to the IP network must also implement other functions (e.g. it may also need to be an IP router).

Note 2.— The guidance material discusses this issue in more depth and presents examples showing how resilient operation may be achieved.

3.7.6.6.2 Even if the ATN system has more than one interface to the IP network, a single IP address shall be used to support an adjacency with a given remote BIS.

Note 1.— This IP address may be a real one or a logical one.

Note 2.— This does not preclude the use of different IP addresses on the same ATN system for different adjacencies.

3.8 ROUTING INFORMATION EXCHANGE SPECIFICATION

3.8.1 Introduction

3.8.1.1 Scope

Note.— This chapter provides requirements and recommendations pertaining to the use of the ISO/IEC 10747 inter-domain routing protocol over air-ground and ground-ground data links, and the use of ISO/IEC 9542 in support of route initiation over air-ground data links. This chapter is concerned with the interoperability of protocol implementations and provides a compliance statement and APRL for each of the above protocols. It does not specify how routing information exchanged using ISO/IEC 10747 is used by routers when forwarding ISO/IEC 8473 NPDUs, or the application of routing policy controlling route aggregation and re-advertisement of routes. These subjects are covered in ¶3.3.

3.8.1.2 Applicability of requirements

3.8.1.2.1 All ATN airborne routers, with the exception of ATN airborne routers implementing the procedures for the optional non-use of IDRP, shall comply with the provisions contained in ¶3.8.2, ¶3.8.3, ¶3.8.3.2.2 to ¶3.8.3.2.5 inclusive, ¶3.8.3.2.8 to ¶3.8.3.2.9 inclusive, ¶3.8.3.2.11, ¶3.8.3.3.2.1, ¶3.8.3.3.3 and the APRLs specified for an airborne router in ¶3.8.3.5.

3.8.1.2.2 ATN airborne routers implementing the procedures for the optional non-use of IDRP shall be compliant with ¶3.8.2.

3.8.1.2.3 All ATN air-ground routers shall comply with the provisions contained in ¶3.8.2, ¶3.8.3, ¶3.8.3.2.2 to ¶3.8.3.2.9 inclusive, ¶3.8.3.2.11, ¶3.8.3.3.2.2, ¶3.8.3.3.3 and the APRLs specified for an air-ground router in ¶3.8.3.5.

3.8.1.2.4 All ground-ground inter-domain routers shall comply with the provisions contained in ¶3.8.2, ¶3.8.3.2.2 to ¶3.8.3.2.9 inclusive, ¶3.8.3.2.11, ¶3.8.3.3.2.2, ¶3.8.3.3.3 and the APRLs specified for a ground-ground router in ¶3.8.3.5.

3.8.1.2.5 All ATN routers, with the exception of airborne routers implementing the procedures for the optional non-use of IDRP, shall comply with the provisions contained in ¶3.8.3.2.10.1.

3.8.2 End system to intermediate system routing information exchange protocol (ES-IS) over mobile subnetworks

3.8.2.1 General

3.8.2.1.1 ATN airborne and air-ground routers directly connected to a mobile subnetwork (e.g. Mode S, AMSS or VDL) shall operate ISO/IEC 9542 over each such mobile subnetwork.

3.8.2.1.2 Configuration information shall be exchanged by both ATN air-ground and airborne routers over each mobile subnetwork connection supporting an adjacency between them.

Note.— The use of ISO/IEC 9542 configuration information over mobile subnetworks in support of air-ground route initiation is specified in ¶3.3.5.2.6.

3.8.2.1.3 ATN data link capabilities parameter

3.8.2.1.3.1 ATN air-ground and airborne routers shall include the ATN data link capabilities parameter in the options part of each ISO/IEC 9542 ISH PDU which they send over an ATN mobile subnetwork and evaluate the ATN data link capabilities parameter on reception.

Note 1.— The ATN data link capabilities parameter is used to inform the peer ATN router about the extended capabilities which are supported by the sending ATN router over the air-ground adjacency. The receiving ATN router will use this information to invoke those extended capabilities for use over the air-ground adjacency which are supported by both ATN routers forming the air-ground adjacency. This procedure supports backwards compatibility between ATN routers which may implement different editions of this specification.

Note 2.— The extended capabilities comprise those protocol features and capabilities which have been added to this specification beyond Edition 1 for use over the air-ground link.

Note 3.— The ATN data link capabilities parameter has to be sent over the air-ground adjacency even if its value field comprises all zeroes.

3.8.2.1.3.2 The ATN data link capabilities parameter shall not occur more than once in the options part of an ISO/IEC 9542 ISH PDU.

3.8.2.1.3.3 The ATN data link capabilities parameter shall consist of three fields, as illustrated Figure 3-22.

ATN data link capabilities parameter code	ATN data link capabilities parameter length	ATN data link capabilities parameter value
Octet 1	2	3 ..... end

Figure 3-22. The ATN data link capabilities parameter

3.8.2.1.3.4 *Encoding of the ATN data link capabilities parameter*

3.8.2.1.3.4.1 The ATN data link capabilities parameter code field shall be one octet in length.

3.8.2.1.3.4.2 The ATN data link capabilities parameter code field shall always be encoded as binary [1000 1000] to indicate the ATN data link capabilities parameter.

Note.— The above parameter code and its associated semantics are defined by this specification for the ATN in addition to the parameter codes specified by ISO/IEC 9542. ISO/IEC 9542 only uses eight bit parameter codes with bits 8 and 7 set to one and has reserved a parameter code of 255 for possible future extensions. The future use of the above ATN parameter code by an ISO standard cannot be ruled out but is highly unlikely.

3.8.2.1.3.4.3 The ATN data link capabilities parameter length field shall be one octet long.

3.8.2.1.3.4.4 The ATN data link capabilities parameter length field shall define the length in octets of the ATN data link capabilities parameter value field.

3.8.2.1.3.4.5 ATN data link capabilities parameter value field

Note.— The ATN data link capabilities parameter value field identifies the extended capabilities which are

supported over the air-ground adjacency by the ATN router issuing the ISO/IEC 9542 ISH PDU.

3.8.2.1.3.4.5.1 The ATN data link capabilities parameter value field shall comprise a bit map, where bit 0 is the low order bit.

3.8.2.1.3.4.5.2 The assignment of bits in the ATN data link capability parameter value field and the semantic of each bit shall be according to Table 3-26.

Table 3-26. Bit assignment and semantic of data link capabilities parameter value field

Bit Position	*Value*	*Semantic*
0	1 0	UPDATE PDUs without air-ground subnetwork type security tag supported UPDATE PDUs without air-ground subnetwork type security tag not supported
1	0 / 1	Not currently used
2	0 / 1	Not currently used

Note.— By setting bit 0 to one an airborne router which supports the use of IDRP for the exchange of routing information (i.e. a Class 6 airborne router) indicates its capability to receive and process UPDATE PDUs without air-ground subnetwork type security tag(s). In this case, the airborne router must be in a position to use mobile subnetwork-specific information received during air-ground route initiation (see 3.3.5.2.6.7) to update its FIB, Loc_RIB and relevant Adj_RIB-Outs. By setting bit 0 to one an air-ground router indicates its capability to generate and forward UPDATE PDUs without air-ground subnetwork type security tag(s) across the mobile adjacency.

3.8.2.1.3.4.5.3 The remaining bits of the ATN data link capabilities parameter value field are reserved for future use by this specification and shall be set to zero by the sending ATN router and ignored on reception.

3.8.2.1.3.5 When an ATN air-ground or airborne router recognizes an ATN data link capabilities parameter in a received ISO/IEC 9542 ISH PDU, then it shall determine from the parameter value field the extended capabilities supported by the sending ATN router.

Note.— Backwards compatibility is a goal of all editions of this specification, and this mechanism is used to determine whether features defined in later editions of this specification can be used in communications with the remote ATN systems.

3.8.2.1.3.6 The receiving ATN router, having determined the extended capabilities of the sending ATN router, shall invoke and use in further communications with this ATN router only those extended capabilities which are supported by both ATN routers.

3.8.2.1.4 Mobile subnetwork capabilities parameter

3.8.2.1.4.1 ATN air-ground and airborne routers shall support the mobile subnetwork capabilities parameter in the options part of an ISO/IEC 9542 ISH PDU.

3.8.2.1.4.2 The mobile subnetwork capabilities parameter shall be used in the ATN to convey information about the ATSC class and the traffic type(s) supported by an ATN mobile subnetwork.

3.8.2.1.4.3 The mobile subnetwork capabilities parameter shall consist of three fields, as illustrated in Figure 3-23, and shall not occur more than once in the options part of an ISO/IEC 9542 ISH PDU.

Subnetwork capabilities parameter code	Subnetwork capabilities parameter length	Subnetwork capabilities parameter value
Octet 1	2	3 ... 4

Figure 3-23. The mobile subnetwork capabilities parameter

3.8.2.1.4.4 *Encoding of the mobile subnetwork capabilities parameter*

3.8.2.1.4.4.1 The mobile subnetwork capabilities parameter code field shall be one octet in length and shall always be encoded as binary [1000 0001] to indicate the mobile subnetwork capabilities parameter.

Note.— The above parameter code and its associated semantics are defined by this specification for the ATN in addition to the parameter codes specified by ISO/IEC 9542. ISO/IEC 9542 only uses eight bit parameter codes with bits 8 and 7 set to one and has reserved a parameter code of 255 for possible future extensions. The future use of the above ATN parameter code by an ISO standard cannot be ruled out but is highly unlikely.

3.8.2.1.4.4.2 The mobile subnetwork capabilities parameter length field shall be one octet long and shall define the length in octets of the mobile subnetwork capabilities parameter value field.

3.8.2.1.4.4.3 Mobile subnetwork capabilities parameter value field

3.8.2.1.4.4.3.1 The first octet of this field shall indicate the traffic type(s) allowed to pass over the air-ground subnetwork over which the ISO/IEC 9542 ISH PDU is exchanged.

3.8.2.1.4.4.3.2 This octet shall comprise a bit map, where each bit corresponds to a different traffic type.

3.8.2.1.4.4.3.3 The assignment of bits to traffic types shall be according to Table 3-30, where bit 0 is the low order bit.

3.8.2.1.4.4.3.4 Setting a bit to one shall indicate that the corresponding traffic type is allowed to pass over the air-ground subnetwork.

3.8.2.1.4.4.3.5 The semantics of bits 5 to 7 shall be reserved for future use and shall always be set to one.

Note 1.— A value of FFh is used to imply no restrictions.

Note 2.— The first octet of the mobile subnetwork capabilities parameter value field has the same encoding and semantics as the second octet of the air-ground subnetwork type security tag set of the IDRP security path attribute which is defined in 3.8.3.2.3.2.4 through 3.8.3.2.3.2.6.

3.8.2.1.4.4.3.6 If bit 0 of the first octet of the mobile subnetwork capabilities parameter value field is set to one, then this field shall contain a second octet which defines the ATSC class supported by that air-ground subnetwork.

Note.— Bit 0 of the first octet set to one indicates that the air-ground subnetwork is available to the ATN operational communications traffic type – Air traffic service communications traffic category.

3.8.2.1.4.4.3.7 If present, the second octet of the mobile subnetwork capabilities parameter value field shall be encoded according to Table 3-27.

Table 3-27. Encoding of supported ATSC class

Value	*ATSC Class*
0000 0001	A
0000 0010	B
0000 0100	C
0000 1000	D
0001 0000	E
0010 0000	F
0100 0000	G
1000 0000	H

Note.— ATSC Class "H" is the lowest class and Class "A" is the highest.

3.8.2.1.4.4.3.8 Those ATSC class values which are not defined in Table 3-27 shall be reserved for future use by this specification.

3.8.2.1.5 Route redirection information shall not be exchanged between an ATN air-ground and airborne router.

3.8.2.2 ATN protocol requirements list — ISO/IEC 9542

An implementation of the ISO/IEC 9542 protocol shall be used in ATN airborne and air-ground routers, if and only if its PICS is in compliance with the APRL given in Table 3-28.

Table 3-28. ISO/IEC 9542 — Intermediate system

Item	*Protocol function*	*Clauses*	*ISO status*	*ATN support*
CI	Is configuration information supported over the associated subnetwork?	ATN Ref.: 3.8.2	O	M
RI	Is redirection information supported over the associated subnetwork?	ATN Ref.: 3.8.2	O	OX
	Are the following functions supported?			
ErrP	Protocol error processing	6.13	M	M
HCsV	PDU header checksum validation	6.12	M	M

Item	*Protocol function*	*Clauses*	*ISO status*	*ATN support*
HCsG	PDU header checksum generation	6.12	O	O
RpCf	Report configuration	6.2, 6.2.2	CI:M	M
RcCf	Record configuration	6.3, 6.3.1	CI:M	M
FlCf	Flush old configuration	6.4	CI:M	M
RqRd	Request redirect	6.8	RI:M	OX
CfNt	Configuration notification	6.7	CI:O	OX
CTGn	ESCT generation	6.3.2	CI:O	OX
AMGn	Address mask (only) generation	6.8	RI:O	OX
SMGn	Address mask and SNPA mask generation	6.8	RI:O	OX
	Are the following PDUs supported?			
ESH-r	<r> end system hello	7.1, 7.5	CI:M	O
ISH-r	<r> intermediate system hello	7.1, 7.6	CI:M	M
ISH-s	<s> intermediate system hello	7.1, 7.6	CI:M	M
RD-s	<s> redirect	7.1, 7.7	RI:M	OX
RD-r	<r> (ignore) redirect	6.9, 7.1, 7.7	M	M
	Are the following PDU fields supported?			
FxPt	<s> fixed part <r> fixed part	7.2.1, 7.2.7 7.2.1, 7.2.7	M M	M M
SA-r	<r> source address, one or more NSAPs	7.3.1/2/3	CI:M	ESH-r:M
NET-s	<s> network entity title	7.3.1/2/4	M	M
NET-r	<r> network entity title	7.3.1/2/4	ISH-r:M	ISH-r:M
DA-s	<s> destination address	7.3.1/2/5	RI:M	OX
BSNPA-s	<s> subnetwork address	7.3.1/2/6	RI:M	OX
Scty-s	<s> security	7.4.2	O	O
Scty-r	<r> security	7.4.2	O	O
Pty-s	<s> priority	7.4.3	O	O
Pty-r	<r> priority	7.4.3	O	O
QoSM-s	<s> QOS maintenance	7.4.4	RI:O	OX

Item	*Protocol function*	*Clauses*	*ISO status*	*ATN support*
AdMk-s	<s> address mask	7.4.5	RI:O	OX
SNMk-s	<s> SNPA mask	7.4.6	RI:O	OX
DLC-s	<s> data link capabilities	ATN Ref: §3.8.2.1.3	—	ISH-s:M
DLC-r	<r> data link capabilities	ATN Ref: §3.8.2.1.3	—	ISH-r:M
MSNC-s	<s> mobile subnetwork capabilities	ATN Ref: §3.8.2.1.4, §3.3.5.2.6.5	—	ISH-s and AGR:M
MSNC-r	<r> mobile subnetwork capabilities	ATN Ref: §3.8.2.1.4, §3.3.5.2.6.9	—	ISH-r and ABR:M
ESCT-s	<s> suggested ES configuration timer	7.4.7	CI:O	OX
ESCT-r	<r> (ignore) suggested ES configuration timer	7.4.7	ISH-r:M	ISH-r:M
OOpt-r	<r> (ignore) unsupported or unknown options	7.4.1	M	M
OOpt-s	<s> other options		P	P

	Parameter ranges				
HTv	What range of values can be set for the holding time field in transmitted PDUs ?	ATN Ref.: §3.3.5.2.9	M	M	from: 0 seconds to: 65 535 seconds with a tolerance of: 10%
CTv	If configuration information is supported, what range of values can be set for the configuration timer ?	ATN Ref.: §3.3.5.2.5	CI:M	M	from: 0 seconds to: 65 535 seconds with a tolerance of: 10%

AGR: If the intermediate system is an ATN air-ground router, **then** AGR is true, **else** AGR is false.

ABR: If the intermediate system is an ATN airborne router, **then** ABR is true, **else** ABR is false.

Note 1.— In the case where IDRP is used over the air-ground link, the holding time field of transmitted ISH PDUs is preferably set to 65 534 seconds as recommended in §3.3.5.2.10.9. The purpose of this recommendation is to effectively suppress the regular generation of ISH PDUs on the air-ground link.

Note 2.— In the case where the procedures for the optional non-use of IDRP are used on the air-ground link, the holding time field of the transmitted ISH PDUs and the configuration timer are set appropriately based on operational experience so that the exchange of ISH PDUs ensures a regular update of the respective FIBs in both the

air-ground and airborne routers, without overloading the air-ground link.

Note 3.— The classification "OX" indicates optional to implement, precluded to use.

3.8.3 Intermediate system to intermediate system inter-domain routing information exchange protocol

3.8.3.1 General

With the exception of airborne routers that implement the procedures for the optional non-use of IDRP, ATN routers shall implement ISO/IEC 10747, including the ATN specific features specified in this section, and the APRLs specified in 3.8.3.5.

3.8.3.2 ATN specific features

3.8.3.2.1 Purpose of ATN specific features

Note.— The ATN specific features specified in the following subsections support user requirements concerned with:

a) ensuring that application data passed over air-ground data links conform with any national and/or ITU restrictions applicable to that air-ground data link;

b) ensuring that a classification scheme can be applied to routes throughout the ATN ground environment, reflecting the expected QoS available over each such route;

c) ensuring that information on air-ground subnetwork types that a route passes over is available for determining which route to choose for a given application's data;

d) ensuring that changes to routing information that report negative changes (e.g. a downgrading of the classification of a route) are reported in a timely manner;

e) ensuring that routing information is received from an authentic source.

3.8.3.2.2 Use of the security path attribute

3.8.3.2.2.1 ATN routers supporting inter-domain routing shall support the IDRP security path attribute with a security registration identifier set to the value defined in 3.6.2.2.6 for the ATN security registration identifier.

3.8.3.2.2.2 The security information provided with a so identified IDRP security path attribute shall consist of zero, one or more security tag sets as defined in 3.6.2.2.6.

3.8.3.2.2.3 The following security tag sets shall be supported:

a) the air-ground subnetwork type, as defined in 3.8.3.2.3.2; and

b) the ATSC class, as defined in 3.8.3.2.3.3.

3.8.3.2.2.4 When an ATN router supports data classified according to a security policy and for the purpose of implementing mandatory access controls, then the ATN router should also support the security classification security tag set defined in 3.6.2.2.6.

3.8.3.2.2.5 When a route is available over more than one air-ground subnetwork type, then a separate security tag set shall be encoded into this field to identify each air-ground subnetwork that may support the route.

3.8.3.2.2.6 When an air-ground subnetwork is restricted to carrying data of only certain traffic types, then the security tag set that identifies that air-ground subnetwork shall enumerate the traffic types that may pass over that subnetwork.

3.8.3.2.2.7 At most one ATSC class security tag set shall be present in a route's security path attribute.

3.8.3.2.2.8 An ATSC class security tag set shall not be present when one or more air-ground subnetwork type security tag sets are also present, and when none of these air-ground subnetwork type security tag sets indicates support of ATN operational communications traffic type — air traffic service communications traffic category.

3.8.3.2.3 Encoding of the security path attribute security information field

3.8.3.2.3.1 *General*

The security path attribute security information field shall comprise zero, one or more security tag sets as defined in 3.6.2.2.6.

Note.— The security tag set format defined for use with CLNP in 3.6 has been adopted here as a convenient method for the extensible encoding of security-related information.

3.8.3.2.3.2 *Encoding of the air-ground subnetwork type security tag set*

3.8.3.2.3.2.1 The tag set name of the air-ground subnetwork type security tag set shall be set to [0000 0101], and the security tag shall always be two octets in length.

3.8.3.2.3.2.2 The first (lowest numbered) octet of the security tag shall define the air-ground subnetwork type over which the route may be available according to Table 3-29.

Table 3-29. Air-ground subnetwork type security tag values

Subnetwork type	*Security tag (1st Octet)*
Mode S	0000 0001
VDL	0000 0010
AMSS	0000 0011
Gatelink	0000 0100
HF	0000 0101

3.8.3.2.3.2.3 Those air-ground subnetwork type security tag values which are not defined in Table 3-29 shall be reserved for future use by this specification.

3.8.3.2.3.2.4 The second (highest numbered) octet of the security tag shall indicate the traffic types allowed to pass over

the air-ground subnetwork identified in the first octet.

3.8.3.2.3.2.5 This octet shall comprise a bit map, where each bit corresponds to a different traffic type. A value of FFh shall be used to imply no restrictions.

3.8.3.2.3.2.6 The assignment of bits to traffic type shall be according to Table 3-30, where bit 0 is the low order bit:

Table 3-30. Identification of permissible traffic types

Bit Number	*Traffic Type*
0	ATN operational communications — Air traffic service communications
1	ATN operational communications — Aeronautical operational control
2	ATN administrative communications
3	General communications
4	ATN systems management communications

3.8.3.2.3.2.7 The semantics of bits 5 to 7 shall be reserved for future use and shall always be set to one.

3.8.3.2.3.3 *Encoding of the ATSC class security tag set*

3.8.3.2.3.3.1 The tag set name of the ATSC class security tag set shall be set to [0000 0110] if the associated route is available to both ATSC and non-ATSC traffic.

3.8.3.2.3.3.2 The tag set name of the ATSC class security tag set shall be set to [0000 0111] if the associated route is available to ATSC traffic only.
3.8.3.2.3.3.3 The security tag shall always be one octet in length.

3.8.3.2.3.3.4 If a security tag with one of these tag set names is received which is longer than one octet, then all octets after the first octet shall be ignored.

3.8.3.2.3.3.5 When a security tag with one of these tag set names is present, the security tag shall identify the ATSC class(es) supported by the route.

3.8.3.2.3.3.6 The ATSC class(es) supported shall be identified according to Table 3-31, where bit 0 is the low order bit, and setting a bit to one shall indicate that the corresponding ATSC class is supported.

3.8.3.2.3.3.7 A bit set to zero shall indicate that the corresponding ATSC class is not supported.

Table 3-31. Identification of supported ATSC classes

Bit Number	*ATSC Class*
0	A

Bit Number	*ATSC Class*
1	B
2	C
3	D
4	E
5	F
6	G
7	H

3.8.3.2.4 Update of security information

3.8.3.2.4.1 *The air-ground subnetwork type*

3.8.3.2.4.1.1 When a route which contains a security path attribute and has the ATN security policy identifier as the security path attribute's security registration identifier is either:

a) received by an air-ground router from an airborne router;

or

b) advertised by an air-ground router to an airborne router which has not signaled its capability to receive and process UPDATE PDUs without air-ground subnetwork type security tag(s).

Note.— An ATN airborne router signals its capability to receive and process UPDATE PDUs without air-ground subnetwork type security tag(s) by using the ATN data link capability parameter (see 3.8.2.1.3) contained in the options part of downlinked ISH PDU(s).

Then the security path attribute's security information shall be updated as follows:

1) unless not already contained in the security information, an air-ground subnetwork type security tag shall be added for each air-ground subnetwork supporting the adjacency between the air-ground and airborne router;

2) for each air-ground subnetwork type security tag present in or added to the route, if ITU requirements or local policies restrict the traffic types that may pass over that subnetwork then the second octet of the security tag shall be modified to set to zero the bits corresponding to each traffic type not supported by that air-ground subnetwork.

Note 1.— According to the procedures specified in 3.3.5.2.12 for the optional non-use of IDRP over an air-ground data link, this update of the security information also includes routes which have been originated by an air-ground router on behalf of an airborne router not implementing IDRP.

Note 2.— ITU or local policy restriction(s) on the traffic type(s) that may pass over the mobile subnetwork are known to the air-ground router from local configuration information.

3.8.3.2.4.1.2 When a route containing one or more air-ground subnetwork tags is advertised over an adjacency that supports only ATSC traffic, the air-ground subnetwork tags shall be updated such that the second octet of the security tag shall be modified to set to zero the bits corresponding to all traffic types other than ATSC.

3.8.3.2.4.1.3 Any air-ground subnetwork security tags with a second octet that is all zeroes shall be removed from the route.

3.8.3.2.4.1.4 If all air-ground subnetwork security tags present have a zero second octet then the route shall not be advertised over this adjacency.

3.8.3.2.4.2 *The ATSC class*

3.8.3.2.4.2.1 When a route is advertised to an adjacent ground or air-ground BIS or to an adjacent airborne BIS which has not signalled its capability to support UPDATE PDUs without air-ground subnetwork type security tag (see ⁋3.8.2.1.3) then:

a) if the route has been originated by an air-ground router according to the procedures for the optional non-use of IDRP (as specified in ⁋3.3.5.2.12), and the adjacency with the airborne router is over an air-ground data link approved for ATSC use, then an ATSC class security tag shall be added to the route identifying the ATSC class(es) supported by the adjacency with that airborne router;

b) if the route had been received from an airborne router by an air-ground router, over an air-ground data link approved for ATSC use, then an ATSC class security tag shall be added, replacing any that may already be present, identifying the ATSC class(es) supported by the adjacency with that airborne router;

c) if the route:

1) has been originated locally (i.e. within the same routing domain) by a router other than an airborne router; and

2) is required by the local security policy to be available for ATSC traffic; and

3) is to be advertised to an adjacent BIS over an adjacency supported by one or more subnetworks approved for ATSC traffic; then

an ATSC class security tag shall be added to the route which identifies the ATSC class(es) supported by the route, as defined by the local security policy, and the ATSC class(es) of the route shall be downgraded, as specified in ⁋3.8.3.2.4.2.5, to the ATSC class(es) supported by the adjacency.

Note 1.— A route to a mobile RD's home and a route to all AINSC and ATSC mobiles are two specific examples of routes falling within this category. According to ⁋3.3.7.1.2.1 e), ⁋3.3.7.1.5.1 c), ⁋3.3.7.3.2.1 d) and ⁋3.3.7.1.3.1 c), these routes are defined to be available for any kind of air-ground data traffic and supporting all ATSC classes. However, when these routes are to be advertised to an adjacent BIS, the ATSC class security tag of these routes must be downgraded to signal the support of all ATSC classes except those not supported by the adjacency.

Note 2.— In the case of an airborne router, the ATSC class is inserted by the air-ground router (see case (b) above), and this avoids an airborne router having to know which air-ground data links are approved for ATSC use.

d) if the route:

1) has been received from another BIS; and

2) is to be advertised to an adjacent BIS over an adjacency supported by one or more subnetworks approved for ATSC traffic; and

3) has an ATSC class security tag that is higher than the ATSC class that the system administrator has specified as being supported by the adjacency; then

the ATSC class of the route shall be downgraded, as specified below, to the ATSC class supported by the adjacency;

e) if the route:

1) has been received from another BIS; and

2) is to be advertised to an adjacent BIS over an adjacency supported by subnetworks that are not approved for ATSC traffic; then

the ATSC class security tag shall be removed from the route before it is advertised to the adjacent BIS;

f) if the route:

1) has been received from an air-ground BIS by an airborne BIS over an adjacency supported by one or more subnetworks approved for ATSC traffic; and

2) includes an ATSC class security tag; then

the ATSC class(es) of the route shall be downgraded, as specified below, to the ATSC class(es) supported by the adjacency.

Note.— The airborne BIS knows the ATSC class(es) supported by the adjacency from the information contained in the mobile subnetwork capability parameter of the ISH PDU(s) received from the adjacent air-ground BIS.

g) if the route:

1) has been received from an air-ground BIS by an airborne BIS over an adjacency supported by subnetworks that are not approved for ATSC traffic; and

2) includes an ATSC class security tag; then

the ATSC class security tag shall be removed from the route.

3.8.3.2.4.2.2 When an ATSC class security tag is added to a route, then the value of the tag set name shall be set according to 3.8.3.2.3.3 and depending upon whether the adjacency has been specified to support ATSC traffic only or both ATSC and non-ATSC traffic.

3.8.3.2.4.2.3 When the ATSC class security tag indicating support for both ATSC and non-ATSC traffic is updated then the tag set name shall be changed to that indicating support for ATSC only traffic if the adjacency is specified to support only ATSC traffic.

3.8.3.2.4.2.4 In all other cases, the ATSC class security tag name shall not be modified.

Note.— The tag set name is set to [0000 0110] when both ATSC and non-ATSC traffic is supported, and to [0000 0111] when only ATSC traffic is supported.

3.8.3.2.4.2.5 When the ATSC class is downgraded, the ATSC class security tag set shall be modified such that all bits indicating support for an ATSC class higher than that supported by the local policy shall be set to zero, and the bit corresponding to the highest ATSC class supported by local policy shall be set to one. All remaining bits shall be unaffected.

3.8.3.2.4.2.6 When an ATSC class security tag indicating support for ATSC only is present in a route, an air-ground subnetwork security tag when present in the same route shall not indicate support for any traffic type other than ATSC.

3.8.3.2.4.2.7 When a route is advertised by an air-ground BIS to an adjacent airborne BIS which has signalled its capability to support UPDATE PDUs without air-ground subnetwork type security tag (see 3.8.2.1.3), then:

a) if the route has been originated locally (i.e. within the same routing domain) and is required by the local security policy to be available for ATSC traffic, then an ATSC class security tag shall be added to the route which identifies the ATSC class(es) supported by the route, as defined by the local security policy, without being downgraded to the ATSC class(es) temporarily supported by the adjacency;

b) if the route has been received from another BIS, the ATSC class security tag shall not be modified.

3.8.3.2.4.3 *The security classification*

3.8.3.2.4.3.1 When it is required by the local security policy that:

a) the router supports classified data; and

b) a route is advertised to an adjacent BIS; and

c) the highest level of protection offered by the subnetworks supporting the adjacency is lower than that reported by a security classification security tag;

then that security tag shall be replaced by a security classification security tag reporting the highest protection offered by those subnetworks, as specified in the applicable security policy.

3.8.3.2.5 Route selection

Note.— ISO/IEC 10747 clause 7.16.2 permits a Loc-RIB that is identified by a RIB_Att containing the security path attribute to contain more than one route to the same NLRI, provided that those routes provide the same level of protection.

3.8.3.2.5.1 When the security registration identifier in the IDRP security path attribute is the ATN security registration identifier, and when no security classification is present in the route's security information, then all such routes shall be assumed to offer the same level of protection.

Note.— The purpose of this statement is to permit, within the limitations imposed by ISO/IEC 10747, the existence in the Loc-RIB of multiple routes to the same aircraft which differ in the security-related information.

3.8.3.2.5.2 During the Phase 2 routing decision process, when:

a) two or more routes to the same or overlapping destination are found in the Adj-RIB-Ins identified by a RIB_Att that includes the security path attribute, but which differ in the security information contained

in their security path attribute, then all such routes shall be selected and copied to the corresponding Loc-RIB.

b) two routes are found in the Adj-RIB-Ins identified by a RIB_Att that includes the security path attribute, which differ in the security information contained in their security path attribute, and when the NLRI of the less preferable route is a proper subset of the NLRI of the more preferable route, then only the more preferable route shall be copied to the corresponding Loc-RIB. Otherwise, both such routes shall be copied to the corresponding Loc-RIB.

3.8.3.2.6 Route aggregation and route information reduction

3.8.3.2.6.1 *General*

ATN routers shall implement the procedures for route aggregation and route information reduction when required to do so according to ¶3.8.3.2.6.2 through ¶3.8.3.2.6.5.

Note 1.— Route aggregation is defined by ISO/IEC 10747 as a procedure for the merging or aggregation of two routes in order to form a single replacement route. Route aggregation may be applied as the result of a routing policy decision in order to reduce the routing information advertised to an adjacent router. It is also necessary to aggregate two routes in the same Loc-RIB and with identical NLRI prior to being advertised to an adjacent router. This latter case of route aggregation is automatic, not subject to routing policy, and necessary for the proper dissemination of routing information.

Note 2.— Route information reduction is defined by ISO/IEC 10747 as a procedure for replacing two or more NSAP address prefixes in a route's NLRI by a single shorter NSAP address prefix. The decision on when to apply route information reduction is also subject to routing policy and is typically associated with the application of route aggregation when applied as a result of routing policy.

3.8.3.2.6.2 *Policy-based route aggregation*

3.8.3.2.6.2.1 An air-ground router should aggregate all routes to destinations in routing domains in its own ATN island, other than those to destinations in its own routing domain.

3.8.3.2.6.2.2 An air-ground router should aggregate all routes to destinations in ATN islands, other than those to destinations in its own ATN island.

3.8.3.2.6.2.3 ATN ground-ground routers should perform route aggregation and route information reduction on routes to ground destinations, in line with local policy requirements for reducing the amount of routing information distributed within the ATN ground environment.

Note.— The need for this will be determined according to local topology and NSAP address assignment and is outside of the scope of this specification. However, this feature is a necessary condition for the development of a large scale and scalable internet.

3.8.3.2.6.2.4 The selection of candidate routes for aggregation shall be performed separately for each adjacent BIS according to a filter on each route's destination, with a combination of inclusion and exclusion filters.

Note.— For example, filters might be applied in order to select all routes to NSAP address prefixes within the local ATN island, while excluding those to the local administrative domain.

3.8.3.2.6.3 *Aggregation of routes in the same Loc-RIB with identical NLRI*

3.8.3.2.6.3.1 When two or more routes exist in the same Loc-RIB which have identical NLRI, then such routes shall be aggregated after the application of local policy rules that select routes for re-advertisement to each adjacent BIS.

3.8.3.2.6.3.2 Such routes shall be consequently copied to the associated Adj-RIB-Out.

3.8.3.2.6.3.3 For each adjacent BIS, the resulting aggregated route shall be inserted into the associated Adj-RIB-Out.

3.8.3.2.6.3.4 In order to aggregate such routes, an ATN router shall apply one of the following two strategies:

a) **True route aggregation:** the routes are aggregated according to ISO/IEC 10747 route aggregation procedures and the procedures for aggregation of the security path attribute specified in 3.8.3.2.6.4.

b) **Route merging:** the routes are merged by arbitrarily selecting one of these routes and updating its security path attribute to the value that would have resulted had the routes been aggregated, as above. The selected route with its updated security path attribute is then the result of the merging procedure.

Note 1.— The former of the two strategies is preferred.

Note 2.— The second strategy has been introduced as an interim measure to simplify initial implementations. However, this second strategy leads to a situation where routing decisions based on RD_PATH information cannot be performed, as this information is lost in the merging process. The second strategy may therefore be deleted in a future revision of these detailed technical specifications.

Note 3.— Whenever local policy rules that select routes for advertisement to adjacent BISs select different combinations of routes from the same Loc-RIB and with identical NLRI, for advertisement to different adjacent BISs, then the route aggregation or merging procedure has to be carried out separately for each Adj-RIB-Out. For each Adj-RIB-Out, only those routes which are eligible for advertisement to the corresponding BIS will be input to the merging/aggregation procedure. For example, a route may not be eligible for advertisement to an adjacent BIS due to distribution restrictions or a potential route loop recognized from the RD_PATH information.

Note 4.— An aggregated route resulting from these procedures may also be aggregated with other routes in an Adj-RIB-Out, due to the application of local policy rules.

3.8.3.2.6.4 *Aggregation of the security path attribute information field*

3.8.3.2.6.4.1 General

3.8.3.2.6.4.1.1 ATSC and non-ATSC routes with dissimilar NLRI shall not be aggregated.

Note 1.— An ATSC route is a route containing an ATSC class security tag in its security path attribute. A non-ATSC route is similarly a route that does not contain an ATSC class security tag in its security path attribute.

Note 2.— Two possible strategies for aggregating such routes were considered. However, neither gave a satisfactory outcome. This is because the aggregated route must either be identified as an ATSC route or a non-ATSC route. If the aggregated route is identified as a non-ATSC route, then this would result in ATSC routes being "hidden" when aggregated with non-ATSC routes. On the other hand, if the aggregated route is identified as an ATSC route, then this would result in a situation where an aggregated route that was apparently approved for ATSC traffic included a destination which could not be reached over a path that was approved end-to-end for ATSC traffic. This runs the risk of creating a "black hole" for ATSC traffic.

3.8.3.2.6.4.1.2 Similarly, routes available to ATSC traffic only and routes available to both ATSC and non-ATSC

traffic with dissimilar NLRI shall not be aggregated.

3.8.3.2.6.4.1.3 Otherwise, the aggregation rules for the security information field contained in security path attributes that include the ATN security registration Identifier shall be as follows.

3.8.3.2.6.4.2 Air-ground subnetwork security tag

3.8.3.2.6.4.2.1 The aggregated security path attribute shall comprise each air-ground subnetwork security tag contained in the security path attribute of the component routes.

3.8.3.2.6.4.2.2 When an air-ground subnetwork type security tag for the same air-ground subnetwork type occurs in more than one component route, then these shall be combined by a logical “OR” of the second octet of the air-ground subnetwork type security tags.

3.8.3.2.6.4.2.3 Only a single air-ground subnetwork type security tag for each distinct air-ground subnetwork type shall be present in the aggregated route.

3.8.3.2.6.4.3 ATSC class security tag

3.8.3.2.6.4.3.1 General

If an ATSC class security tag is not present in any component route, then the aggregated route shall not contain an ATSC class security tag.

3.8.3.2.6.4.3.2 Non-identical NLRI in component routes

3.8.3.2.6.4.3.2.1 If the NLRI of the component routes is not identical then, when an ATSC class security tag with the same tag set name occurs in all component routes, the aggregated route shall contain an ATSC class security tag with the same tag set name.

3.8.3.2.6.4.3.2.2 The ATSC class of the aggregated route shall be the lowest ATSC class of the aggregated route’s component routes, indicated by setting the value of the corresponding bit in the security tag value to one.

3.8.3.2.6.4.3.2.3 All the other bits in this tag shall be set to zero.

3.8.3.2.6.4.3.3 Identical NLRI in component routes

3.8.3.2.6.4.3.3.1 If the NLRI of the component routes is identical then, when an ATSC class security tag occurs in one or more component routes then the aggregated route shall contain an ATSC class security tag.

3.8.3.2.6.4.3.3.2 If an ATSC class tag set occurs in all component routes and the ATSC class tag set names in all such tag sets are identical, then the tag set name of the aggregated route shall be the same as in the component routes.

3.8.3.2.6.4.3.3.3 If the ATSC class tag set names in the component routes are different, or one or more component routes do not include an ATSC class security tag, then the ATSC class security tag set in the aggregated route shall use the tag set name that indicates that the route is available for both ATSC and non-ATSC traffic.

Note.— This tag set name is defined by 3.8.3.2.3.3.1 to take the value [0000 0110].

3.8.3.2.6.4.3.3.4 The ATSC class of the aggregated route shall be formed by a logical “OR” of the encoded representation of the supported ATSC class in each of the aggregated route’s component routes that contains an ATSC class security tag.

3.8.3.2.6.4.3.3.5 If none of the component routes contains an ATSC class security tag, then the aggregated route shall not contain an ATSC class security tag.

3.8.3.2.6.4.3.4 Security classification security tag

3.8.3.2.6.4.3.4.1 When a security classification security tag occurs in all component routes, then the aggregated route shall contain a security classification security tag.

3.8.3.2.6.4.3.4.2 This tag shall be set to the lowest classification from the classifications given to the aggregated route's component routes.

3.8.3.2.6.4.3.4.3 If a security classification security tag is not present in at least one component route then the aggregated route shall not contain a security classification security tag.

3.8.3.2.6.5 *Route information reduction*

3.8.3.2.6.5.1 An air-ground router should perform route information reduction as permitted by the ATN addressing plan, before advertising aggregated routes to an airborne router.

Note.— It is intended that the result of route information reduction is a single NSAP address prefix to each destination group to which aggregation is performed. However, this will only be possible if NSAP addresses have been allocated appropriately (e.g. all systems within the same ATN island have a single common prefix for all such addresses).

3.8.3.2.6.5.2 Route information reduction shall be performed using local policy rules, with such routing policy rules required to specify when a set of NSAP address prefixes is replaced by a shorter NSAP address prefix. Two types of rules shall be supported:

a) the explicit replacement of a set of NSAP address prefixes by another shorter NSAP address prefix, only when all members of the set are present; or

b) the explicit replacement of a set of NSAP address prefixes by another shorter NSAP address prefix when any members of the set are present.

3.8.3.2.7 Frequency of route advertisement

Note.— ISO/IEC 10747 clause 7.17.3.1 requires that the advertisement of feasible routes to some common set of destinations received from BISs in other routing domains must be separated in time by at least ***minRouteAdvertisementInterval*** *except for certain identified cases. The list of exceptions to this requirement is extended by this specification.*

3.8.3.2.7.1 If a selected route to a given destination changes in respect of the security information contained in its security path attribute, then that route shall be immediately re-advertised to all adjacent BISs to which that route had previously been advertised and not since withdrawn.

3.8.3.2.7.2 The procedure for ensuring a minimum time interval of minRouteAdvertisementInterval between successive advertisements of routes to the same destination shall not apply in this case.

3.8.3.2.8 Interpretation of route capacity

3.8.3.2.8.1 For the ATN environment, the CAPACITY path attribute shall contain one of the values listed in Table 3-32 and shall be assumed to have the semantics given there:

Table 3-32. Interpretation of capacity route metric

Value	*Meaning*
1 ... 9	Unassigned
13	0 – 19.2 Kbits/sec
12	19.2 – 56 Kbits/sec
11	56 – 1 500 Kbits/sec
10	> 1 500 Kbits/sec
14 .. 255	Unassigned

Note.— The CAPACITY path attribute is a well-known mandatory attribute that is used to denote the traffic handling capacity of the RD_PATH listed in the same UPDATE PDU. Higher values indicate a lower traffic handling capacity than do low values.

3.8.3.2.8.2 Those capacity route metric values which are not assigned in Table 3-32 shall be reserved for future use by this specification.

3.8.3.2.9 Network layer reachability information

3.8.3.2.9.1 *General*

3.8.3.2.9.1.1 In support of ATN communications, ATN routers shall encode the NLRI Addr_info field of each route as a list of NSAP address prefixes.

3.8.3.2.9.1.2 The proto_type, and proto_length fields shall be set to 1 and the protocol field shall be set to X'81' in order to signal support of ISO/IEC 8473.

3.8.3.2.9.2 *NSAP address prefix alignment*

When originating a route or performing route information reduction, an ATN router shall only generate NSAP address prefixes that are octet-aligned.

Note 1.— For IDRP, ATN NSAP address prefixes will be eleven octets (or less).

Note 2.— 3.8.3.2.12 specifies the RIB-Atts that an ATN router must support.

Note 3.— The above requirement does not modify the requirement in ISO/IEC 10747 to be able to accept and correctly handle a non-octet aligned NSAP address prefix.

Note 4.— The above requirement simplifies prefix matching.

3.8.3.2.10 BISPDU authentication

3.8.3.2.10.1 ATN routers shall support the validation of BISPDUs using authentication Type 1.

3.8.3.2.10.2 When an ATN router initiates a BIS-BIS connection, it shall set the value of the authentication code in the OPEN PDU to 1, in order to indicate that the validation field in the header of all BISPDU sent over the BIS-BIS connection will contain an unencrypted checksum.

3.8.3.2.10.3 When an authentication code of 1 is specified in the authentication code field of the OPEN PDU that initiated a BIS-BIS connection, then an ATN router shall generate a validation pattern according to clause 7.7.1 of ISO/IEC 10747, for each BISPDU that it sends over that connection and similarly validate the validation pattern of all received BISPDUs on such a connection.

3.8.3.2.10.4 The Type 1 authentication code shall be generated according to the MD4 specification published in RFC 1320.

Note 1.— The interpretation of MD4 given in Annex B of ISO/IEC 10747 is open to ambiguous interpretation and may lead to interoperability problems.

Note 2.— RFC 1320 supersedes RFC 1186 which was the basis for ISO/IEC 10747 Annex B. Specifications of MD4 algorithm contained in these two RFC documents are technically equivalent.

3.8.3.2.11 Restrictions on route advertisement

A route shall not be advertised to a BIS in another RD when:

a) the route contains the receiving RDs RDI in its RD_PATH path attribute; or

b) the route's RD_PATH path attribute contains the RDI of a routing domain confederation which is being entered when the route is advertised to the other RD.

Note.— This is essential to avoid long lived black holes following the explicit withdrawal of an unfeasible route and when many alternate paths are available (e.g. within an ATN island backbone RDC).

3.8.3.2.12 RIB_Att support

Table 3-34. ISO/IEC 10747 mandatory requirements, for which support is optional for ATN airborne routers

	ISO mandatory requirement	*Notes*
1.	Internal update procedures	*Note 1.— There is only ever a single BIS per routing domain on board an aircraft, and hence, internal update is not applicable.*
2.	Operation of **minRouteAdvertisementInterval** Timer	*Note 2.— An aircraft is always an end routing domain, and hence will never re-advertise routes.*
3.	Recognition of next hop attribute	*Note 3.— No requirement for support in the ATN.*
4.	Recognition of residual error, expense, transit delay and priority distinguishing path attributes	*Note 4.— Never negotiated for use in the ATN.*
5.	Support of RIB refresh	*Note 5.— RIB refresh is necessary for long lived adjacencies rather than the short lived adjacencies anticipated for ATN mobiles.*

ISO mandatory requirement	*Notes*
6. Support of DIST_LIST_EXCL	*Note 6.— There are no known user requirements to control the distribution of routes to or from mobile systems. Implementation may also be problematic due to changing point of attachment to the Fixed ATN.*
7. Support of partial source routing	*Note 7.— There are no known user requirements for partial source routing.*
8. Application of jitter on timers	*Note 8.— An aircraft is always an end routing domain. Hence it will not use the minRouteAdvertisementInterval timer (see 2. above). Furthermore it is unlikely to report changes in locally originated routes at the MinRDOriginationInterval rate, as this routing information does not usually change over the lifetime of a BIS-BIS connection.*

3.8.3.2.12.1 An ATN router incorporating IDRP shall support the following RIB_Att sets:

a) the empty RIB_Att;

b) SECURITY;

and shall attempt to negotiate the use of all those RIB_Atts it supports when opening a BIS-BIS connection.

3.8.3.2.12.2 The semantics of the empty RIB_Att shall be taken as implying that routes advertised under the empty RIB_Att:

a) have a classification of “Unclassified”;
b) have not passed over any mobile subnetworks; and
c) are not available to ATSC traffic.

3.8.3.2.13 Additional update PDU error handling

When an UPDATE PDU is received with a security path attribute containing an ATN security registration identifier and security information that contains:

a) an ATSC class security tag set; and

b) one or more air-ground subnetwork type security tag sets, such that none of these security tag sets indicates support of ATN Operational Communications — Air Traffic Service Communications, then the UPDATE PDU shall be discarded and an IDRP ERROR PDU generated with an Error_Code indicating an UPDATE_PDU_Error, and an error subcode set to 64.

3.8.3.2.14 CLNP data PDU parameters

The CLNP data PDU that carries a BISPDU between two ATN routers shall include:

a) a security parameter providing an ATN security label indicating a traffic type of “Systems Management”;

b) a priority parameter indicating a PDU priority of 14.

Note.— To ensure the exchange of ISO/IEC 10747 BISPDUs over an air-ground adjacency under the above traffic type classification, the air-ground router or airborne router respectively must be configured in a way that includes ATN systems management communications in the set of permissible traffic types allowed to pass over the air-ground subnetwork(s) forming the air-ground adjacency. Otherwise, an IDRP connection may not be established over the air-ground adjacency; consequently no CLNP PDUs will ever flow over it and the adjacency will be unusable.

3.8.3.2.15 Modified sequence number check on received OPEN BISPDU

3.8.3.2.15.1 An ATN router supporting ISO/IEC 10747 shall perform the sequence number check on received BISPDU as indicated in ISO/IEC 10747 clause 7.7.5 c) except on OPEN BISPDU.

3.8.3.2.15.2 An incoming OPEN BISPDU whose sequence corresponds to the next expected sequence number less one shall be discarded.

3.8.3.2.15.3 An incoming OPEN BISPDU whose sequence does not correspond to the next expected sequence number less one shall be accepted and passed to the finite state machine described on ISO/IEC 10747 clause 7.6.1.

Note.— This deviation from the base standard accommodates air-ground subnetworks that generate out of synch leave-events on air and ground sides (or even drop some leave events). The modified behaviour limits the persistence of a “single-ended” IDRP connection to the delay necessary for the other end to detect the IDRP connection loss and attempt its recovery.

3.8.3.3 Compliance with ISO/IEC 10747

3.8.3.3.1 General

The IDRP protocol exchange shall use the connectionless network service provided by ISO/IEC 8473, as specified in ISO/IEC 10747.

3.8.3.3.2 ISO/IEC 10747 mandatory requirements

3.8.3.3.2.1 *Airborne router*

An ATN airborne router supporting the ISO/IEC 10747 inter-domain routing protocol shall support all mandatory requirements as specified in clause 12.1 of ISO/IEC 10747 with the exception of the requirements listed in Table 3-34, for which support is optional.

Note.— This specification deviates from ISO/IEC 10747 for airborne routers, in order to simplify the specification of operational equipment by removing all non-applicable requirements.

3.8.3.3.2.2 *Ground router*

Note.— This section refers to both air-ground and ground-ground routers generically as ground routers.

3.8.3.3.2.2.1 An ATN ground router supporting the ISO/IEC 10747 inter-domain routing protocol shall support all mandatory requirements as specified in clause 12.1 of ISO/IEC 10747.

3.8.3.3.2.2.2 However, over adjacencies with airborne routers, ATN air-ground routers shall exclude the dynamic use of the following functions and features:

a) the next hop path attribute;

b) the DIST_LIST_EXCL path attribute;

c) RIB refresh request;

d) the residual error path attribute;

e) the expense path attribute;

f) the priority path attribute;

g) the transit delay path attribute;

h) the locally defined QoS path attribute;

i) hierarchical recording;

j) support of partial source routing.

3.8.3.3.3 ISO/IEC 10747 optional requirements

3.8.3.3.3.1 An ATN router shall support the security path attribute as specified in 3.8.3.2.2 and 3.8.3.2.3.

3.8.3.3.3.2 An ATN air-ground router should implement route aggregation and route information reduction procedures.

3.8.3.3.3.3 An ATN ground-ground router should implement route aggregation and route information reduction procedures.

3.8.3.4 KeepAlive timer

3.8.3.4.1 Air-ground routers and airborne routers (i.e. Router Classes 5 and 6) should utilize initial keepAlive timer values on air-ground BIS-BIS connections as shown in Table 3-35:

Table 3-35. KeepAlive timer values on air-ground BIS-BIS connections

Router capability	*Nominal keepAlive value*
AMSS and/or HFDL	180 minutes
Mode S and/or VDL only	30 minutes

Note 1.— Choice of nominal keepAlive timer value is based on the longest adjacency equipage.

Note 2.— The leave event is the primary means of reporting the loss of connectivity on air-ground adjacencies. A lost leave event in AMSS is trapped by the timer event, and routing tables are thus cleared.

3.8.3.4.2 Ground-ground routers and air-ground routers (i.e. Router classes 4 and 5) should utilize initial keepAlive timer values in the range of 5 to 60 seconds on ground-ground BIS-BIS connections.

3.8.3.4.3 Air-ground and airborne router implementations (i.e. Router Classes 5 and 6) shall implement the capability of different timer values on separate BIS-BIS connections.

Note.— ISO/IEC 10747 section 11.4 in the definition of the adjacentBISPkg-P PACKAGE requires each BIS-BIS connection to operate a separate hold and keepAlive timer.

3.8.3.5 APRLs

3.8.3.5.1 General

An implementation of the ISO/IEC 10747 protocol shall be used in ATN routers if and only if its PICS is in compliance with the APRLs specified in the following sections.

Note.— The IDRP requirements list is a statement of which capabilities and options of the protocol at minimum are required to be implemented for the ATN environment. The requirements list may be used by the protocol implementor as a checklist to conform to this standard; by the supplier and procurer to provide a detailed indication of the capabilities of an implementation; by the user to check the possibility of interworking between two different implementations; and by the protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance to the protocol.

3.8.3.5.2 ATN specific protocol requirements

Item	*Description*	*ATN Ref*	*G-G router*	*A/G router*	*Airborne router*
ATNIDRP1	Does this BIS encode and use the security path attribute?	3.8.3.2.2, 3.8.3.2.3	M	M	M
ATNIDRP2	Does this BIS immediately re-advertise routes if the security information contained in the route's security path attribute changes?	3.8.3.2.7	M	M	—
ATNIDRP3	Does this BIS support "policy based route aggregation"?	3.8.3.2.6.2	O	O	—
ATNIDRP4	Does this BIS support "policy based route information reduction"?	3.8.3.2.6.5	O	O	—
ATNIDRP5	Does this BIS support aggregation of routes with identical NLRI using "true route aggregation"?	3.8.3.2.6.3	O.1	O.1	—
ATNIDRP6	Does this BIS support aggregation of routes with identical NLRI using "route merging"?	3.8.3.2.6.3	O.1	O.1	—

Item	Description	ATN Ref	G-G router	A/G router	Airborne router
ATNIDRP7	Does this BIS support aggregation of security path attribute information field?	3.8.3.2.6.4	M	M	—

3.8.3.5.3 IDRP general

Item	Description	ISO/IEC 10747 Ref.	ISO status	G-G router	A/G router	Airborne router
BASIC	Are all basic BIS functions implemented?	12.1	M	M	M	M
MGT	Is this system capable of being managed by the specified management information?	11	M	O	O	O
VER	Does this BIS support version negotiation?	7.8	M	M	M	M
RTSEP	Does this BIS support the ROUTE_SEPARATOR attribute?	7.12.1	M	M	M	M
HOPS	Does this BIS support the RD_HOP_COUNT attribute?	7.12.13	M	M	M	M
PATH	Does this BIS support the RD_PATH attribute?	7.12.3	M	M	M	M
CAPY	Does this BIS support the capacity attribute?	7.12.15	M	M	M	M
FSM	Does this BIS manage BIS-BIS connections according to the BIS FSM description?	7.6.1	M	M	M	M
FCTL	Does this BIS provide flow control?	7.7.5	M	M	M	M
SEQNO	Does this BIS provide sequence number support?	7.7.4	M	M	M	M
INTG1	Does this BIS provide data integrity using authentication Type 1?	7.7.1	O.1	M	M	M
INTG2	Does this BIS provide data integrity using authentication Type 2?	7.7.2	O.1	O	O	O
INTG3	Does this BIS provide data integrity using authentication Type 3?	7.7.3	O.1	O	O	O

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
ERROR	Does this BIS handle error handling for IDRP?	7.20	M	M	M	M
RIBCHK	Does this BIS operate in a “fail-stop” manner with respect to corrupted routing information?	7.10.2	M	M	M	M

Note.— The interpretation of the Item MGT is that mandatory compliance requires that access to the MO is provided via a systems management agent. Remote systems management is not currently required and hence it is not reasonable to require mandatory support for this requirement.

3.8.3.5.4 *IDRP update send process*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
INT	Does the BIS provide the internal update procedures?	7.17.1	M	M	M	O
RTSEL	Does this BIS support the MinRouteAdvertisementInterval timer (except in the case specified in ATNIDRP2)?	7.17.3.1	M	M	M	O
RTORG	Does this BIS support the MinRDOriginationInterval timer?	7.17.3.2	M	M	M	M
JITTER	Does this BIS provide jitter on its timers?	7.17.3.3	M	M	M	O

3.8.3.5.5 *IDRP update receive process*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
INPDU	Does the BIS handle inbound BISPDUs correctly?	7.14	M	M	M	M
INCONS	Does this BIS detect inconsistent routing information?	7.15.1	M	M	M	INT:O

3.8.3.5.6 *IDRP decision process*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
TIES	Does this BIS break ties between candidate routes correctly?	7.16.2.1	M	M	M	M
RIBUPD	Does this BIS update the Loc-RIBs correctly?	7.16.2	M	M	M	M
AGGRT	Does this BIS support route aggregations?	7.18.2.1, 7.18.2.2, 7.18.2.3	O	ATNIDRP3 or ATNIDRP5:M	ATNIDRP3 or ATNIDRP5: M	-
LOCK	Does this BIS provide interlocks between its decision process and the updating of the information in its Adj-RIBs-In?	7.16.4	M	M	M	M

3.8.3.5.7 *IDRP receive*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
RCV	Does the BIS process incoming BISPDUs and respond correctly to error conditions?	7.14, 7.20	M	M	M	M
OSIZE	Does this BIS accept incoming OPEN PDUs whose size in octets is between MinBISPDULength and 3000?	6.2,7.20	M	M	M	M
MXPDU	Does the BIS accept incoming UPDATE, IDRP ERROR and RIB REFRESH PDUs whose size in octets is between minBISPDULength and maxBISPDULength?	6.2,7.20	M	M	M	BISREF: OX ^BISREF: M

BISREF: if RIB REFRESH PDU **then** true **else** false

3.8.3.5.8 *Peer entity authentication*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
AUTH	Does this BIS correctly authenticate the source of a BISPDU?	7.7.2	O	M	M	M

Note.— Only support for an authentication code 1 is required.

3.8.3.5.9 *IDRP CLNS forwarding*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
PSRCRT	Does the BIS correctly handle ISO/IEC 8473 NPDUs that contain a partial source route?	8	M	O	OX	O
DATTS	Does the BIS correctly extract the NPDU-derived distinguishing attributes from an ISO/IEC 8473 NPDU?	8.2	M	M	M	M
MATCH	Does the BIS correctly match the NPDU-derived distinguishing attributes with the corresponding FIB-Atts?	8.3	M	M	M	M
EXTF	Does the BIS correctly forward NPDUs with destinations outside its own routing domain?	8.4	M	M	M	M
INTF	Does the BIS correctly forward NPDUs with destinations inside its own routing domain?	8.1	M	M	M	M

3.8.3.5.10 *IDRP optional transitive attributes*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
MEXIT	Does this BIS support use of the MULTI-EXIT DISC attribute?	7.12.7	O	O	O	O

3.8.3.5.11 *Generating well-known discretionary attributes*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
EXTG	Does the BIS support generation of the EXT_INFO attribute?	7.12.2	O	O	O	O
NHRS	Does the BIS support generation of the NEXT_HOP attribute in support of route servers?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	O
NHSN	Does the BIS support generation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	O

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
DLI	Does the BIS support generation of the DIST_LIST_INCL attribute?	7.12.5	O	O	O	O
DLE	Does the BIS support generation of the DIST_LIST_EXCL attribute?	7.12.6	O	O	IDRPAG:OX ^IDRPAG:O	O
TDLY	Does the BIS support generation of the TRANSIT DELAY attribute?	7.12.8	O	O	IDRPAG:OX ^IDRPAG:O	O
RERR	Does the BIS support generation of the RESIDUAL ERROR attribute?	7.12.9	O	O	IDRPAG:OX ^IDRPAG:O	O
EXP	Does the BIS support generation of the EXPENSE attribute?	7.12.10	O	O	IDRPAG:OX ^IDRPAG:O	O
LQOSG	Does the BIS support generation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	OX	OX	OX
HREC	Does the BIS support generation of the HIERARCHICAL RECORDING attribute?	7.12.12	O	OX	OX	OX
SECG	Does the BIS support generation of the SECURITY attribute?	7.12.14	O	M	M	M
PRTY	Does the BIS support generation of the PRIORITY attribute?	7.12.16	O	O	IDRPAG:OX ^IDRPAG:O	O

IDRPAG: if air-ground adjacency **then** true **else** false

3.8.3.5.12 *Propagating well-known discretionary attributes*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
EXTGP	Does the BIS support propagation of the EXT_INFO attribute?	7.12.2	M	M	M	—
NHRSP	Does the BIS support propagation of the NEXT_HOP attribute in support of route servers?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	—
NHSNP	Does the BIS support propagation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	—
DLIP	Does the BIS support propagation of the DIST_LIST_INCL attribute?	7.12.5	O	M	M	—

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
DLEP	Does the BIS support propagation of the DIST_LIST_EXCL attribute?	7.12.6	O	M	IDRPAG: OX ^IDRPAG:M	—
TDLYP	Does the BIS support propagation of the TRANSIT DELAY attribute?	7.12.8	O	O	IDRPAG: OX ^IDRPAG:O	—
RERRP	Does the BIS support propagation of the RESIDUAL ERROR attribute?	7.12.9	O	O	IDRPAG:OX ^IDRPAG:O	—
EXPP	Does the BIS support propagation of the EXPENSE attribute?	7.12.10	O	O	IDRPAG: OX ^IDRPAG:O	—
LQOSP	Does the BIS support propagation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	OX	OX	—
HRECP	Does the BIS support propagation of the HIERARCHICAL RECORDING attribute?	7.12.12	O	OX	OX	—
SECP	Does the BIS support propagation of the SECURITY attribute?	7.12.14	O	M	M	—
PRTYP	Does the BIS support propagation of the PRIORITY attribute?	7.12.16	O	O	IDRPAG:OX ^IDRPAG:O	—

3.8.3.5.13 *Receiving well-known discretionary attributes*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
EXTR	Does the BIS recognize upon receipt the EXT_INFO attribute?	7.12.2	M	M	M	M
NHRSR	Does the BIS recognize upon receipt the NEXT_HOP attribute?	7.12.4	M	M	M	O
DLIR	Does the BIS recognize upon receipt the DIST_LIST_INCL attribute?	7.12.5	M	M	M	M
DLER	Does the BIS recognize upon receipt the DIST_LIST_EXCL attribute?	7.12.6	M	M	M	O
TDLYR	Does the BIS recognize upon receipt the TRANSIT DELAY attribute?	7.12.8	M	M	M	O

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
RERRR	Does the BIS recognize upon receipt the RESIDUAL ERROR attribute?	7.12.9	M	M	M	O
EXPR	Does the BIS recognize upon receipt the EXPENSE attribute?	7.12.10	M	M	M	O
LQOSR	Does the BIS recognize upon receipt the LOCALLY DEFINED QOS attribute?	7.12.11	M	O	O	O
HRECR	Does the BIS recognize upon receipt the HIERARCHICAL RECORDING attribute?	7.12.12	M	M	M	O
SECR	Does the BIS recognize upon receipt the SECURITY attribute?	7.12.14	M	M	M	M
PRTYR	Does the BIS recognize upon receipt the PRIORITY attribute?	7.12.16	M	M	M	O

3.8.3.5.14 *IDRP timer*

Item	*Description*	*ISO/IEC 10747 Ref.*	*ISO status*	*G-G router*	*A/G router*	*Airborne router*
Ta	KeepAlive timer	11.4, ATN Ref: 3.8.3.4	M	M	M	M
Tr	Retransmission (tr) timer	7.6.1.2, 7.6.1.3	M	M	M	M
Tmr	maxRIBIntegrityCheck timer	7.10.2	M	M	M	M
Tma	MinRouteAdvertisement timer	7.17.3.1	M	M	M	O
Trd	MinRDOriginationInterval timer	7.17.3.2	M	M	M	M
Tcw	closeWaitDelay timer	7.6.1.5	M	M	M	M

3.9 SYSTEMS MANAGEMENT PROVISIONS

Note 1.— The ATN is dependent upon systems management procedures to monitor and maintain the provided quality of service. For those ATN systems, which support ATN systems management, there is a minimum set of systems management requirements which applies to each type of ATN system (ES, BIS, IS, etc.).

Note 2.— ATN systems are expected to support general systems management capabilities as the minimum functionality available to a suitably authorized and authenticated local systems manager.

Note 3.— The details of the mechanisms used to satisfy these requirements within a given management domain are a local matter.

— END —

ISBN 978-92-9258-142-8