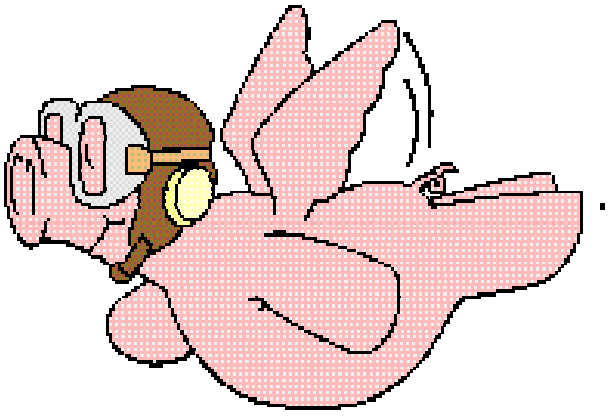
The ATN SARPs



Subvolume Five

Internet Communications Service (ICS)

Third Edition
(Final Editor's Draft)

Please note that this is the final editor's draft of the "Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN) – ICAO DOC 9705/AN956 - as circulated within the ATNP. This text will be passed to ICAO for publication. However, it should be noted that this text in no way replaces the ICAO version, nor can it be considered to be of equal status. The official definitive version is that published in hardcopy by ICAO and all claims of compliance must be made against that version.

This PDF version has been prepared for the ATNP Working Groups by Helios Information Services Ltd. – http://www.helios-is.com

Please check our web site regularly for updates to the draft SARPs

Errata and Disclaimer

Please note that this document has been prepared from a number of separate files and no attempt has been made to ensure continuity of page numbers. You may therefore find some overlap between page numbers.

This document has been prepared on a “best efforts” basis and no warrantee is offered as to its correctness.

FOREWORD

The material contained in this document was originally developed as the detailed part of the first set of Standards and Recommended Practices (SARPs) for the aeronautical telecommunication network (ATN) which has commonly been referred to as the CNS/ATM-1 Package. It was intended to make the material an appendix to the new Chapter 3 of Annex 10, Volume III, Part I, containing broad, general, stable and mostly regulatory-type provisions (the core part of new ATN SARPs).

In December 1997, the Air Navigation Commission (ANC), while conducting the final review of draft ATN SARPs, agreed that the detailed part of ATN SARPs should be published as an ICAO manual (to be updated annually, if necessary), while retaining its SARPs-style language. The ANC has reviewed the status of the document in light of continuing worldwide ATN implementation. The Third Edition includes amendments from implementors and regulatory authorities, as well as four new Sub-Volumes to answer requirements for further standardization, in the interests of safety, regularity and efficiency of international civil aviation.

This document consists of nine Sub-Volumes:

Sub-Volume I — Introduction and System Level Requirements
Sub-Volume II — Air-Ground Applications
Sub-Volume III — Ground-Ground Applications
Sub-Volume IV — Upper Layer Communications Service (ULCS)
Sub-Volume V — Internet Communications Service (ICS)
Sub-Volume VI — System Management (SM)
Sub-Volume VII — Directory Services (DIR)
Sub-Volume VIII — Security (SEC)
Sub-Volume IX — Registration (REG)

Provisions contained in Sub-Volumes II, III, IV, V, VI, VII, VIII, and IX have been developed in accordance with system requirements specified in Sub-Volume I.

In line with the agreement by the ANC that the document should be updated on a yearly basis (if deemed necessary), the Third Edition has been published to incorporate changes necessitated by continuing validation and actual implementation activities.

TABLE OF CONTENTS

SUB-VOLUME I. INTRODUCTION AND SYSTEM LEVEL REQUIREMENTS

SUB-VOLUME II. AIR-GROUND APPLICATIONS

SUB-VOLUME III. GROUND-GROUND APPLICATIONS

SUB-VOLUME IV. UPPER LAYER COMMUNICATIONS SERVICE

SUB-VOLUME V. INTERNET COMMUNICATIONS SERVICE

SUB-VOLUME VI. SYSTEMS MANAGEMENT SERVICE

SUB-VOLUME VII. DIRECTORY SERVICE

SUB-VOLUME VII. SECURITY SERVICES

SUB-VOLUME IX. REGISTRATION SERVICE

5.1 INTRODUCTION

5.1.1 This sub-volume defines the provisions that ATN compliant End Systems (ESs) and Intermediate Systems (ISs) must implement in order to provide the ATN SARPs compliant "Internet Communications Service" to the "User" i.e. the Upper Layer Architecture as defined in Section 4 of the ATN SARPs. For the protocols, the majority of such provisions are specified in a tabular fashion under the title of "ATN Protocol Requirements Lists" (APRLs).

5.1.2 This sub-volume comprises nine Chapters as introduced below.

Chapter 5.1, contains introductory material to the remainder of the Section.

Chapter 5.2, 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 SARPs related to security and priority handling within the ATN internet.

Chapter 5.3, 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.

Chapter 5.4, contains provisions related to the ATN Internet addressing architecture and responsibilities related to the definition and allocation of ATN Internet address fields.

Chapter 5.5, contains "Transport Layer" provisions applicable to ATN End Systems. Provisions for the ISO Connection Oriented Transport Protocol (Class 4) and the Connectionless Transport Protocol are defined.

Chapter 5.6, contains "Inter-Network Layer" provisions, based on the ISO Connectionless Network Protocol (CLNP), applicable to ATN End Systems and ATN Intermediate Systems.

Chapter 5.7, 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.

Chapter 5.8, contains provisions related to the secure 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.

Chapter 5.9, contains a set of notes regarding the implementation of Internet Systems Management.

5.2 DEFINITIONS AND CONCEPTS

5.2.1 Objectives and Goals

Note 1.— In computer data networking terminology, the infrastructure required to support the interconnection 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 (International Civil Aviation Organization) 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.

5.2.2 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).

5.2.2.1 The ATN Internet

5.2.2.1.1 The ATN shall consist of a set of interconnected Routing Domains (RDs), within the global OSI Environment (OSIE). Each such RD shall contain Air Traffic Service Communication (ATSC) and/or Aeronautical Industry Service Communication (AINSC) related Intermediate and End Systems.

5.2.2.1.2 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.

5.2.2.1.3 Otherwise, the Routing Domain shall be defined as an End Routing Domain (ERD).

5.2.2.2 ATN RDs

5.2.2.2.1 General

5.2.2.2.1.1 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.

5.2.2.2.1.2 Every ATN RD shall have at least one Routing Domain Identifier (RDI).

5.2.2.2.1.3 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.

5.2.2.2.2 Fixed RDs

5.2.2.2.2.1 Each State and Organisation 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 Organisations may alternatively combine their RDs into a single RD.

5.2.2.2.3 Mobile RDs

5.2.2.2.3.1 Each ATN equipped Mobile platform (e.g. an aircraft) shall operate at least one ATN RD. This shall be an End Routing Domain.

5.2.2.2.3.2 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 5.2.-1).

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

5.2.2.2.3.3 When more than one Airborne Router (BIS) is installed on board an aircraft, then each shall be in a separate Routing Domain.

5.2.2.2.3.4 **Recommendation.**— *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 (e.g. airport surface vehicles, etc.) may be operated as ATN routing domains in the future.

5.2.2.3 The Ground ATN Internet

5.2.2.3.1 General

5.2.2.3.1.1 The Ground ATN Internet shall consist of one or more ATN Island RDCs (Routing Domain Confederations).

5.2.2.3.2 ATN Island RDC

5.2.2.3.2.1 Each ATN Island shall comprise one or more ATN RDs forming a single ATN Island RDC.

5.2.2.3.2.2 An ATN Island RDC shall not contain any ATN Mobile RDs.

Note.— An example ATN Island RDC topology is presented in Figure 5.2-1.

5.2.2.3.3 The Fixed ATN RDC

5.2.2.3.3.1 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 (Routing Domain Identifiers) of all ATN RDs in the RD_Path Attribute.

5.2.2.4 The Global ATN Backbone

5.2.2.4.1 General

5.2.2.4.1.1 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.

5.2.2.4.2 ATN Island Backbone RDCs

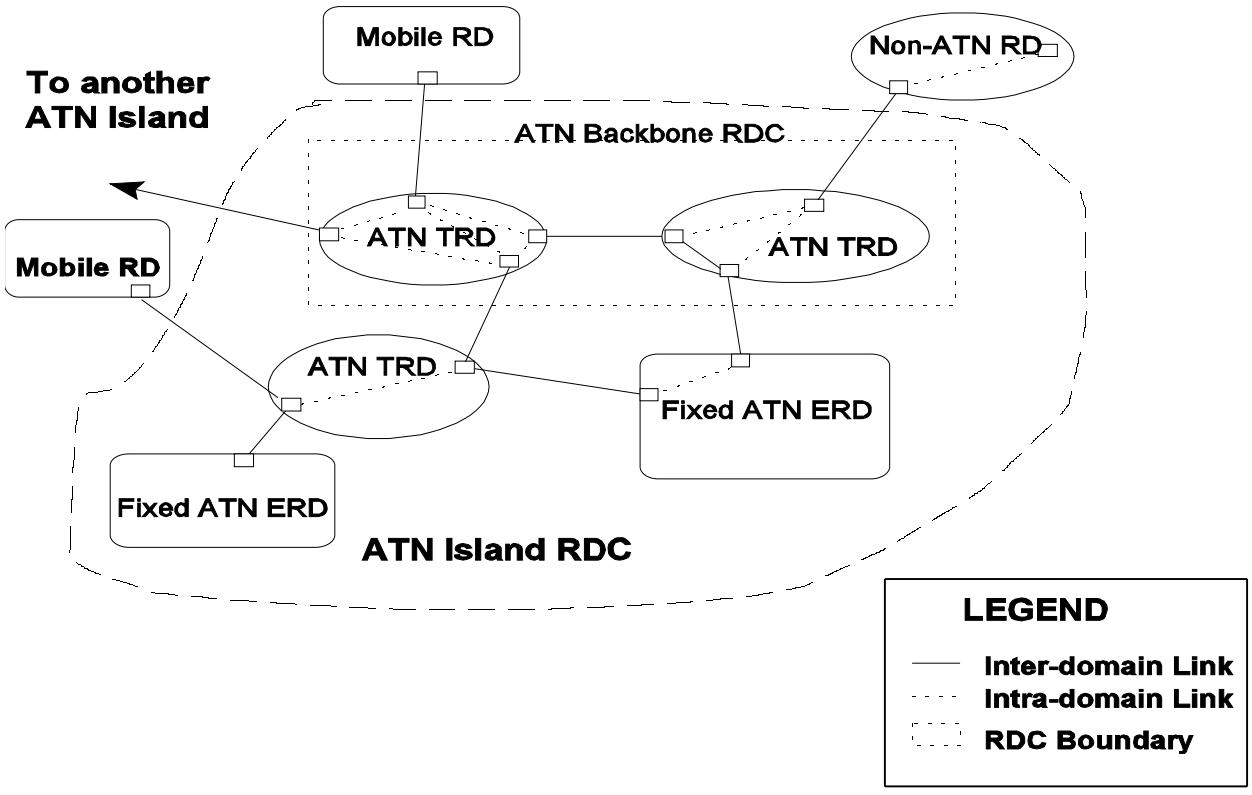


Figure 5.2-1 Example ATN Island Routing Domain Confederation Structure

5.2.2.4.2.1 **Recommendation.**— *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.*
5.2.2.4.2.2 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 only a recommended practice as in some regions, simpler, or other alternative structures may be more appropriate for an ATN Island.

5.2.2.5 The "Home" Domain

5.2.2.5.1 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" needs 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 5.3.7.

5.2.2.6 Administrative Domains and the ATN

5.2.2.6.1 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 requirements of the SARPs, the distribution of end system and intermediate system functionality and the use of interworking processes exclusively within an Administrative Domain is a local matter.

5.2.2.7 Default Routes

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

a) is available to all traffic types (see 5.2.7.1.2), 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.

5.2.2.7.2 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 5.2.7.1.2), 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.

5.2.3 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 realisation 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.

5.2.3.1 Physical and Data Link Layer

5.2.3.1.1 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.

5.2.3.2 Network Layer

5.2.3.2.1 ATN End Systems shall implement:

a) The End System provisions of ISO/IEC 8473, as specified in 5.6, 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 5.7.

5.2.3.2.2 **Recommendation.**— *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).*

5.2.3.3 Transport Layer

5.2.3.3.1 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 5.5

b) ISO/IEC 8602 as specified in 5.5.

5.2.3.4 Upper Layers

Note.— The requirements for session, presentation and application layer protocols to support end-user applications on ATN End Systems are defined in Section 4 of the ATN SARPs.

5.2.3.5 Applications

Note.— The requirements for Air/Ground and Ground/Ground applications are contained in Sections 2 and 3 of the ATN SARPs respectively.

5.2.4 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 realisation of the OSI Intermediate System architectural entity. ATN Routers that additionally implement ISO/IEC 10747 are also known as Boundary Intermediate Systems (BISs).

5.2.4.1 ATN Router Classes

5.2.4.1.1 The classes of ATN Router and the Routing Protocols supported, that are recognised by this specification, are listed below in Table 5.2-1.

Table 5.2-1 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 5.3.5.2)
6.	Airborne Router with IDRP	ISO/IEC 9542 ISO/IEC 10747 Route Initiation Procedures (see 5.3.5.2)
7.	Airborne Router without IDRP	ISO/IEC 9542 Route Initiation Procedures (see 5.3.5.2)

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.

5.2.4.1.2 All ATN Routers (i.e. Router Classes 1 to 7 inclusive) shall support the ISO/IEC 8473 Connectionless Network Protocol (CLNP) as specified in 5.6, 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.

5.2.4.1.3 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 5.8 for the exchange of inter-domain routing information according to 5.3.6 and 5.3.7.

5.2.4.1.4 An Airborne (Router Classes 6 or 7) or Air/Ground Router (Router Class 5) shall support the Mobile SNDCF specified in 5.7 for the use of CLNP over an ATN Mobile Subnetwork, and the ISO/IEC 9542 ES-IS routing information exchange protocol, as specified in 5.8 for support of the route initiation procedures specified in 5.3.5.2.

5.2.4.2 Physical and Data Link Layers

5.2.4.2.1 ATN Routers shall implement the appropriate Physical and Data Link Layer functions for access to the ATN subnetwork(s) to which they are attached.

5.2.4.3 Network Layer

5.2.4.3.1 An ATN Router shall implement:

a) the Intermediate System provisions of ISO/IEC 8473, as specified in 5.6, 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 selected Subnetwork Access Protocol, as specified in 5.7.

d) The routing protocols specified in Table 5.2-1 for the Router's Router Class, as specified in 5.8.

e) The Route Initiation procedures appropriate to the Router Class, as specified in 5.3.

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 5.3 (see 5.3.5.2) and in 5.8.

5.2.4.3.2 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 5.3.

5.2.4.3.3 **Recommendation**.— *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.

5.2.5 ATN Subnetworks

Note.— An ATN Subnetwork is any fixed or Mobile data communications network that fulfils the following requirements.

5.2.5.1 Requirements for All ATN Subnetworks

5.2.5.1.1 Paragraph has been deleted.

5.2.5.1.2 Byte and Code Independence

5.2.5.1.2.1 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.

5.2.5.1.3 Subnetwork QoS

5.2.5.1.3.1 A Subnetwork service provider shall provide an indication of the Subnetwork Quality of Service (QoS) available, in order to support the internetwork routing decision process.

5.2.5.1.4 Subnetwork Addressing

5.2.5.1.4.1 An ATN subnetwork shall provide a mechanism for uniquely and unambiguously identifying each ATN router attached to that subnetwork.

5.2.5.1.5 Internal Subnetwork Routing

5.2.5.1.5.1 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.

5.2.5.2 Requirements for ATN Mobile Subnetworks

5.2.5.2.1 Paragraph has been deleted.

5.2.5.2.2 Invocation of Subnetwork Priority

5.2.5.2.2.1 When priority is implemented within that subnetwork, an ATN Mobile Subnetwork shall provide a SNAcP mechanism for invocation of subnetwork priority.

5.2.5.2.3 Invocation of Subnetwork Quality of Service for Mobile Subnetworks

5.2.5.2.3.1 **Recommendation.**— *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.

5.2.5.2.4 Connection-Mode Subnetwork Service

5.2.5.2.4.1 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.

5.2.5.2.4.2 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.

5.2.5.2.5 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.

5.2.5.2.5.1 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 5.3.

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.

5.2.5.2.5.1.1 ATN Mobile Subnetworks shall issue a Join Event (see 5.3.5.2) to the attached IS-SME to indicate the availability of a physical communication path between a pair of SNPAs.

5.2.5.2.5.1.2 ATN Mobile Subnetworks shall issue a Leave Event (see 5.3.5.2.13) to the attached IS-SME to indicate that a previously available physical communication path between a pair of SNPAs is no longer available.

5.2.5.2.5.1.2.1 ATN Mobile Subnetworks supporting the ATN Operational Communications traffic type and the ATSC traffic category (see 5.2.7.1.2) shall have a maximum delay, at 95% probability, for issueing a Leave Event consistent with the requirements in 5.2.7.1.3 for the ATSC Class supported by that subnetwork.

5.2.5.2.6 Segmentation/Reassembly Mechanism

5.2.5.2.6.1 **Recommendation.**— *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.

5.2.6 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 of 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 5.2.7.1.3), 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 1-1) 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 5.2-2).

5.2.7 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;

c) Ensuring that Air/Ground subnetworks are used in accordance with ITU resolutions on frequency utilisation; and

d) Protecting routing information exchanges among ATN BISs.

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 4.

Note 3.— The ATN Internet supports item (d) above through the use of ISO/IEC 10747 type 2 authentication in ATN ISs which implement ATN security services.

Note 4.— 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 5.— 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 6.— 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 utilisation.

5.2.7.1 The ATN Security Label

5.2.7.1.1 General

5.2.7.1.1.1 The ATN Security Label shall be encoded according to 5.6.2.2.2.

5.2.7.1.1.2 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.

5.2.7.1.2 Traffic Types

5.2.7.1.2.1 A CLNP Data 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 5.6-1).

5.2.7.1.2.2 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.

5.2.7.1.2.3 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 ordering of Air/Ground subnetworks are specified in Table 5.6-1.

5.2.7.1.3 ATSC Class

5.2.7.1.3.1 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 5.2-2 for the advertised ATSC Class.

5.2.7.1.3.2 ATN Mobile Subnetworks supporting the ATN Operational Communications traffic type and the ATSC traffic category shall satisfy the maximum delay requirements in issueing a Leave Event as indicated in either the third or/and the fourth column of Table 5.2-2 for the advertised ATSC Class.

Table 5.2-2 Subnetwork Transit Delay and Leave Event Issuance Maximum Delay

ATSC Class	Maximum One-way ATN Mobile Subnetwork Transit Delay at 95% Probability (in seconds)	Maximum Delay, at 95% Probability, in Issuing a Leave Event in the Absence of NPDU Traffic (in seconds)	Maximum Delay, at 95% 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 1-1.

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 Table 1-3, 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 5.2.5.2.5.1.2.1) 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 5.2-2) 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 5.2-2).

Note 6.— The semantics of the ATSC Class for other QoS metrics and availability are outside of the scope of this specification.

5.2.7.1.4 Security Classification

Note.— The Security Classification may be used to convey the confidentiality level of application data.

5.2.7.2 Applications Use of ATN Security Labels

5.2.7.2.1 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 5.2.7.1.2.

5.2.7.2.2 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.

5.2.7.2.3 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.

5.2.7.3 Transport Layer Security

5.2.7.3.1 In the Connection Mode

5.2.7.3.1.1 Except when a transport connection is used to convey general communications data, each transport connection shall be associated with a single ATN Security Label.

5.2.7.3.1.2 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.

5.2.7.3.1.3 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.

5.2.7.3.1.4 TPDUs from transport connections associated with different ATN Security Labels shall not be concatenated into the same NSDU.

5.2.7.3.1.5 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.

5.2.7.3.2 In the Connectionless Mode

5.2.7.3.2.1 In the connectionless mode, unless used to convey General Communications data, each incoming or outgoing TSDU shall be associated with an ATN Security Label.

5.2.7.3.2.2 For outgoing TSDUs, this ATN Security Label shall be encoded into the header of the resulting NPDU(s).

5.2.7.3.2.3 For incoming TSDUs, the associated ATN Security Label shall be the ATN Security Label that was encoded into the header of the incoming NPDU(s) that contained the TSDU.

Note.— The mechanism by which ATN Security Labels are associated with TSDUs is a local matter.

5.2.7.4 Network Layer Security

5.2.7.4.1 Service Provider to the Transport Layer

5.2.7.4.1.1 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 5.6.2.2.2.

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).

5.2.7.4.2 Routing Control

5.2.7.4.2.1 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.— 5.3.2.2 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.

5.2.7.4.3 Protection of the Routing Information Base

5.2.7.4.3.1 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.

5.2.7.4.3.2 ATN Routers supporting ATN security services shall support IDRP type 2 authentication in addition.

Note 1.— Support of type 2 authentication enables the routing information base to be protected from attackers that try to modify routing information while in transit, or which attempt to masquerade as genuine ATN Routers.

Note 2.— The ATN security services comprise a set of information security provisions which allow the receiving ES or IS to unambiguously identify the source of the received information and to verify the integrity of this information. Use of the IDRP type 2 authentication is a key feature of the ATN security services provided in the ATN Internet.

Note 3.— The use of the ATN security services in the ATN Internet is a conceptually different mechanism to those functions provided by the use of the ATN Security Label. The latter mechanism ensures that application QoS, routing policy requirements and restrictions of Mobile Subnetworks are enforced within a common domain of trust.

5.2.7.5 Subnetwork Provisions

Note.— There are no requirements for security mechanisms in ATN Subnetworks. However, Administrations and other Organisations implementing ATN subnetworks are encouraged to ensure the general security and availability of ATN subnetworks through the use of physical security mechanisms.

5.2.8 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 5.2-2 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.

5.2.8.1 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.

5.2.8.1.1 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 Table 1-2 .

Note.— An ATN Application may include messages from more than one category.

5.2.8.1.2 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 Table 1-2 for the message's message category, or

b) the connectionless transport service, signalling the Connectionless Transport Service Priority listed in Table 1-2 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.

5.2.8.2 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.

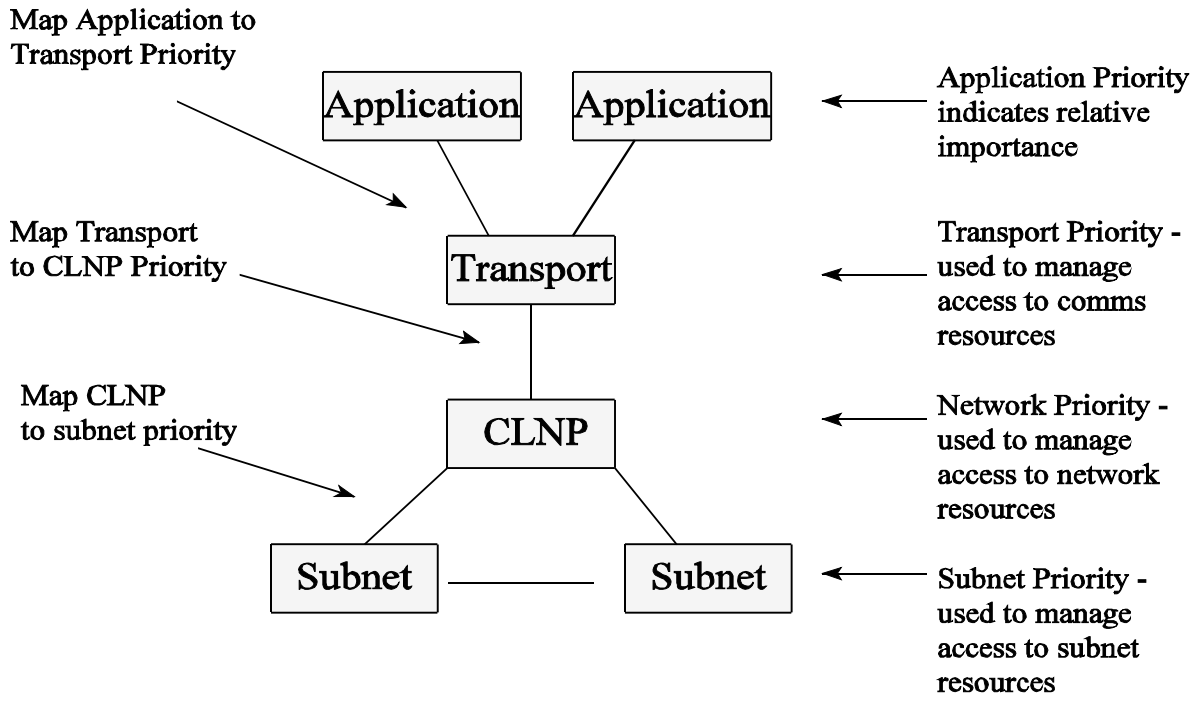


Figure 5.2-2 Use of Priority in the ATN

Note 2.— The transport connection priority is specified by the transport user either explicitly or implicitly, when the transport connection is established.

5.2.8.2.1 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.

5.2.8.2.2 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 Table 1-2.

5.2.8.3 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.

5.2.8.3.1 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 Table 1-2.

5.2.8.4 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 utilisation, 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.

5.2.8.4.1 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.

5.2.8.4.2 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.

5.2.8.4.3 BISPDUs exchanged by IDRP shall be considered as Network/Systems Management category messages, and shall be sent using CLNP priority 14.

5.2.8.4.4 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.

5.2.8.5 ATN Subnetwork Priority

5.2.8.5.1 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.

5.2.8.5.1.1 When an ATN connection mode subnetwork does not support prioritisation 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.

5.2.8.5.1.2 When an ATN connection mode subnetwork does support prioritisation 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.

5.2.8.5.1.3 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.

5.2.8.5.2 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.

5.2.8.5.2.1 When an NPDU is sent over a connectionless-mode ATN Subnetwork which supports data prioritisation, then the subnetwork priority assigned to the transmitted packet shall be that specified by the subnetwork provider as corresponding to the NPDU priority.

5.3 ATN ROUTING

5.3.1 Introduction

5.3.1.1 Scope

Note.— This chapter 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 compliancy with the ISO/IEC 10747 and ISO/IEC 9542 protocols. This is the subject of 5.8.

5.3.1.2 Applicability of Requirements

Note 1.— The classes of ATN Router referred to below are defined in 5.2.4.1.

Note 2.— The ATN RDs referred to below are defined in 5.2.2.2.

5.3.1.2.1 ATN Ground/Ground Routers shall comply with the provisions of 5.3.4 and 5.3.6.

5.3.1.2.2 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 5.3.7.1.

5.3.1.2.3 When used in any other ATN Transit Routing Domain, an ATN Ground/Ground Router shall also comply with the provisions of 5.3.7.3.

5.3.1.2.4 Otherwise, an ATN Ground/Ground Router shall comply with the provisions of 5.3.7.4.

5.3.1.2.5 ATN Air/Ground Routers shall comply with the provisions of 5.3.4 for Ground/Ground interconnection, 5.3.5 for Air/Ground interconnection and 5.3.6.

5.3.1.2.6 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 5.3.7.1.

5.3.1.2.7 When used in any other ATN Transit Routing Domain, an ATN Air/Ground Router shall also comply with the provisions of 5.3.7.3.

5.3.1.2.8 ATN Airborne Routers shall comply with the provisions of 5.3.5, 5.3.6, and 5.3.7.2.

5.3.1.2.9 When an RD is declared to be an ATN RD, then it shall comply with the provisions of 5.2.2.2.

5.3.1.2.10 When an RD is declared to be a Mobile RD, then it shall comply with the provisions of 5.2.2.2.3.

5.3.1.2.11 When an RDC is declared to be an ATN Island RDC, then its member RDs shall comply with the provisions of 5.2.2.3.2.

5.3.1.2.12 When an RDC is declared to be an ATN Island Backbone RDC, then its member RDs shall comply with the provisions of 5.2.2.4.2.

5.3.2 Service Provided by an ATN Router

5.3.2.1 General

5.3.2.1.1 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.

5.3.2.2 Forwarding CLNP NPDUs

5.3.2.2.1 General

5.3.2.2.1.1 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.

5.3.2.2.1.2 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.

5.3.2.2.2 Forwarding a CLNP NPDU when no Security Parameter is present in the PDU Header

Note.— This case applies for General Communications data (see 5.2.7.1).

5.3.2.2.2.1 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.

5.3.2.2.2.2 If no such route can be found then the NPDU shall be discarded.

5.3.2.2.3 Forwarding a CLNP NPDU when a Security Parameter is present in the PDU Header

5.3.2.2.3.1 General

5.3.2.2.3.1.1 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 5.6.2.2 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.

5.3.2.2.3.2 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.

5.3.2.2.3.2.1 No Traffic Type Policy Preference

Note.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 000 00001.

5.3.2.2.3.2.1.1 If the NPDU contains a CLNP NPDU Header Security Parameter in the globally unique format, and encodes:

a) security related information according to 5.6.2.2 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 5.3.2.2.1.1 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.

5.3.2.2.3.2.1.2 If no such route can be found, then the NPDU shall be discarded.

5.3.2.2.3.2.2 ATSC Class Specified

Note.— This case corresponds to Traffic Type and Associated Routing Policy Security Tag values 000 10000 to 000 10111 inclusive.

5.3.2.2.3.2.2.1 If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to 5.6.2.2 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 5.3.2.2.1.1 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.

5.3.2.2.3.2.2.2 If no such route can be found then the NPDU shall be discarded.

5.3.2.2.3.2.2.3 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.

5.3.2.2.3.2.2.4 If the monetary cost is the same or unknown, then the hop count shall be used as the relative cost metric.

5.3.2.2.3.3 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.

5.3.2.2.3.3.1 No Traffic Type Policy Preference

Note.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 001 00001.

5.3.2.2.3.3.1.1 If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to 5.6.2.2 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.

5.3.2.2.3.3.1.2 If no such route can be found, then the NPDU shall be discarded.

5.3.2.2.3.3.2 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.

5.3.2.2.3.3.2.1 If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to 5.6.2.2 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.

5.3.2.2.3.3.2.2 If no such route can be found, then the NPDU shall be discarded.

5.3.2.2.3.3.3 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.

5.3.2.2.3.3.3.1 If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to 5.6.2.2 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.

5.3.2.2.3.3.3.2 If no such route can be found, then the NPDU shall be discarded.

5.3.2.2.3.3.3.3 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.

5.3.2.2.3.4 ATN Administrative Communications Traffic Type

Note.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 001 10000.

5.3.2.2.3.4.1 If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to 5.6.2.2 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.

5.3.2.2.3.4.2 If no such route can be found, then the NPDU shall be discarded.

5.3.2.2.3.5 ATN Systems Management Communications Traffic Type

Note.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 011 00000.

5.3.2.2.3.5.1 If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to 5.6.2.2 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.

5.3.2.2.3.5.2 If no such route can be found, then the NPDU shall be discarded.

5.3.3 The Deployment of ATN Components

5.3.3.1 Interconnection of ATN RDs

5.3.3.1.1 General

5.3.3.1.1.1 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 5.2-1.

Note 2.— There is no requirement for all ATN RDs to be fully interconnected.

5.3.3.1.1.2 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 5.2.5.1.

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 5.3.4, and for interconnection of an Air/Ground and an Airborne Router in 5.3.5. The remainder of this section is concerned with static interconnection requirements.

5.3.3.1.2 Interconnection between Members of an ATN Island Backbone RDC

5.3.3.1.2.1 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.

5.3.3.1.3 Interconnection between Members of an ATN Island Backbone RDC and other ATN RDs within the ATN Island

5.3.3.1.3.1 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.

5.3.3.1.4 Interconnection of ATN Islands

5.3.3.1.4.1 ATN Islands shall only interconnect via ATN RDs which are members of each ATN Island's Backbone RDC.

5.3.3.1.4.2 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.

5.3.3.1.5 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.

5.3.3.1.5.1 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 dependant 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.

5.3.3.1.6 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.

5.3.4 Ground/Ground Interconnection

5.3.4.1 Interconnection Scenarios

Note 1.— Ground/Ground interconnection procedures apply to the interconnection of two Ground/Ground Routers, and to 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.

5.3.4.2 Ground/Ground 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.

5.3.4.2.1 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, and supporting the Quality of Service necessary for the applications data that will be routed over this interconnection.

Note.— 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.

b) Using global or local Systems Management mechanisms, establish one or more subnetwork connections between the two ATN Routers, unless the subnetwork technology is connectionless in which case this step may be omitted.

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.

c) Using global or local Systems Management mechanisms, ensure that the forwarding information base in each ATN Router, used to support the connectionless network protocol specified in 5.6, 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 connectionless network service can be used to exchange the BISPDUs of IDRP.

d) 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,

e) Using global or local Systems Management mechanisms, create an **AdjacentBIS** Managed Object (MO) in each ATN Router to represent the other ATN Router, and

f) Using global or local Systems Management mechanisms, invoke the start event action on each such MO, in order to initiate a BIS-BIS connection between the two ATN Routers.

Note.— As a matter for the bilateral agreement of the network administrators, either (a) both ATN Routers will attempt to open the BIS-BIS connection, or (b) one and only one acts as the BIS-BIS connection initiator.

5.3.4.3 Ground/Ground Routing Information Exchange

5.3.4.3.1 Routing information shall be exchanged using the ISO/IEC 10747 Inter-Domain Routing Protocol according to the profile specified in 5.8.

5.3.4.3.2 In support of Air/Ground communications, the exchange of routing information shall be subject to appropriate routing policies specified in 5.3.7.1, 5.3.7.3, or 5.3.7.4, depending upon the role of the Routing Domain in which each ATN Router is located.

5.3.4.4 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 useable 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 5.3.4.2 may be re-invoked, as appropriate to re-establish communication, and to exchange routing information.

5.3.4.4.1 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.

5.3.4.4.2 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.

5.3.4.4.3 For either temporary or permanent termination, and if required, by using global or local Systems Management mechanisms, the network administrator(s) shall also terminate the underlying subnetwork connections.

5.3.5 Air/Ground Interconnection

5.3.5.1 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 5.3.5.2.12.

Note 4.— For the purposes of this specification, the functional model of an ATN Router illustrated in Figure 5.3-1 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 5.3-1 introduces a new architectural entity, the Intermediate System - Systems Management Entity (IS-SME). As specified below, this plays an important role in the realisation 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 5.3.5.2.

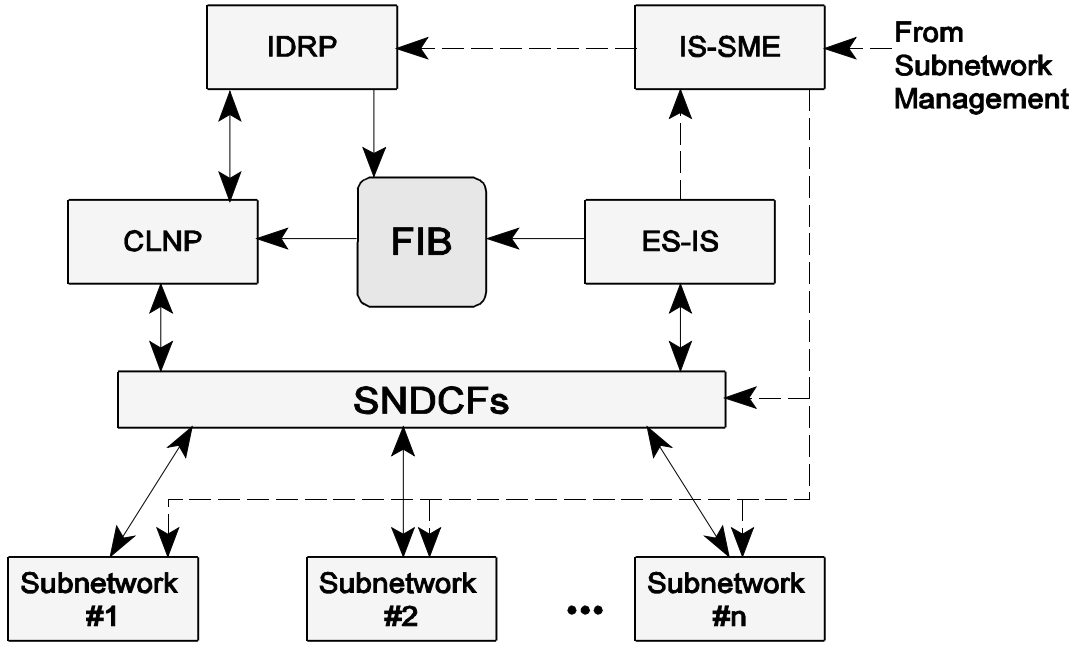


Figure 5.3-1 Assumed ATN Router Architecture for Air/Ground Route Initiation

5.3.5.2 Air/Ground Route Initiation

5.3.5.2.1 General

5.3.5.2.1.1 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.

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 SARPs specified by the relevant ICAO panel.

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.

5.3.5.2.1.2 Paragraph has been deleted.

5.3.5.2.1.3 For Air-Initiated Subnetworks, Airborne Routers shall comply with the procedures specified in 5.3.5.2.3.2, and Air/Ground Routers shall comply with the procedures specified in 5.3.5.2.2.

5.3.5.2.1.4 For Ground-Initiated Subnetworks, Air/Ground Routers shall comply with the procedures specified in 5.3.5.2.4, and Airborne Routers shall comply with the procedures specified in 5.3.5.2.2.

5.3.5.2.1.5 For Air or Ground-Initiated Subnetworks, Air/Ground and Airborne Routers shall comply with the procedures specified in 5.3.5.2.2 and 5.3.5.2.5.

5.3.5.2.1.6 Air/Ground Subnetworks accessed using a network access service compatible with ISO/IEC 8208 shall use the Mobile SNDCF specified in 5.7.6 for providing the SN-Service required by ISO/IEC 8473.

5.3.5.2.1.7 Other types of air-initiated Air/Ground Subnetworks shall use the Frame Mode SNDCF specified in 5.7.8 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.

5.3.5.2.1.8 Air/Ground and Airborne Routers which support ATN security services shall comply with the procedures specified in 5.3.5.2.16.

5.3.5.2.2 Route Initiation Procedures for a Responding ATN Router

5.3.5.2.2.1 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.

5.3.5.2.2.1.1 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.

5.3.5.2.2.1.2 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.

5.3.5.2.2.1.3 When a subnetwork connection is successfully established, then the procedures of 5.3.5.2.6 shall be applied to that subnetwork connection.

5.3.5.2.2.2 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.

5.3.5.2.2.2.1 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.

5.3.5.2.2.2.2 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.

5.3.5.2.2.2.3 The data link shall be made available for user data exchange according to the provisions of the Frame Mode SNDCF specified in 5.7.8.

5.3.5.2.3 Air-Initiated Route Initiation

Note.— This section specifies the procedures to be used by an Airborne Router for Air-Initiated route initiation.

5.3.5.2.3.1 Paragraph has been deleted.

5.3.5.2.3.2 Airborne Router Procedures

5.3.5.2.3.2.1 General

Note 1.— The connectivity information is provided as a "Join Event". This is an event generated by a Mobile Subnetwork when it is recognised 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.

5.3.5.2.3.2.1.1 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 5.3.5.2.3.2.2.1.

5.3.5.2.3.2.1.2 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 5.3.5.2.3.2.3.1.

5.3.5.2.3.2.1.3 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 5.3.5.2.3.2.2.1 for ISO/IEC 8208 Subnetworks or 5.3.5.2.3.2.3.1 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 5.3.5.2.3.2.2.1 for ISO/IEC 8208 Subnetworks or 5.3.5.2.3.2.3.1 for non-ISO/IEC 8208 Subnetworks respectively.

5.3.5.2.3.2.1.4 ***Recommendation.***— *The timer t_{le} defined in 5.3.5.2.3.2.1.3 should be configurable within the range of 0 to 1000 seconds to enable performance optimisation.*

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.

5.3.5.2.3.2.2 ISO/IEC 8208 Subnetworks

5.3.5.2.3.2.2.1 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.

5.3.5.2.3.2.2.2 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 5.3.5.2.14), 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.

5.3.5.2.3.2.2.3 When a subnetwork connection is successfully established, then the procedures of 5.3.5.2.6 shall be applied to that subnetwork connection.

5.3.5.2.3.2.3 Non-ISO/IEC 8208 Subnetworks

5.3.5.2.3.2.3.1 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 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.

5.3.5.2.3.2.3.2 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 5.7.8.

5.3.5.2.3.2.3.3 The procedures of 5.3.5.2.6 shall be applied.

5.3.5.2.4 Ground-Initiated Route Initiation

Note 3.— Ground-Initiated Route Initiation is only appropriate for Mobile subnetworks that originate a Join Event from their ground component.

Note 4.— 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 5.— 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.

5.3.5.2.4.1 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 5.3.5.2.4.3.

5.3.5.2.4.2 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 5.3.5.2.4.3.

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 5.3.5.2.4.3.

5.3.5.2.4.3 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 organisation 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.

5.3.5.2.4.4 ***Recommendation.***— *The timer t_{le} defined in 5.3.5.2.4.2 should be configurable within the range of 0 to 1000 seconds to enable performance optimisation.*

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.

5.3.5.2.4.5 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 5.3.5.2.14), 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.

5.3.5.2.4.6 When a subnetwork connection is successfully established, then the procedures of 5.3.5.2.6 shall be applied to that subnetwork connection.

5.3.5.2.5 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.

5.3.5.2.5.1 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 5.3.5.2.5.3.

5.3.5.2.5.2 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 5.3.5.2.5.3.

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 5.3.5.2.5.3.

5.3.5.2.5.3 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 of the scope of this specification.

5.3.5.2.5.4 ***Recommendation.***— *The timer t_{le} defined in 5.3.5.2.5.2 should be configurable within the range of 0 to 1000 seconds to enable performance optimisation.*

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.

5.3.5.2.5.5 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 5.3.5.2.14), 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.

5.3.5.2.5.6 When a subnetwork connection is successfully established, then the procedures of 5.3.5.2.6 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.

5.3.5.2.6 Exchange of Configuration Information using the ISO/IEC 9542 ISH PDU

5.3.5.2.6.1 ATN Airborne and Air/Ground Routers shall implement the ISO/IEC 9542 "Configuration Information" Function for use over each Mobile Subnetwork that they support.

5.3.5.2.6.2 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 5.8.2.1.3, 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.

5.3.5.2.6.3 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).

5.3.5.2.6.4 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).

5.3.5.2.6.5 Encoding of ATN Data Link Capability Parameter

5.3.5.2.6.5.1 ATN Air/Ground and Airborne Routers shall include the ATN Data Link Capabilities Parameter, as defined in 5.8.2.1.3, 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.

5.3.5.2.6.5.2 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.

Note.— Other bits of the ATN Data Link Capabilities Parameter value field are used to signal support of ATN security services and to request associated authentication data from the peer system as defined in 5.3.5.2.16 and 5.8.2.1.3.

5.3.5.2.6.5.3 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.

5.3.5.2.6.6 An ATN Air/Ground Router shall include the Mobile Subnetwork Capabilities Parameter, as defined in 5.8.2.1.3, 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.

5.3.5.2.6.7 ***Recommendation.****— 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 5.7.

b) Other types of subnetworks, an ATN Router should use the Data Link Start DLCP User Data facility to exchange the first ISH PDU.

5.3.5.2.6.8 ***Recommendation.—*** *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 5.7.

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 minimise the number of messages sent over limited bandwidth Mobile Subnetworks and the time taken to complete the route initiation procedures.

5.3.5.2.6.9 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.

5.3.5.2.6.10 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.

5.3.5.2.6.11 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.

5.3.5.2.6.12 A Systems Management notification shall be generated to report the arrival of the ISH PDU to the ATN Router's IS-SME.

5.3.5.2.7 Validation of the Received NET

5.3.5.2.7.1 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.

5.3.5.2.7.2 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.

5.3.5.2.7.3 If a BIS-BIS connection is acceptable then an Air/Ground Router shall apply the procedures of 5.3.5.2.8, and an Airborne Router shall apply the procedures of 5.3.5.2.9.

5.3.5.2.8 Determination of the Routing Information Exchange Procedure by an Air/Ground Router

5.3.5.2.8.1 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 5.3.5.2.10. 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 5.3.5.2.12 shall be applied.

5.3.5.2.9 Determination of the Routing Information Exchange Procedure by an Airborne Router

5.3.5.2.9.1 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 5.3.5.2.10 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 5.3.5.2.12 shall be applied.

5.3.5.2.10 Establishment of a BIS-BIS Connection

5.3.5.2.10.1 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.

5.3.5.2.10.2 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.

5.3.5.2.10.3 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 minimises 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.

5.3.5.2.10.4 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.

5.3.5.2.10.5 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.

5.3.5.2.10.6 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 5.8.

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 5.8.3.2.4.2.8). As a consequence, these routes are not affected by the changes and do not need to be re-advertised to the Airborne Router.

5.3.5.2.10.7 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.

5.3.5.2.10.8 This is an error and shall be reported to Systems Management; a BIS-BIS connection shall not be established in this case.

5.3.5.2.10.9 ***Recommendation.***— *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.*

5.3.5.2.10.10 ***Recommendation***.— *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.

5.3.5.2.11 Exchange of Routing Information using IDRP

5.3.5.2.11.1 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 5.3.7.2.

b) An Air/Ground Router shall advertise routes to the Airborne Router in accordance with the Routing Policy specified in 5.3.7.1.4 or 5.3.7.3.4 as appropriate for the role of the Air/Ground Router's RD.

5.3.5.2.11.2 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 5.3.5.2.6.11).

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 5.8.2.1.3) included in the options part of uplinked ISH PDU(s).

5.3.5.2.12 Procedures for the Optional Non-Use of IDRP over an Air/Ground Data Link

5.3.5.2.12.1 General

Note.— In this case, there is no recommendation to suppress the periodic re-transmission of ISH PDUs according to the ISO/IEC 9542 Report Configuration Function. In the absence of IDRP, this re-transmission is necessary to maintain the "liveness" of the connection.

5.3.5.2.12.1.1 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.

5.3.5.2.12.2 Air/Ground Router

5.3.5.2.12.2.1 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 optimise 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 5.8, 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.

5.3.5.2.12.2.2 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.

5.3.5.2.12.2.3 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.

5.3.5.2.12.2.4 This shall include re-update of the security information contained in routes received from the remote ATN Router, according to 5.8.

5.3.5.2.12.2.5 The IS-SME shall also ensure that a normal BIS-BIS connection does not concurrently exist with an ATN Router with the same NET.

5.3.5.2.12.2.6 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.

5.3.5.2.12.3 Airborne Router

5.3.5.2.12.3.1 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.

5.3.5.2.12.3.2 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.

5.3.5.2.13 Air/Ground Route Termination

5.3.5.2.13.1 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.

5.3.5.2.13.1.1 ***Recommendation.*** *— 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.*

5.3.5.2.13.1.2 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.

5.3.5.2.13.1.3 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.

5.3.5.2.13.2 Non-ISO/IEC 8208 Subnetworks

5.3.5.2.13.2.1 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.

5.3.5.2.13.3 Update of Routing Information

5.3.5.2.13.3.1 If, as a result of the procedures specified in 5.3.5.2.13.1 or 5.3.5.2.13.2 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 5.8.

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 5.8.3.2.4.2.8). 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 5.3.5.2.12.3 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.

5.3.5.2.13.3.2 If, as a result of the procedure 5.3.5.2.13.6 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 5.3.5.2.12.2 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 5.3.5.2.12.3 as a result of an ISH PDU having been received from the Air/Ground Router for which a loss of connectivity is reported.

5.3.5.2.13.3.3 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.

5.3.5.2.14 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).

5.3.5.2.14.1 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.

5.3.5.2.14.2 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.

5.3.5.2.14.3 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 5.7.6.2.1.5.4.8), 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 5.7.6.2.1.5.5.8), 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).

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).

5.3.5.2.15 Re-establishment of BIS-BIS Connection

5.3.5.2.15.1 The IS-SME shall attempt to re-establish a BIS-BIS connection using the procedures in 5.3.5.2.10 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 resynchronisation 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.

5.3.5.2.16 Procedures for Exchanging Authentication Information

Note.— During the ISH PDU exchange, the Airborne and Air/Ground Routers signal their intent to perform IDRP autentication type 2 by setting bit 1 of the value field of the ATN Data Link Capability Parameter (see 5.8.2.1.3) in the ISH PDU. In addition, the routers signal whether their respective peers are to send their public key certificate by setting bit 2 of the value field of this parameter. The Airborne Router sets bit 2 if local policy is for mutual authentication and an authentic public key for the Air/Ground Router has not been prestored. The Air/Ground Router sets bit 2 if access to a certificate delivery service is not available.

5.3.5.2.16.1 If an Airborne or Air/Ground Router's local policy permits IDRP authentication type 2, it shall set bit 1 of the value field of the ATN Data Link Capability Parameter (see 5.8.2.1.3) in the ISH PDU.

5.3.5.2.16.2 Exchange of Authentication Data by an Airborne Router

Note.— The following requirements apply to Airborne Routers which support ATN Security Services.

5.3.5.2.16.2.1 If local policy permits mutual type 2 authentication and the authentic public key of the peer Air/Ground Router has not been pre-stored, then the Airborne Router shall indicate in the ATN Data Link Capability Parameter that the public key certificate of the peer router is required, i.e. set bit 2 of the ATN Data Link Capability Parameter value field to 1 (see 5.8.2.1.3).

Note.— A pre-stored public key is considered authentic if the certificate path has been validated and it has not expired.

5.3.5.2.16.2.2 If local policy does not permit mutual authentication and/or the authentic public key of the Air/Ground Router has been pre-stored, then the Airborne Router shall indicate in the ATN Data Link Capability Parameter that the public key certificate is not required, i.e. set bit 2 of the ATN Data Link Capability Parameter value field to 0 (see 5.8.2.1.3).

Note.— It is anticipated that certificates for Air/Ground Routers will be short-lived and therefore, it may not be practical to pre-store these certificates.

5.3.5.2.16.3 Exchange of Authentication Data by an Air/Ground Router

Note.— The following requirements apply to Air/Ground Routers which support ATN Security Services.

5.3.5.2.16.3.1 If access to a supporting delivery service is not available, then the Air/Ground Router shall set bit 2 of the ATN Data Link Capability Parameter value field to 1 (see 5.8.2.1.3) to indicate that the public key certificate of the Airborne Router is required.

5.3.5.2.16.3.2 If access to a supporting delivery service is available, then the Air/Ground Router shall retrieve and validate the certificate path of the Airborne Router according to the procedure specified in 8.4.5.

Note.— Whether to perform validation prior to or after sending the ISH PDU is a local implementation issue.

5.3.5.2.16.3.3 If certificate path validation is performed prior to sending the ISH PDU and validation is successful, then the Air/Ground Router shall set bit 2 of the ATN Data Link Capability Parameter value field to 0 (see 5.8.2.1.3) to indicate that the public key certificate of the Airborne Router is not required.

5.3.5.2.16.3.4 If certificate path validation is performed prior to sending the ISH PDUand validation fails, then the Air/Ground Router shall not send the ISH PDU and an IDRP connection shall not be established.

Note.— The subnetwork connection processing (i.e. whether to clear or leave the subnetwork connection up) is a local matter.

5.3.5.2.16.3.5 If certificate path validation is performed subsequent to sending the ISH PDU, then the Air/Ground Router shall set bit 2 of the ATN Data Link Capability Parameter value field to 0 (see 5.8.2.1.3) to indicate that the public key certificate of the Airborne Router is not required.

Note.— 5.8.3.2.10.2.3.4 requires that public key certificate required be signalled in the OPEN PDU in the event that the Airborne Router's certificate can not be retrieved.

5.3.5.2.16.3.6 If certificate path validation is performed subsequent to sending the ISH PDU and validation fails, then an IDRP connection shall not be established.

Note.— The subnetwork connection processing (i.e. whether to clear or leave the subnetwork connection up) is a local matter.

5.3.5.2.17 APRL for Air/Ground Route Initiation

5.3.5.2.17.1 General

Item	**Description**	**ATN SARPs Reference**	**ATN Support**
jSubnet	Support of Subnetworks that do provide a Join Event	5.3.5.2	M
giSubnet	Support of Ground-Initiated Subnetworks	5.3.5.2	O.1
aiSubnet	Support of Air-Initiated Subnetworks	5.3.5.2	O.1
agSubnet	Support of Air- or Ground-Initiated Subnetworks	5.3.5.2	O.1
fsSubnet	Support of Subnetworks that support Fast Select	-	O
noIDRP-a	Support of optional non-use of IDRP by Airborne BIS	5.3.5.2.12.3	O

Item	Description	ATN SARPs Reference	ATN Support
noIDRP-ag	Support of optional non-use of IDRP by Air/Ground BIS	5.3.5.2.12.2	M
lvSubnet	Support of Subnetworks that provide a Leave Event	5.3.5.2.13	M
HoSubnet	Support of Subnetworks that provide a Handoff Event	5.3.5.2.14	O
auEXCG	Support of Exchanging Authentication Information	5.3.5.2.16	M

5.3.5.2.17.2 Airborne Router - Subnetwork Connection Responder

Item	Description	ATN SARPs Reference	ATN Support
respAR-ar	Response to incoming Call Request	5.3.5.2.2	giOragSubnet: M
valCR-ar	Validation of incoming Call Request	5.3.5.2.2	giOragSubnet:O
RespISH-ar	Generation of ISH PDU	5.3.5.2.6	giOragSubnet: M
ISHinCC-ar	Encoding ISH PDU in Call Accept User Data	5.3.5.2.6	RespISH-ar and fsSubnet: O
negNoIDRP-ar	Transmission of ISH PDU with SEL field of NET set to FEh	5.3.5.2.6	giOragSubnet and noIDRP-a:M
negIDRP-ar	Transmission of ISH PDU with SEL field of NET set to zero	5.3.5.2.6	giOragSubnet and ^noIDRP-a:M
dlCap-ar	Encoding of ATN Data Link Capability Parameter in ISH PDU	5.3.5.2.6.5	RespISH-ar:M
autoRoute-ar	Inference of available routes from received NET of A/G Router	5.3.5.2.12	giOragSubnet and noIDRP-a:M
initIDRP-ar	IDRP startup procedures - Invoke activate action	5.3.5.2.10	giOragSubnet and ^noIDRP-a:M
supISH-ar	Suppression of multiple ISH PDUs	5.3.5.2.10	giOragSubnet and ^noIDRP-a: O
valNET-ar	Validation of received NET	5.3.5.2.7	giOragSubnet and ^noIDRP-a: O
Handoff-ar	Processing of Handoff Event	5.3.5.2.14.1	HoSubnet:M

giOragSubnet: giSubnet or agSubnet

5.3.5.2.17.3 Airborne Router - Subnetwork Connection Initiator

Item	Description	ATN SARPs Reference	ATN Support
connect-ai	Connect on receipt of Join Event	5.3.5.2.3.2	EventDrvn:M
ValJoin-ai	Validation of Join Event	5.3.5.2.3.2	EventDrvn:O
SendISH-ai	Generation of ISH PDU	5.3.5.2.6	EventDrvn:M
ISHinCR-ai	Encoding of ISH PDU in Call Request	5.3.5.2.6	SendISH-ai and fsSubnet: O
negNoIDRP-ai	Transmission of ISH PDU with SEL field of NET set to FEh	5.3.5.2.8	EventDrvn and noIDRP-a:M
negIDRP-ai	Transmission of ISH PDU with SEL field of NET set to zero	5.3.5.2.8	EventDrvn and ^noIDRP-a:M
dlCap-ai	Encoding of ATN Data Link Capability Parameter in ISH PDU	5.3.5.2.6.5	SendISH-ai:M
autoRoute-ai	Inference of available routes from received NET of A/G Router	5.3.5.2.12.3	EventDrvn and noIDRP-a:M
initIDRP-ai	IDRP startup procedures - listenForOpen set to true	5.3.5.2.10	EventDrvn and ^noIDRP-a:M
supISH-ai	Suppression of multiple ISH PDUs	5.3.5.2.10	EventDrvn and ^noIDRP-a: O
valNET-ai	Validation of received NET	5.3.5.2.7	EventDrvn and ^noIDRP-a: O
RelateDTE-ai	Maintain relationship between originally Called and Returned Called DTE Address	5.3.5.2.3.2.2	HoSubnet: M
Handoff-ai	Processing of Handoff Event	5.3.5.2.14.4	HoSubnet: M

EventDrvn: jSubnet and (aiSubnet or agSubnet)

5.3.5.2.17.4 Air/Ground Router - Subnetwork Connection Responder

Item	Description	ATN SARPs Reference	ATN Support
respAR-agr	Response to incoming Call Request	5.3.5.2.2	aiOragSubnet: M
valCR-agr	Validation of incoming Call Request	5.3.5.2.2	aiOragSubnet:O

Item	Description	ATN SARPs Reference	ATN Support
RespISH-agr	Generation of ISH PDU	5.3.5.2.6	aiOragSubnet: M
ISHinCC-agr	Encoding ISH PDU in Call Accepted User Data	5.3.5.2.6	RespISH-agr and fsSubnet: O
dlCap-agr	Encoding of ATN Data Link Capability Parameter in ISH PDU	5.3.5.2.6.5	RespISH-agr:M
msCap-agr	Encoding of Mobile Subnetwork Capability Parameter in ISH PDU	5.3.5.2.6.6	RespISH-agr:M
negNoIDRP-agr	Receipt of ISH PDU with SEL field of NET set to FEh	5.3.5.2.8	aiOragSubnet:M
negIDRP-agr	Receipt of ISH PDU with SEL field of NET set to zero	5.3.5.2.8	aiOragSubnet:M
autoRoute-agr	Inference of available routes from received NET of Airborne Router	5.3.5.2.12.2	aiOragSubnet:M
initIDRP-agr	IDRP startup procedures - Invoke activate action	5.3.5.2.10	aiOragSubnet:M
supISH-agr	Suppression of multiple ISH PDUs	5.3.5.2.10	aiOragSubnet:O
valNET-agr	Validation of received NET	5.3.5.2.7	aiOragSubnet:O
Handoff-agr	Processing of Handoff Event	5.3.5.2.14.1	HoSubnet:M
valPrISH-agr	Support of Certificate Path Validation prior to ISH sending	5.3.5.2.16.3.3, 5.3.5.2.16.3.4	auEXCG:O.1
valSbISH-agr	Support of Certificate Path Validation subsequent to ISH sending	5.3.5.2.16.3.5, 5.3.5.2.16.3.6	auEXCG:O.1

aiOragSubnet: aiSubnet or agSubnet

5.3.5.2.17.5 Air/Ground Router - Subnetwork Connection Initiator

Item	Description	ATN SARPs Reference	ATN Support
connect-agi	Connect on receipt of Join Event	5.3.5.2.4	goOragSubnet: M
ValJoin-agi	Validation of Join Event	5.3.5.2.4	connect-agi: O
SendISH-agi	Generation of ISH PDU	5.3.5.2.6	connect-agi: M

Item	Description	ATN SARPs Reference	ATN Support
ISHinCR-agi	Encoding of ISH PDU in Call Request	5.3.5.2.6	Send-ISH-agi and fsSubnet: O
dlCap-agi	Encoding of ATN Data Link Capability Parameter in ISH PDU	5.3.5.2.6.5	SendISH-agi:M
msCap-agi	Encoding of Mobile Subnetwork Capability Parameter in ISH PDU	5.3.5.2.6.6	SendISH-agi:M
negNoIDRP-agi	Receipt of ISH PDU with SEL field of NET set to FEh	5.3.5.2.8	goOragSubnet:M
negIDRP-agi	Receipt of ISH PDU with SEL field of NET set to zero	5.3.5.2.8	goOragSubnet:M
autoRoute-agi	Inference of available routes from received NET of Airborne Router	5.3.5.2.12.2	goOragSubnet:M
initIDRP-agi	IDRP startup procedures - listenForOpen set to true	5.3.5.2.10	goOragSubnet:M
supISH-agi	Suppression of multiple ISH PDUs	5.3.5.2.10	goOragSubnet:O
valNET-agi	Validation of received NET	5.3.5.2.7	goOragSubnet:O
RelateDTE-agi	Maintain relationship between originally Called and Returned Called DTE Address	5.3.5.2.4.2	HoSubnet:M
Handoff-agi	Processing of Handoff Event	5.3.5.2.14.1	HoSubnet: M
valPrISH-agi	Support of Certificate Path Validation prior to ISH sending	5.3.5.2.16.3.3, 5.3.5.2.16.3.4	auEXCG:O.1
valSbISH-agi	Support of Certificate Path Validation subsequent to ISH sending	5.3.5.2.16.3.5, 5.3.5.2.16.3.6	auEXCG:O.1

goOragSubnet: giSubnet or agSubnet

5.3.5.2.17.6 Termination Procedures

Item	Description	ATN SARPs Reference	ATN Support
lvEvent	Processing of Leave Event	5.3.5.2.13	M
conLeave	Processing of a per connection Leave Event	5.3.5.2.13	M
subnetLeave	Processing of a per subnetwork Leave Event	5.3.5.2.13	M

5.3.6 Handling Routing Information

5.3.6.1 All ATN Routers in the same RD shall implement the same routing policy.

Note 1.— As specified in 5.8, 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 5.3.7 specifies the baseline Routing Policy for each class of RD identified in 5.2.2.2 to 5.2.2.5 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.

5.3.7 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.

5.3.7.1 Routing Policy Requirements for Members of an ATN Island Backbone RDC

5.3.7.1.1 General

5.3.7.1.1.1 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.

5.3.7.1.2 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.

5.3.7.1.2.1 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 characterised 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.

5.3.7.1.3 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.

5.3.7.1.3.1 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.

5.3.7.1.4 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.

5.3.7.1.4.1 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.

5.3.7.1.4.2 **Recommendation.**— *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.

5.3.7.1.5 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.

5.3.7.1.5.1 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 or 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 needs 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 RD's belonging to the organisation responsible for the Mobile RD (i.e. aircraft), or all the Mobile RDs belonging to the organisation. 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.

5.3.7.2 Routing Policy Requirements for a Mobile RD

5.3.7.2.1 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.

5.3.7.3 Routing Policy Requirements for an ATN TRD that is not a Member of the ATN Island Backbone RDC

5.3.7.3.1 General

5.3.7.3.1.1 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.

5.3.7.3.2 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.

5.3.7.3.2.1 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.

5.3.7.3.3 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.

5.3.7.3.3.1 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.

5.3.7.3.4 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.

5.3.7.3.4.1 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.

5.3.7.3.4.2 **Recommendation.**— *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.

5.3.7.4 The Routing Policy for a Fixed ATN ERD

5.3.7.4.1 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.

5.4 NETWORK AND TRANSPORT ADDRESSING SPECIFICATION

5.4.1 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.

5.4.1.1 Addressing Plan Scope

5.4.1.1.1 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.

5.4.1.2 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.

5.4.1.3 Reserved Values in Address Fields

5.4.1.3.1 Address field values specified as “reserved” shall not be used until assigned by future editions of this specification.

5.4.1.4 Values of Character Format Fields

5.4.1.4.1 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.

5.4.1.4.2 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.

5.4.1.4.3 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.

5.4.1.4.4 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.

5.4.2 Transport Layer Addressing

5.4.2.1 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.

5.4.2.2 ATN TSAP Selector

5.4.2.2.1 An ATN TSAP selector shall be either one or two octets in length.

5.4.2.2.2 The TSAP Selector field shall be administered on a local basis.

5.4.2.2.3 Valid ATN TSAP Selector field values shall be in the range **0** to **65535**.

5.4.2.2.4 The TSAP Selector field shall be encoded as an unsigned binary number.

5.4.2.2.5 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.

5.4.2.2.6 **Recommendation**.— *TSAP selector values in the range **0** to **255** should be encoded using one octet, higher values should be encoded using two octets.*

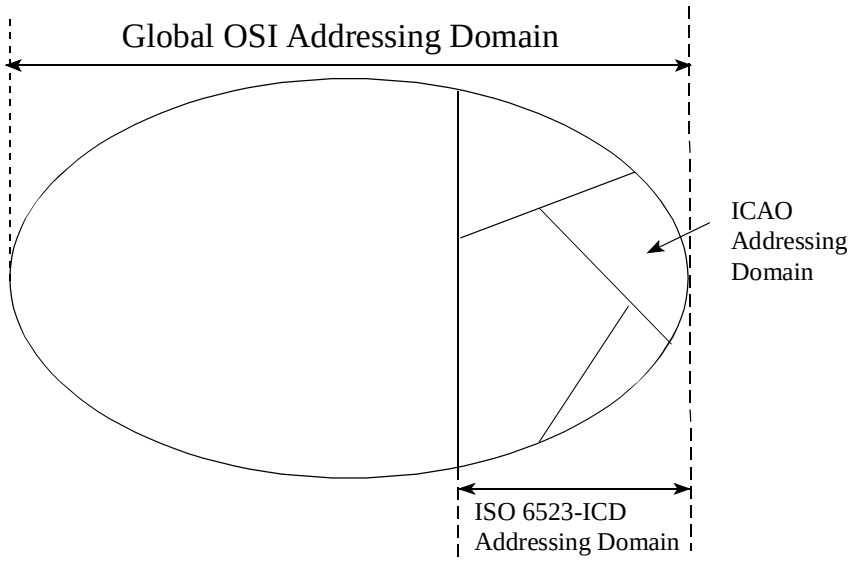


Figure 5.4-1 The Global OSI Network Addressing Domain

5.4.3 Network Layer Addressing

5.4.3.1 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.

5.4.3.2 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 5.4-1.

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 sub-divided into a number of sub-ordinate domains each characterised by a unique NSAP Address Prefix. Management of such sub-ordinate Network Addressing Domains may then be devolved to another Administrator.

5.4.3.2.1 An ATSC Network Addressing Domain shall be a Network Addressing Domain administered by an ATSC authority.

5.4.3.2.2 An AINSC Network Addressing Domain shall be a Network Addressing Domain administered by a member of the Aeronautical Industry.

5.4.3.2.3 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.

5.4.3.3 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 5.4-2 below.

Figure 5.4-2 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.

5.4.3.4 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.

5.4.3.4.1 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.

5.4.3.4.2 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.

5.4.3.5 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.

5.4.3.5.1 **Recommendation**.— *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.

5.4.3.5.2 Each successive pair of hexadecimal digits shall correspond to the next binary octet of the DSP.

5.4.3.6 The ATN NSAP Address Format

Note 1.— The derivation of the ATN NSAP Address Format is illustrated in Figure 5.4-3. 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 co-ordinate 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.

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 onboard 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.

5.4.3.7 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 emphasise 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.

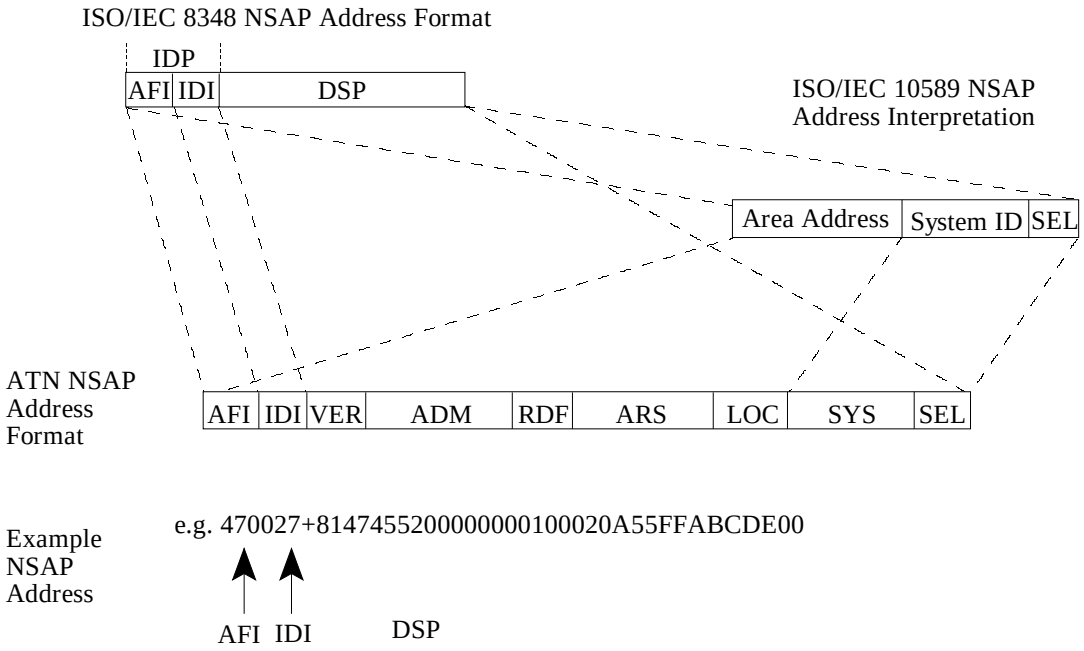


Figure 5.4-3 Derivation of the ATN NSAP Address Format

5.4.3.8 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 5.4-1.

5.4.3.8.1 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 summarised in Table 5.4-2.

5.4.3.8.1.1 The VER Field shall be one octet in length.

5.4.3.8.1.2 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.

5.4.3.8.1.3 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.

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

Table 5.4-1 DSP NSAP Address Field Sizes

5.4.3.8.1.4 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.

5.4.3.8.1.5 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.

5.4.3.8.1.6 All other VER field values shall be reserved.

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

Table 5.4-2 VER Field Assigned Values

5.4.3.8.2 The Administration (ADM) Field

5.4.3.8.2.1 General

Note.— The purpose of the ADM field is to sub-divide 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 Organisation.

5.4.3.8.2.1.1 The ADM field shall be three octets in length.

5.4.3.8.2.2 Fixed AINSC NSAP Addresses and NETs

Note.— In the Fixed AINSC Network Addressing Domain, the ADM field is used to sub-divide 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 Organisation.

5.4.3.8.2.2.1 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 organisation identified by the value of the ADM field.

5.4.3.8.2.2.2 **Recommendation**.— *The field value should be derived from the set of three-character alphanumeric symbols representing an IATA Airline or Aeronautical Stakeholder Designator, according to 5.4.1.4.*

Note.— AINSC Organisations are intended to register their ADM values with IATA.

5.4.3.8.2.3 Fixed ATSC NSAP Addresses and NETs

Note.— In the Fixed ATSC Network Addressing Domain, the ADM field is used to sub-divide 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.

5.4.3.8.2.3.1 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.

5.4.3.8.2.3.2 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.

5.4.3.8.2.3.3 In this case, the value of the field shall be determined according to 5.4.1.4.

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.

5.4.3.8.2.3.4 When used to identify an ICAO Region, the first octet of the ADM field shall identify the ICAO Region, according to Table 5.4-3, while the values of the remaining two octets shall be assigned by the identified ICAO Region.

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 5.4-3 do not conflict with ISO 3166 derived State 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

Table 5.4-3 ICAO Region Identifiers

Note 2.— This Addressing Plan enables ICAO Regions to allocate ADM field values in the Fixed ATSC Network Addressing Domain to States and Organisations 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 5.3.7.1.4.2.

5.4.3.8.2.3.5 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.

5.4.3.8.2.4 Mobile NSAP Addresses and NETs

Note.— In both the Mobile AINSC and the Mobile ATSC Network Addressing Domains, the ADM field is used to sub-divide 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.

5.4.3.8.2.4.1 For Mobile AINSC NSAP Address and NETs, the ADM field value shall be set according to 5.4.3.8.2.2, and the corresponding sub-ordinate Network Addressing Domain administered by the organisation identified by the value of the ADM field.

5.4.3.8.2.4.2 For Mobile ATSC NSAP Address and NETs, the ADM field value shall be set according to 5.4.3.8.2.3, and the corresponding sub-ordinate Network Addressing Domain administered by the State identified by the value of the ADM field.

5.4.3.8.3 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 co-ordinated 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.

5.4.3.8.3.1 The RDF field shall be one octet in length and its value shall be [0000 0000] in binary.

5.4.3.8.3.2 All other values shall be reserved.

5.4.3.8.4 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 Organisation.

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 onboard an aircraft form a single Routing Domain, then the ARS field also identifies the Routing Domain. When the systems onboard an aircraft form multiple RDs, then part of the LOC field is used to distinguish them.

5.4.3.8.4.1 The ARS field shall be three octets in length.

5.4.3.8.4.2 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 Organisation 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.

5.4.3.8.4.3 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 5.4.3.8.5), be used to uniquely identify the Routing Areas within those Routing Domains.

5.4.3.8.4.4 In the Fixed AINSC and ATSC Network Addressing Domains, the State or Organisation 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.

5.4.3.8.4.5 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.

5.4.3.8.5 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.

5.4.3.8.5.1 The LOC field shall be two octets in length and may be given any binary value.

5.4.3.8.5.2 The administrator of the Network Addressing Domain that co-incides 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.

5.4.3.8.6 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.

5.4.3.8.6.1 In an ATN NSAP Address or NET, the System Identifier (SYS field) shall be six octets in length.

5.4.3.8.6.2 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.

5.4.3.8.7 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).

5.4.3.8.7.1 The SEL field shall be one octet in length.

5.4.3.8.7.2 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.

5.4.3.8.7.3 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].

5.4.3.8.7.4 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.

5.4.3.8.7.5 SEL field values other than those defined for Intermediate System Network Entities in 5.4.3.8.7.2 and 5.4.3.8.7.3 above or being reserved, shall be assigned by the addressing authority responsible for the identified End or Intermediate System.

5.4.3.9 Pre-Defined NSAP Address Prefixes

5.4.3.9.1 All AINSC Mobiles

5.4.3.9.1.1 The NSAP Address Prefix 470027+41 shall provide a common NSAP Address Prefix for all AINSC Mobiles.

5.4.3.9.2 All ATSC Mobiles

5.4.3.9.2.1 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.

5.4.3.9.3 All Aircraft Belonging to an Airline

5.4.3.9.3.1 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.

5.4.3.9.4 All General Aviation and Other Types of Aircraft Registered by a State

5.4.3.9.4.1 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.

5.5 TRANSPORT SERVICE AND PROTOCOL SPECIFICATION

5.5.1 General

5.5.1.1 Overview

5.5.1.1.1 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.

5.5.1.1.2 In ATN End Systems, the implementation of the COTP shall conform to ISO/IEC 8073 and the mandatory requirements given in this Chapter.

5.5.1.1.3 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.

5.5.1.1.4 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.

5.5.1.2 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 Table 1-2;

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 1-1, 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 5.6-1. The encoding of the ATN Security Label is specified in Figure 5.6-1 and 5.6.2.2.2.2 bullet b).

Note 6.— The TS-user is not required to specify any other Transport Service Quality of Service parameters.

5.5.1.3 Transport Service Access Point Addresses

5.5.1.3.1 A TSAP address shall comprise two elements, a NSAP address and a TSAP selector.

5.5.1.3.2 The NSAP address and the TSAP selector shall conform to the provisions in 5.4.

5.5.1.4 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.

5.5.1.4.1 The transport entity shall support Transport-Selector parameters to accommodate the ATN TSAP selector syntax and encoding requirements as specified in 5.4.

5.5.1.4.2 **Recommendation**.— *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.

5.5.1.4.3 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.

5.5.1.4.4 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.

5.5.1.4.5 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.

5.5.1.4.6 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.

5.5.2 Connection Mode Transport Layer Operation

5.5.2.1 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.

5.5.2.2 ATN Specific Requirements

5.5.2.2.1 ATN End Systems shall implement the ISO/IEC 8073 Class 4 transport protocol in order to provide Connection Mode communications over the ATN Internet.

5.5.2.2.2 The COTP shall operate using the CLNS (Connectionless Network Service) as specified in 5.6.

Note.— TPDUs (Transport Protocol Data Units) are sent via the N-UNITDATA Request primitive.

5.5.2.2.3 The transport entity shall not concatenate TPDUs from TCs with different transport priorities or different Security Labels.

5.5.2.2.4 **Recommendation.—** *The Selective Acknowledgement mechanism should be used for conservation of bandwidth by preventing retransmission of correctly received out-of-sequence TPDUs.*

5.5.2.2.5 **Recommendation.—** *The Request of Acknowledgement mechanism should be used to reduce AK traffic.*

5.5.2.2.6 **Recommendation. —** *The maximum TPDU size should be at least 1024 octets.*

Note.— This is to support efficient transmission of anticipated application data exchanges.

5.5.2.2.7 **Recommendation.—** *The Transport Layer should propose a TPDU size of at least 1024 octets.*

5.5.2.2.8 **Recommendation**.— *The Transport Layer should use the TPDU size parameter rather than the preferred maximum TPDU size parameter.*

5.5.2.2.9 **Recommendation**.— *Implementations of the ATN Transport Layer should propose use of normal format in the CR TPDU.*

5.5.2.2.10 **Recommendation.**— *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.

5.5.2.2.11 **Recommendation.**— *The Transport Layer should accept non-use of checksum when proposed in a CR TPDU.*

5.5.2.2.12 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.

5.5.2.2.13 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 5.5-1.

5.5.2.2.13.1 **Recommendation**.— *When intended for operation over Air/Ground subnetworks, the nominal values indicated in Table 5.5-1 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 5.5.2.8). The recommended algorithms for the dynamic computation of the Local Retransmission Time are specified in 5.5.2.8.

5.5.2.2.13.2 **Recommendation**.— *The assignment of initial values for timers and parameters other than the nominal values indicated in Table 5.5-1 should be based on operational experience.*

5.5.2.2.14 **Recommendation**.— *When intended for operation exclusively over Ground/Ground subnetworks, implementations of transport protocol timer values should be optimized to ensure interoperability.*

Table 5.5-1 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

Name	Description	Minimum Value	Nominal Value	Maximum Value
R	Persistence Time, seconds	1	405	6310
N	Maximum Number of Transmissions	1	3	10
L	Time bound on reference and/or sequence numbers, seconds	160	1206	7910
I	Inactivity Time, seconds	600	4500	6000
W	Window Time, seconds	160	4000	5500

Note 1.— In Table 5.5-1, 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 5.5-1 may not be directly configurable. They may be determined based on the relationships defined in clause 12.2.1.1 of ISO/IEC 8073.

5.5.2.3 Connection Mode Transport Quality of Service

5.5.2.3.1 Connection Mode Transport Priority

5.5.2.3.1.1 The Transport Layer shall allow a TC (Transport Connection) priority in the range [0 - 14]

5.5.2.3.1.2 The Transport Layer shall not alter the proposed TC priority specified by the TS-user.

5.5.2.3.1.3 The Transport Layer shall treat all connections without expressed priority as being at the default TC priority.

5.5.2.3.1.4 The default TC priority shall be the lowest priority, i.e. priority **[14]**.

5.5.2.3.1.5 When a TS-user specifies a TC priority, the relationship between this TC priority and the CLNP priority shall be as specified in Table 1-2.

5.5.2.3.2 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.

5.5.2.3.2.1 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 5.2.7.3.1.

5.5.2.3.2.2 The Security Label format shall be according to 5.2.7.1. 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.

5.5.2.3.3 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.

5.5.2.3.3.1 The Transport Layer shall allow a TS-user to specify a Residual Error Rate as three qualitative levels, i.e. low, medium and high.

5.5.2.3.3.2 When supported, a low Residual Error Rate shall correspond to the use of the extended 32-bit checksum described in 5.5.4. Otherwise, a low residual error rate shall be equivalent to a medium Residual Error Rate.

5.5.2.3.3.3 A medium Residual Error Rate shall correspond to the use of the 16-bit TPDU checksum specified in ISO/IEC 8073.

5.5.2.3.3.4 A high Residual Error Rate shall correspond to non-use of any transport layer checksum.

5.5.2.4 Encoding of Transport Protocol Data Units

5.5.2.4.1 General

5.5.2.4.1.1 The encoding of TPDUs shall conform to ISO/IEC 8073 for the COTP.

5.5.2.4.2 Encoding of the Acknowledgment Time Parameter

5.5.2.4.2.1 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 65536 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.

5.5.2.4.3 Encoding of the Extended 32-bit Checksum Parameter

5.5.2.4.3.1 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 5.5.4.5

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 unrecognised. 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.

5.5.2.5 Transport Layer Congestion Avoidance

5.5.2.5.1 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.

5.5.2.5.1.1 The transport entity shall implement the congestion avoidance algorithm defined in this section.

5.5.2.5.1.2 This algorithm shall be applied for each transport connection individually.

5.5.2.5.2 Advertised Window

5.5.2.5.2.1 General

5.5.2.5.2.1.1 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.*

5.5.2.5.2.2 Initialisation of the Advertised Window

5.5.2.5.2.2.1 The initial value of the window W_0 that is advertised to the sending transport entity shall have a locally configurable value.

5.5.2.5.2.2.2 This initial window shall be sent to the sending transport entity in the first CDT field transmitted.

5.5.2.5.3 Receiving Transport Entity Congestion Avoidance

5.5.2.5.3.1 General

5.5.2.5.3.1.1 Congestion avoidance shall be performed within repeated update phases.

5.5.2.5.3.1.2 Each update phase shall terminate with the possible advertisement of a new window size to the sending transport entity.

5.5.2.5.3.2 Start of Update Phase

5.5.2.5.3.2.1 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.

5.5.2.5.3.3 Ignoring Congestion Information

5.5.2.5.3.3.1 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.

5.5.2.5.3.3.2 When the sending transport entity advertises the initial window size W_0, it shall set W to 0.

5.5.2.5.3.4 Sampling Congestion Information

5.5.2.5.3.4.1 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.

.

5.5.2.5.3.4.2 Upon entering the sampling sub-phase, these counts shall be reset to zero.

5.5.2.5.3.4.3 These counts shall be updated upon receipt of a DT-TPDU using the congestion information supplied by the Network Layer.

5.5.2.5.3.4.4 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.

5.5.2.5.3.5 Action Upon the End of the Update Phase

5.5.2.5.3.5.1 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.

5.5.2.5.4 Recommended Algorithm Values

5.5.2.5.4.1 **Recommendation.**— *The value settings defined in the following table should be implemented and configurable by a System Manager:*

Table 5.5-2. Congestion Avoidance algorithm values

Name	Description	Recommended value/range
β	Window decrease factor	0.75 to 0.95
δ	Window increase amount	1
W_0	Initial window	1
λ	Congestion ratio	50 %

5.5.2.6 Use of the ATN Network Service

Note.— This section specifies how the COTP operates over the CLNS provided by the ATN Network Layer.

5.5.2.6.1 Use of the N-UNITDATA Request

5.5.2.6.1.1 General

5.5.2.6.1.1.1 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.

5.5.2.6.1.1.2 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.

5.5.2.6.1.2 NS-user-data

Note.— Transport entities transmit TPDUs as NS-user-data of the N-UNITDATA Request primitive.

5.5.2.6.1.3 Network Service Access Point Addresses

Note.— The Transport Layer has knowledge of the source and destination address parameters only as octet strings.

5.5.2.6.1.4 Network Quality of Service

5.5.2.6.1.4.1 General

5.5.2.6.1.4.1.1 The COTP shall use the network QoS parameters as defined in the sections below.

5.5.2.6.1.4.2 Network Layer Priority

5.5.2.6.1.4.2.1 The COTP shall use the network priority parameter to indicate the relative priority of a NSDU.

5.5.2.6.1.4.2.2 When a transport priority has been specified, the value of network priority shall be determined based on the transport connection priority, as defined in Table 1-2.

5.5.2.6.1.4.2.3 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. Table 1-2 defines the required mapping between these two schemes for use by ATN systems.

5.5.2.6.1.4.3 Network Layer Security

Note.— The use of the Network Layer security is specified in 5.2.7.3.1.

5.5.2.6.2 Use of the N-UNITDATA Indication

5.5.2.6.2.1 General

5.5.2.6.2.1.1 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.

5.5.2.6.2.2 NS-user-data

Note.— Transport entities receive TPDUs as NS-user-data of the N-UNITDATA Indication primitive.

5.5.2.7 Connection Mode Transport APRL

5.5.2.7.1 Mandatory and Optional Functions

5.5.2.7.1.1 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.

5.5.2.7.1.1.1 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 with these SARPs.

5.5.2.7.1.2 Protocol Implementation

5.5.2.7.1.2.1 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
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

5.5.2.7.1.2.2 Specific ATN Requirements

Index	Feature	SARPs Reference	ATN Support
ATN1	Support of Congestion Avoidance Procedures?	5.5.2.5	M
ATN2	Transport to Network Priority Mapping?	5.5.2.6.1.4.2	M
ATN3	Support of ATN Security Label?	5.5.2.6.1.4.3	M
ATN4	Configurable Transport Timers?	5.5.2.2.12	M
ATN5	Enhanced encoding of Acknowledgment Time Parameter?	5.5.2.4.2	M
ATN6	Support of Extended 32-bit Checksum?	5.5.4	M
ATN7	Dynamic Local Retransmission Time Adaptation?	5.5.2.8	M

5.5.2.7.1.3 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

Index		ISO/IEC 8073 References	ISO Status	ATN Support
IR2	Responding to CR TPDU	14.5 a)	O.2	M

5.5.2.7.1.4 Supported Functions

5.5.2.7.1.4.1 Supported Functions for Class 4 (C4 or C4L::)

5.5.2.7.1.4.1.1 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
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

5.5.2.7.1.4.1.2 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

5.5.2.7.1.4.1.3 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

5.5.2.7.1.5 Supported TPDUs

Index	TPDUs		ISO/IEC 8073 References	ISO Status	ATN Support
ST1	CR	supported on transmission	13.1	IR1:M	M

Index	TPDUs		ISO/IEC 8073 References	ISO Status	ATN Support
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.— The following table states for which classes, if any, ER TPDU is supported on transmission.

Index	Class	ISO/IEC 8073 References	ISO Status	ATN Support
SER4L	ER support on transmission of Class 4 over CLNS	6.22.2	O	O

5.5.2.7.1.6 Supported Parameters of Issued TPDUs

5.5.2.7.1.6.1 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

5.5.2.7.1.6.1.1 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

5.5.2.7.1.6.2 Supported parameters for Class 4 TPDUs (C4L::)

5.5.2.7.1.6.2.1 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
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

Index	Supported parameters	ISO/IEC 8073 References	ISO Status	ATN Support
I4CR18	Preferred maximum TPDU size	13.3.4 c)	O	O
I4CR19	Inactivity timer	13.3.4 r)	O	M

5.5.2.7.1.6.2.2 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.

5.5.2.7.1.6.2.3 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

5.5.2.7.1.6.2.4 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

5.5.2.7.1.6.2.5 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

5.5.2.7.1.6.2.6 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

5.5.2.7.1.6.2.7 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

5.5.2.7.1.6.2.8 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

5.5.2.7.1.7 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.

5.5.2.7.1.7.1 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

5.5.2.7.1.8 User Data in Issued TPDUs

5.5.2.7.1.8.1 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

Index	User Data	ISO/IEC 8073 References	ISO Status	ATN Support
D4IDR	User data of up to 64 octets in a DR	13.5.5	M	M

5.5.2.7.1.9 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

5.5.2.7.1.10 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.

5.5.2.7.1.10.1 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.

5.5.2.7.1.10.2 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
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.

5.5.2.7.1.10.3 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 1024 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, 1024, 2048, 4096, 8192	One of 128, 256, 512, 1024, 2048, 4096, 8192
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, 1024, 2048, 4096, 8192	128, 256, 512, 1024, 2048, 4096, 8192

5.5.2.7.1.10.4 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.

5.5.2.7.1.10.5 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.— Expedited data is proposed using the Additional Options Parameters in the CR and CC TPDUs.

5.5.2.7.1.10.6 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.

5.5.2.7.1.10.7 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

5.5.2.7.1.10.8 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

5.5.2.7.1.11 Error Handling

Note.— Using Class 4 over CLNS, a TPDU with an invalid checksum will be discarded.

5.5.2.7.1.11.1 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.

5.5.2.7.1.11.2 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
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

Index	Event	ISO/IEC 8073 Reference	ISO Allowed Value	ATN Supported Value
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.

5.5.2.7.1.11.3 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

5.5.2.7.1.12 Class 4 Timers and Protocol Parameters

Index		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	I_L (Local Inactivity Time)	12.2.1.1.7	M	M
TA4	W (Window Update)	12.2.1	M	M
TA5	L (Frozen Reference Time)	12.2.1.1.6	M	M

Index		ISO/IEC 8073 References	ISO Status	ATN Support
ATN-TA1	R (Persistence)	12.2.1.1.5	O	O

Index		ISO/IEC 8073 References	ISO Status	ATN Support
ATN-TA2	M_{LR} (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA3	M_{RL} (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA4	E_{LR} (Maximum Transit Delay)	12.2.1.1.2	O	O
ATN-TA5	E_{RL} (Maximum Transit Delay)	12.2.1.1.2	O	O
ATN-TA6	A_L (Acknowledgement Time)	12.2.1.1.3	O	M
ATN-TA7	A_R (Acknowledgement Time)	12.2.1.1.3	O	M
ATN-TA8	I_R (Remote Inactivity Time)	12.2.1.1.7	O	M

Note.— According to ISO, the following applies to an implementation under test (IUT):

Index		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

5.5.2.7.1.13 Extended 32-bit Checksum

Index		ATN SARPs Reference	ATN Support
ETC1	Extended 32-bit Checksum in CR TPDU	5.5.4.2	ATN6:M
ETC2	Extended 32-bit Checksum in CC TPDU	5.5.4.3.2	ETC1:M
ETC3	ISO/IEC 8073 Checksum Parameter in CC TPDU	5.5.4.3.2 b)	ETC1:X
ETC4	Rejection of Use of 16-bit Checksum in CC TPDU	5.5.4.3.2 c)	ETC1:M
ETC5	Extended 32-bit Checksum in all subsequent TPDUs	5.5.4.3.4	(ETC1 and ETC2):M
ETC6	Encoding of Extended 32-bit Checksum	5.5.2.4.3.1	ATN6:M
ETC7	Computation of Extended 32-bit Checksum	5.5.4.4	ATN6:M
ETC8	Validation of Extended 32-bit Checksum	5.5.4.6	ATN6:M

5.5.2.8 Dynamic Local Retransmission Time Adaptation

5.5.2.8.1 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 time out interval every time a new packet is acknowledged.

5.5.2.8.2 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.

5.5.2.8.2.1 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 respectively. Acknowledgement of a DT TPDU corresponds to the receipt of an AK TPDU.

5.5.2.8.2.2 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.

5.5.2.8.2.3 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.

5.5.2.8.2.4 If one or more retransmissions of one or more TPDUs being acknowledged occured 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.

5.5.2.8.3 Retransmission Time Calculation

5.5.2.8.3.1 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).

5.5.2.8.3.2 **Recommendation.**— *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.*

5.5.2.8.3.3 **Recommendation.**— *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.

5.5.2.8.3.4 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.

5.5.2.8.4 Retransmission Time Backoff Procedure

5.5.2.8.4.1 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.

5.5.2.8.4.2 If as a result of this procedure the Local Retransmission Time exceeds its maximum value (see 5.5.2.8.5), then the Local Retransmission Time shall be set to its maximum value.

5.5.2.8.4.3 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.

5.5.2.8.5 Initial, Minimum and Maximum Local Retransmission Time Value

5.5.2.8.5.1 The transport entity shall maintain the value of the Local Retransmission Time within a bounded range.

5.5.2.8.5.2 The lower and upper bound of the Local Retransmission Time shall be configurable.

5.5.2.8.5.3 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 5.5-1.

5.5.2.8.5.4 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 5.5-1.

5.5.2.8.5.5 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.

5.5.3 Connectionless Mode Transport Protocol Operation

5.5.3.1 Connectionless Mode Transport Protocol Overview

5.5.3.1.1 ATN End Systems shall implement the ISO/IEC 8602 transport protocol in order to provide Connectionless Mode communications over the ATN Internet.

Note.— The ATN CLTS model conforms to the service model defined in ISO/IEC 8072.

5.5.3.1.2 The CLTP shall operate over the CLNS provided by the ATN Network Layer, according to the provisions in 5.5.3.5.

5.5.3.2 Connectionless Mode Transport Service Primitives

Note 1.— For the purposes 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.— ISO/IEC 8072 limits CL user-data to a maximum of 63488 octets per TSDU.

Note 3.— There is no requirement to implement the service specified in ISO/IEC 8072 as a software interface.

5.5.3.2.1 T-UNITDATA Request

5.5.3.2.1.1 The source and destination Transport Addresses shall conform to the ATN Transport Layer Addressing provisions as specified in 5.4.

5.5.3.2.2 T-UNITDATA Indication

Note.— All of the associated parameter values are equal to the values passed to the TS provider via the T-UNITDATA Request primitive, except possibly the QoS parameter values.

5.5.3.3 ATN Connectionless Mode Transport Quality of Service Parameters

5.5.3.3.1 General

5.5.3.3.1.1 The Transport Layer shall support the use of checksums on a per TSDU (Transport Service Data Unit) basis.

Note.— The actual use of this feature will be dependant upon the application's requirements.

5.5.3.3.2 Priority

5.5.3.3.2.1 The transport entity providing the connectionless mode transport service shall allow a TS-user to specify TSDU priority in the range [0-14].

Note.— The CLTP itself does not support a priority field in the TPDU.

5.5.3.3.3 Security

5.5.3.3.3.1 The transport entity providing the connectionless mode transport service shall allow a TS-user to specify the ATN Security Label in the T-UNITDATA request.

Note.— The CLTP itself does not support a security parameter field in the TPDU.

5.5.3.3.4 Residual Error Rate

Note.— Three qualitative levels of RER are possible for use with the connectionless transport service. These correspond to no checksums, use of the 16-bit checksum specified in ISO/IEC 8602, and the Extended 32-bit Checksum described in this specification.

5.5.3.3.4.1 The Transport Layer shall allow a TS-user to specify a Residual Error Rate as three qualitative levels, i.e. low, medium and high.

5.5.3.3.4.2 When supported, a low Residual Error Rate shall correspond to the use of the Extended 32-bit Checksum described in 5.5.4. Otherwise, a low residual error rate shall be equivalent to a medium Residual Error Rate.

5.5.3.3.4.3 A medium Residual Error Rate shall correspond to the use of the 16-bit TPDU checksum described in ISO/IEC 8602.

5.5.3.3.4.4 A high Residual Error Rate shall correspond to non-use of any transport layer checksum.

5.5.3.4 Encoding of Transport Protocol Data Units

5.5.3.4.1 The encoding of TPDUs shall conform to ISO/IEC 8602 for the CLTP.

5.5.3.5 Use of the ATN Network Service

Note.— This section specifies how the CLTP operates over the CLNS provided by the ATN Network Layer.

5.5.3.5.1 Use of the N-UNITDATA Request

5.5.3.5.1.1 General

5.5.3.5.1.1.1 The Transport Layer shall use the N-UNITDATA Request Primitive, as defined in ISO/IEC 8602, to transmit TPDUs.

5.5.3.5.1.2 NS-user-data

Note.— Transport Entities transmit TPDUs as NS-user-data of the N-UNITDATA Request primitive.

5.5.3.5.1.3 Network Service Access Point Addresses

Note.— The Transport Layer has knowledge of source and destination address parameters only as octet strings.

5.5.3.5.1.4 Network Quality of Service

5.5.3.5.1.4.1 General

5.5.3.5.1.4.1.1 The transport entity providing the connectionless mode transport service shall use the network QoS parameters as defined in the sections below.

5.5.3.5.1.4.2 Network Layer Priority

5.5.3.5.1.4.2.1 The transport entity providing the connectionless mode transport service shall use the network priority parameter to indicate the relative priority of an NSDU. The NSDU priority shall be determined from the TSDU priority, using the mapping given in Table 1-2.

5.5.3.5.1.4.3 Network Layer Security

5.5.3.5.1.4.3.1 The transport entity providing the connectionless mode transport service shall use the Security Label provided in the T-UNITDATA request as the value of the N-UNITDATA security parameter.

5.5.3.5.2 Use of the N-UNITDATA Indication

Note.— Following ISO/IEC 8602, the Transport Layer receives TPDUs from the Network Layer-provided N-UNITDATA Indication primitive.

5.5.3.5.2.1 Network Quality of Service

5.5.3.5.2.1.1 To meet the ISO/IEC 8072 service specification, the transport entity providing the connectionless mode transport service shall translate the received NSDU priority to the TSDU priority using the mapping shown in Table 1-2.

5.5.3.6 ATN Connectionless Mode Transport APRL

Note.— The requirements for the CLTP are provided in the form of an APRL. The APRL has been prepared using the PICS proforma provided with ISO/IEC 8602.

5.5.3.6.1 General

5.5.3.6.1.1 An implementation of the ISO/IEC 8602 Transport Protocol shall be used in an ATN End System if and only if its PICS is in compliance with the APRL provided with these SARPs.

5.5.3.6.2 Protocol Implementation

Item	**Protocol Function Support**	**ISO/IEC 8602 Reference**	**ISO Status**	**ATN Support**
NS	Network service selection	5.3.2.2	M	M
AM	Address mapping	5.3.2.3	M	M

Item	Protocol Function Support	ISO/IEC 8602 Reference	ISO Status	ATN Support
	PDU Support			
UD1	Unitdata PDU supported on transmission	6.1.3	M	M
UD2AM	Unitdata PDU supported on reception	6.1.3	M	M
	Parameters of the Unitdata PDU on Transmission			
TpTc	<t> TPDU UD Checksum	6.2.4.1, ATN SARPs Reference: 5.5.4.4	O	RER_Medium :M, RER_High or (RER_Low and ATN6):X
TpTs	<t> TPDU UD Source Transport-Selector	6.2.4.1	M	M
TpTd	<t> TPDU UD Destination Transport-Selector	6.2.4.1	M	M
TpTu	<t> TPDU UD User Data	6.2.4.1	M	M
TpTetc	<t> TPDU UD Extended 32-bit Checksum	ATN SARPs Reference: 5.5.4.4.1	--	(RER_Low and ATN6):M
	Parameters of the Unitdata PDU on Reception			
TpRc	<r> TPDU UD Checksum	6.2.4.2	M	M
TpRs	<r> TPDU UD Source Transport-Selector	6.2.4.2	M	M
TpRd	<r> TPDU UD Destination Transport-Selector	6.2.4.2	M	M
TpRu	<r> TPDU UD User Data	6.2.4.2	M	M
TpRetc	<r> TPDU UD Extended 32-bit Checksum	ATN SARPs Reference: 5.5.4.1.1	--	M
	Service Support			
CL	Connectionless Mode Network Service	6.2	M	M

RER_Low: if low RER requested **then** true **else** false
RER_Medium: if medium RER requested **then** true **else** false
RER_High: if high RER requested **then** true **else** false

5.5.4 Extended 32-bit Checksum

5.5.4.1 General

5.5.4.1.1 When present in a TPDU, the Extended 32-bit Checksum parameter shall be validated using the algorithm specified in 5.5.4.6.

5.5.4.1.2 If the validation fails, the TPDU shall be discarded without further processing.

5.5.4.2 Negotiating the Use of Extended 32-bit Checksum in Transport Connections

5.5.4.2.1 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 5.5.4.4 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.

5.5.4.2.2 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.

5.5.4.2.3 The value of the ISO/IEC 8073 checksum parameter shall be set to zero before the Extended 32-bit Checksum is computed.

5.5.4.2.4 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.

5.5.4.2.5 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.

5.5.4.3 Accepting the Use of Checksums

5.5.4.3.1 A CR TPDU that does not contain an Extended 32-bit Checksum parameter shall be processed in compliance with ISO/IEC 8073.

5.5.4.3.2 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 5.5.4.6 and, in order to signal acceptance of Extended 32-bit Checksum:

a) Compute and include an Extended 32-bit Checksum parameter, as specified in 5.5.4.4, 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 respevctively.

5.5.4.3.3 The ISO/IEC 8073 checksum shall be verified as correct before the Extended 32-bit Checksum is verified.

5.5.4.3.4 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 5.5.4.4, 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.

5.5.4.3.5 If a TPDU other than a CR TPDU includes both an Extended 32-bit Checksum parameter and an ISO/IEC 8073 checksum parameter shall be considered as a protocol error.

5.5.4.3.6 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.

5.5.4.3.7 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.

5.5.4.4 Use in Connectionless Mode

5.5.4.4.1 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 5.5.4.4 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 unrecognised parameter.

5.5.4.4.2 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.

5.5.4.4.3 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.

5.5.4.5 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.

5.5.4.5.1 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).

5.5.4.5.2 Arithmetic Conventions

5.5.4.5.2.1 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) shall be regarded as though it were plus zero (i.e. 0).

5.5.4.5.3 Algorithm for Generating the Checksum Parameter

5.5.4.5.3.1 The complete TPDU with the Extended 32-bit Checksum Parameter value field set to zero shall be set up.

5.5.4.5.3.2 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.

5.5.4.5.3.3 The Extended 32-bit Checksum shall be created by the following algorithm:

1) Initialise 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.

5.5.4.6 Algorithm for Checking the Checksum Parameter

5.5.4.6.1 The transport entity shall appended 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.

5.5.4.6.2 The value of the Extended 32-bit Checksum Parameter shall be set to zero.

5.5.4.6.3 If the received TPDU is a CR TPDU, then the value of the 16-bit checksum parameter shall be set to zero.

5.5.4.6.4 The Extended 32-bit Checksum shall be validated as follows:

1) Initialise 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.

5.6 INTERNETWORK SERVICE AND PROTOCOL SPECIFICATION

5.6.1 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.

5.6.1.1 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.

5.6.1.2 Applicability of Requirements

5.6.1.2.1 All ATN Intermediate System and End System Network entities shall comply with the provisions contained in 5.6.2 and 5.6.3, in addition to all APRLs specified in 5.6.4.

5.6.2 ATN Specific Features

5.6.2.1 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.

5.6.2.2 The Security Function

5.6.2.2.1 General

5.6.2.2.1.1 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.

5.6.2.2.1.2 ATN Network entities shall therefore provide the Globally Unique Security format for all created NPDUs.

5.6.2.2.1.3 The sole exception to this requirement is for General Communications traffic where no Security parameter information is required to be encoded in created NPDUs.

5.6.2.2.2 Encoding of the Security Parameter

5.6.2.2.2.1 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.

5.6.2.2.2.2 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 5.6-1, and defined below.

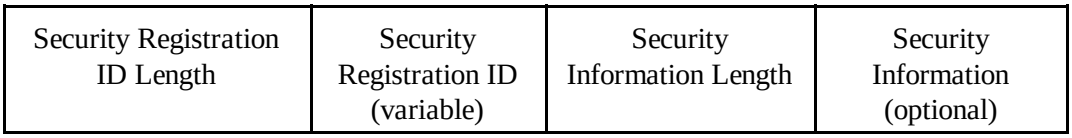


Figure 5.6-1: The ATN Security Label

5.6.2.2.3 Security Registration ID Length

5.6.2.2.3.1 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.

5.6.2.2.4 Security Registration ID

5.6.2.2.4.1 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 useing 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 organisation 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.

5.6.2.2.5 Security Information Length

5.6.2.2.5.1 This field shall be one octet in length and shall define the length in octets of the Security Information.

5.6.2.2.5.2 If there is no security information, this field shall be set to zero.

5.6.2.2.6 Security Information

5.6.2.2.6.1 General

5.6.2.2.6.1.1 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

5.6.2.2.6.1.2 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.

5.6.2.2.6.2 Encoding of the Security Information Field

5.6.2.2.6.2.1 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.

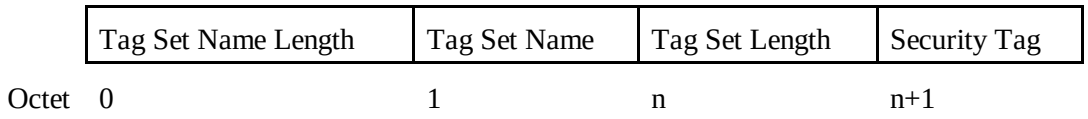


Figure 5.6-2: Security Tag Set Format

5.6.2.2.6.2.2 Each Security Tag Set shall consist of four fields, as illustrated in Figure 5.6-2, 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.

5.6.2.2.6.3 Security Tag Set Name Length

5.6.2.2.6.3.1 The Security Tag Set Name Length shall contain the length in octets of the Tag Set Name field.

5.6.2.2.6.4 Security Tag Set Name

5.6.2.2.6.4.1 The Security Tag Set Name shall be used to uniquely identify the Tag Set.

5.6.2.2.6.5 Tag Set Length

5.6.2.2.6.5.1 The Tag Set Length Field shall contain the length in octets of the Security Tag field.

5.6.2.2.6.6 Security Tag

5.6.2.2.6.6.1 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.

5.6.2.2.6.7 Encoding of the Tag Set for Traffic Type and Associated Routing Policies

5.6.2.2.6.7.1 The Tag Set Name shall be set to [0000 1111].

5.6.2.2.6.7.2 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.

5.6.2.2.6.7.3 The Security Tag shall indicate the Routing Policy Requirements for the data contained in the same NPDU, according to Table 5.6-1.

Note.— See 5.2.7 for detailed information on the ATN Security Policy.

Table 5.6-1 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.

Traffic Type	Category	Security Tag Value	Semantics
		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.

5.6.2.2.6.7.4 Those security tag values which are not defined in Table 5.6-1 shall be reserved for future use by this specification.

5.6.2.2.6.8 Encoding of the Tag Set for Security Classification

5.6.2.2.6.8.1 The Tag Set Name shall be set to [0000 0011].

5.6.2.2.6.8.2 When present in the security parameter, this Tag Set shall always follow the Tag Set for Traffic Type and Associated Routing Policies (see 5.6.2.2.6) 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.

5.6.2.2.6.8.3 The Security Tag shall indicate the security classification of the NPDU according to the following table:

Table 5.6-2 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

5.6.2.2.6.8.4 Those security classification tag values which are not assigned in Table 5.6-2 shall be reserved for future use by this specification.

5.6.2.3 Management of Network Priority

Note.— Network priority handling provisions are specified in 5.2.8.

5.6.2.4 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. 5.5.2.5 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.

5.6.2.4.1 Setting of the congestion experienced flag

5.6.2.4.1.1 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.

5.6.2.4.1.2 When a NPDU is being forwarded by an ATN Intermediate System, the Intermediate System shall examine the depth of the output queue selected for that NPDU.

5.6.2.4.1.3 If the depth of the selected output queue exceeds a threshold α (see Table 5.6-3), 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.

5.6.2.4.1.4 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.

5.6.2.4.2 Forwarding congestion information to the receiving NS-User

5.6.2.4.2.1 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.

5.6.2.4.2.2 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.

5.6.2.4.3 Required algorithm values

5.6.2.4.3.1 The value settings defined in the following table shall be implemented:

Table 5.6-3 Required Value for α

Name	Description	Required range
α	Output queue threshold	1 packet

5.6.3 ATN Specific Requirements for ISO/IEC 8473

Note.— This section defines ATN specific requirements on the ISO/IEC 8473 Protocol.

5.6.3.1 Segmentation Function

5.6.3.1.1 ATN Intermediate Systems (ISs) shall support both the segmenting and the non-segmenting subsets of ISO/IEC 8473.

5.6.3.1.2 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.

5.6.3.2 Security Function

Note.— The ATN Specific use of the ISO/IEC 8473 Security Function is specified in 5.6.2.2.

5.6.3.3 Echo Request Function

5.6.3.3.1 **Recommendation.** — *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.

5.6.3.4 Echo Response Function

5.6.3.4.1 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.

5.6.3.4.2 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.

5.6.3.4.3 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.

5.6.3.4.4 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.

5.6.3.4.5 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.

5.6.3.5 Network Priority

Note.— The ATN Specific use of the ISO/IEC 8473 Priority is specified in 5.2.8.4.

5.6.4 APRLs

5.6.4.1 General

5.6.4.1.1 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 these SARPs.

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 check list 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.

5.6.4.2 Support of ATN-Specific Network Layer features

Index	**Item**	**ATN SARPs Reference**	**ATN Support**
ATN CLNP1	Encoding and use of the Security Parameter	5.6.2.2	M
ATN CLNP2	Management of Network Priority	5.6.2.3, 5.2.8.4	M
ATN CLNP4	Echo Request Function	5.6.3.3	O
ATN CLNP5	Congestion Management	5.6.2.4	M
ATN CLNP6	Echo Response Function	5.6.3.4.1	M
ATN CLNP7	Echo Response parameter setting	5.6.3.4.2, 5.6.3.4.3, 5.6.3.4.4	M

5.6.4.3 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
IAS-s	<s> Inactive subset	8473-1: 5.2	IAS-r:M ^IAS-r:X	IAS-r:M ^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 SARPs Ref: 5.7	N/A	ISMOB:M ISGRD:O ^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 5.6.4.4 through 5.6.4.11. The supported functions, NPDUs, associated parameters and timers required for Intermediate Systems are provided in APRLs 5.6.4.12 through 5.6.4.18.

O.2: APRLs for the SNDCF for use with ISO/IEC 8802-2 subnetworks are provided in 5.7.7.2 and 5.7.7.3. APRLs for the SNDCF for use with ISO/IEC 8208 subnetworks are provided in 5.7.7.4 through 5.7.7.7.

5.6.4.4 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
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 SARPs Ref: 5.6.2.2	O	M
eSecu-r	<r> Security	6.13, ATN SARPs Ref. 5.6.2.2	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 SARPs Ref. 5.6.3.5	O	M

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN Support
ePri-r	<r> Priority	6.17, ATN SARPs Ref. 5.6.3.5	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 SARPs Ref. 5.6.3.3	O	O
eErsp	Echo response	6.20, ATN SARPs Ref. 5.6.3.4	O	M
eSegS	Create segments smaller than necessary	6.8	O	O

5.6.4.5 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

5.6.4.6 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

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
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
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	ePRR-s:M
edPRR-r	<r> Partial Route Recording	7.5.5	ePRR-r:M	ePRR-r: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

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
edUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

5.6.4.7 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
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	ePRR-s:M
eePRR-r	<r> Partial Route Recording	7.5.5	ePRR-r:M	ePRR-r: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

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
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

5.6.4.8 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

5.6.4.9 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	ePRR-s:M
eqPRR-r	<r> Partial Route Recording	7.5.5	ePRR-r:M	ePRR-r: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
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

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
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

5.6.4.10 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 SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	eSecu-s:M	eSecu-s:M
epSecu-r	<r> Security	7.5.3, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	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 SARPs Ref: 5.6.3.4.5	ePRR-s:M	ePRR-s:M
epPRR-r	<r> Partial Route Recording	7.5.5, ATN SARPs Ref: 5.6.3.4.5	ePRR-r:M	ePRR-r: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 SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	eQOSM-s or eCong-s:M	eQOSM-s:M
epQOSM-r	<r> QOS Maintenance	7.5.6, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	eQOSM-r or eCong-r :M	eQOSM-r or eCong-r:M
epPri-s	<s> Priority	7.5.7, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	ePri-s:M	ePri-s:M
epPri-r	<r> Priority	7.5.7, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	ePri-r:M	ePri-r:M
epData-s	<s> Data	7.6	M	M
epData-r	<r> Data	7.6	M	M

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
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

5.6.4.11 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

5.6.4.12 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

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN Support
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 SARPs Ref: 5.6.2.2	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 SARPs Ref: 5.6.3.5	O	M
iQOSM	<s> QOS Maintenance	6.16	O	M
iCong	<s> Congestion Notification	6.18, ATN SARPs Ref: 5.6.2.4	O	M
iPadd	<s> Padding	6.12	M	M
iEreq	Echo request	6.19, ATN SARPs Ref: 5.6.3.3	O	O
iErsp	Echo response	6.20, ATN SARPs Ref: 5.6.3.4	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

5.6.4.12.1 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 SARPs Ref. 5.6.2.2	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.

5.6.4.12.2 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
	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

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN Support
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.

5.6.4.13 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
iERQ-r	ERQ receive	7.10	M	M
iERP-t	ERP transmit	7.11	iErsp:M	iErsp:M

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN Support
iERP-r	ERP receive	7.11	M	M

5.6.4.14 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	iPRR: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

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
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
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

5.6.4.15 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

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
ieSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
ieCRR-s	<s> Complete Route Recording	7.5.5	iCRR:M	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	iPRR:M
ieCSR-s	<s> Complete Source Routing	7.5.4	iCSR:M	-
ieCSR-r	<r> Complete Source Routing	7.5.4	iCSR:M	-
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

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
ieUnsup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

5.6.4.16 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
iqSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
iqCRR-s	<s> Complete Route Recording	7.5.5	iCRR:M	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	iPRR:M
iqCSR-s	<s> Complete Source Routing	7.5.4	iCSR:M	-
iqCSR-r	<r> Complete Source Routing	7.5.4	iCSR:M	-

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
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

5.6.4.17 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
ipAddr-r	<r> Addresses	7.3	M	M
ipSeg-s	<s> Segmentation Part	7.4	M	M

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
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 SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	iSecu:M	iSecu:M
ipSecu-r	<r> Security	7.5.3, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	iSecu:M	iSecu:M
ipCRR-s	<s> Complete Route Recording	7.5.5	iCRR:M	M
ipCRR-r	<r> Complete Route Recording	7.5.5	iCRR:M	-
ipPRR-s	<s> Partial Route Recording	7.5.5, ATN SARPs Ref: 5.6.3.4.5	M	M
ipPRR-r	<r> Partial Route Recording	7.5.5, ATN SARPs Ref: 5.6.3.4.5	iPRR:M	iPRR: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 SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	M	M

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN Support
ipQOSM-r	<r> QOS Maintenance	7.5.6, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	iQOSM or iCong:M	iQOSM or iCong:M
ipPri-s	<s> Priority	7.5.7, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	M	M
ipPri-r	<r> Priority	7.5.7, ATN SARPs Ref: 5.6.3.4.3, 5.6.3.4.4	iPri:M	iPri:M
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

5.6.4.18 Intermediate Systems - Timer and Parameter Values

Item	Timer	ISO/IEC 8473-1 Reference	Status	ATN Support
iReasTim	Reassembly Timer	6.8	iReas:M	M

5.7 SPECIFICATION OF SUBNETWORK DEPENDENT CONVERGENCE FUNCTIONS

5.7.1 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 5.7-1 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.

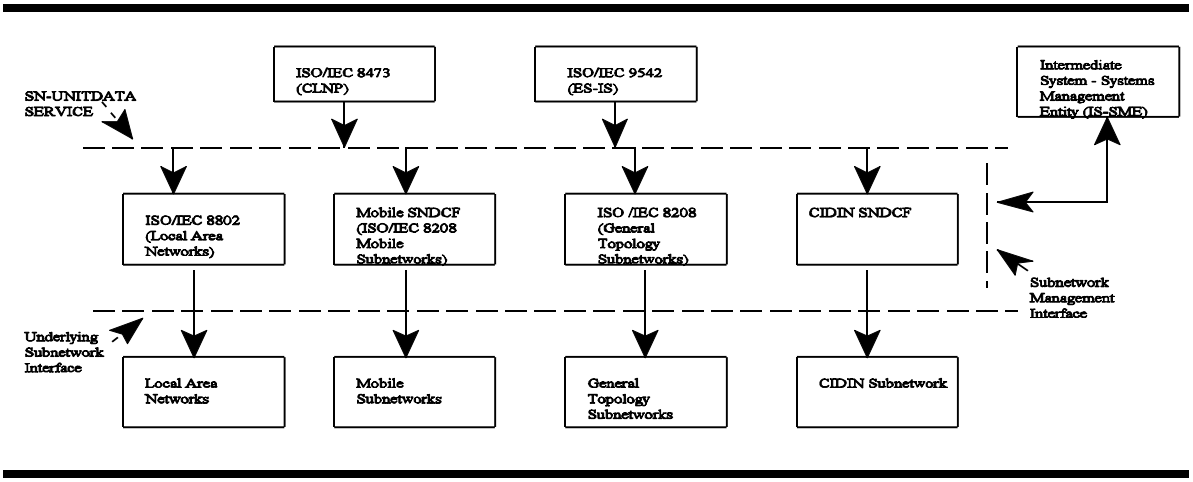


Figure 5.7-1 Relationship of SNDCFs to SN-Service and underlying Subnetworks

Note 5.— There is no requirement to implement this service as a software interface.

5.7.2 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 5.7-1.

Table 5.7-1 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

5.7.2.1 Subnetwork Service Primitive Parameters

Note.— The following sections specify the Subnetwork Service primitive parameters.

5.7.2.1.1 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.

5.7.2.1.2 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 5.2.8.5.

5.7.2.1.3 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.

5.7.2.1.4 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.

5.7.3 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.

5.7.3.1 The SNDCF for use with ISO/IEC 8802-2 Subnetworks shall be implemented according to ISO/IEC 8473-2.

5.7.3.2 APRLs

5.7.3.2.1 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 5.7.3.2.2 and 5.7.3.2.3.

5.7.3.2.2 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

5.7.3.2.3 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

5.7.4 SNDCF for the Common ICAO Data Interchange Network (CIDIN)

5.7.4.1 General Considerations

Note 1.— The ISO/IEC 8473 Protocol assumes a Connectionless underlying subnetwork service. CIDIN provides a Connectionless Mode Service which is already very close to what is required by this protocol in the ATN.

Note 2.— This SNDCF maps to level 4 of CIDIN as specified in Annex 10, Volume III.

5.7.4.1.1 The SNDCF for CIDIN shall be as specified in the following sections.

5.7.4.2 SN-UNITDATA Request and Indication Primitives

5.7.4.2.1 These primitives shall correspond to the request to send a CIDIN message at a CIDIN entry centre and the reception of a CIDIN message at a CIDIN exit centre respectively.

5.7.4.2.2 CIDIN messages shall be sent with the “no acknowledgement” option.

Note.— CIDIN messages requested to be transported to exit addresses which are not reachable are discarded in the entry centre.

5.7.4.3 SN Source Address

5.7.4.3.1 This address shall correspond to a CIDIN entry address in the Entry Address item.

5.7.4.4 SN Destination Address

5.7.4.4.1 This address shall correspond to a CIDIN exit address in an Exit Address item.

5.7.4.5 SN Quality of Service

5.7.4.5.1 A *priori* values for transit delay, protection against unauthorized access, cost determinants and residual error probability shall be entered as management data in the ATN system.

5.7.4.6 SN Priority

5.7.4.6.1 The mapping between SN Priority and the CIDIN Subnetwork Priority shall be entered as management data in the ATN system.

5.7.4.7 SNS-Userdata

5.7.4.7.1 SNS-Userdata shall be conveyed as the contents of the CIDIN message which is transported transparently by CIDIN.

Note.— The coding of the CIDIN message is code and byte independent.

5.7.5 SNDCF for ISO/IEC 8208 General Topology Subnetworks

5.7.5.1 Over ISO/IEC 8208 General Topology Subnetworks, the subnetwork service described in 5.7.2 shall be provided using either the SNDCF for ISO/IEC 8208 General Topology Subnetworks as specified in ISO/IEC 8473-3, or the Mobile SNDCF specified below in 5.7.6.

Note.— Although most ATN Ground Systems are generally expected to use the ISO/IEC 8473-3 specified SNDCF over ISO/IEC 8208 General Topology Subnetworks, Ground Systems may specify the use of the Mobile SNDCF, in order to improve the bandwidth utilisation over fixed ISO/IEC 8208 subnetworks.

5.7.5.2 **Recommendation.**— *Implementations using the Mobile SNDCF as specified in 5.7.6 and the LREF Compression Procedure for Ground/Ground communications, should also use the LREF optional local reference cancellation mechanism.*

5.7.5.3 APRLs

5.7.5.3.1 An implementation of the SNDCF for ISO/IEC 8208 General Topology Subnetworks shall be used in ATN End Systems and Routers if and only if its PICS is in compliance with the APRLs given in 5.7.5.3.2 through 5.7.5.3.5.

5.7.5.3.2 Subnetwork Dependent Convergence Functions SNDCF for use with ISO/IEC 8208 Subnetworks - Functions

Item	Function	ISO/IEC 8473-3 Reference	Status	ATN Support
XSNUD	Is Subnetwork User Data of at least 512 octets transferred transparently by the SNDCF ?	5.2	M	M
XSNTD	Is Transit Delay determined by the SNDCF prior to the processing of user data ?	5.2	M	M
	Call Setup Considerations Is a new call setup:	5.3.1		
XCalla	a. when no suitable call exists ?	5.3.1 a.	O.3	O.3
XCallb	b. when queue threshold reached ?	5.3.1 b.	O.3	O.3
XCallc	c. by systems management ?	5.3.1 c.	O.3	O.3
XCalld	d. when queue threshold reached and timer expires ?	5.3.4	O.3	O.3
XCalle	e. by other local means ?	5.3.1	O.3	O.3

Item	Function	ISO/IEC 8473-3 Reference	Status	ATN Support
	Call Clearing Considerations Are calls cleared:	5.3.2		
XClra	a. when idle timer expires ?	5.3.2 a., 5.3.4	O	O
XClrb	b. when need to re-use circuit ?	5.3.2 b.	O	O
XClrc	c. by systems management ?	5.3.2 c.	O	O
XClrd	d. by provider ?	5.3.2 d.	M	M
XClrer	e. by other local means ?	5.3.2	O	O
XPD	X.25 Protocol Discrimination	5.3.3	M	M
XVCC	Resolution of VC collisions	5.3.5	M	M
XMCR	Multiple VCs responding	5.3.6	M	M
XMCI	Multiple VCs initiating	5.3.6	O	O
Xpri	X.25 Priority procedure	5.3.7	O	M

5.7.5.3.3 Subnetwork Dependent Convergence Functions SNDCF for use with ISO/IEC 8208 Subnetworks - X.25 Call User Data

Item	Parameter	ISO/IEC 8473-3 Reference	Status	ATN Support
PD-s	<s> Protocol Discriminator	5.3.3	M	M
PD-r	<r> Protocol Discriminator	5.3.3	M	M
LI-s	<s> Length Indication	5.3.6	XMCI:M	XMCI:M
LI-r	<r> Length Indication	5.3.6	M	M
Ver-s	<s> SNCR Version	5.3.6	XMCI:M	XMCI:M
Ver-r	<r> SNCR Version	5.3.6	M	M
SNCR-s	<s> SNCR Value	5.3.6	XMCI:M	XMCI:M
SNCR-r	<r> SNCR Value	5.3.6	M	M

5.7.5.3.4 Subnetwork Dependent Convergence Functions SNDCF for use with ISO/IEC 8208 Subnetworks - ISO/IEC 8208 SNDCF Timers

Item	Timer	ISO/IEC 8473-3 Reference	Status	Values	ATN Support
XIDL	X25 VC Idle	5.3.4	XClra:O	Any	XClra:O
XNVC	additional VC	5.3.4	O	Any	M

5.7.5.3.5 Subnetwork Dependent Convergence Functions SNDCF for use with ISO/IEC 8208 Subnetworks - SNDCF Multi Layer Dependencies

Item	Dependency	ISO/IEC 8473-3 Reference	Status	Values Supported
XSSg-r	<r> Maximum SN data unit size (Rx)	5.2	>=512	>=512
XSSg-s	<s> Maximum SN data unit size (Tx)	5.2	>=512	>=512

Item	Dependency	ISO/IEC 8473-3 Reference	Status	ATN Support
Xvc	X.25 Virtual call service	5.3.8	M	M
Xdt	X.25 Data transfer	5.3.8	M	M
Xfc	X.25 flow control procedures	5.3.8	M	M
Xfrp	X.25 flow control + reset packets	5.3.8	M	M
Xccp	X.25 call setup and clear packets	5.3.8	M	M
Xdp	X.25 DTE and DCE data packets	5.3.8	M	M
Xrs	X.25 restart procedures	5.3.8	M	M
XDct	X.25 DCE timeouts	5.3.8	M	M
XDtT	X.25 time limits	5.3.8	M	M
Xpco	X.25 network packet coding	5.3.8	M	M
Xfcn	X.25 flow control parameter negotiation	5.3.8	O	O
Xtd	X.25 transit delay selection and negotiation	5.3.8	O	O
Xtc	X.25 throughput class negotiation	5.3.8	O	O
Xoth	Other X.25 elements	5.3.8	O	O

5.7.6 SNDCF for ISO/IEC 8208 Mobile Subnetworks

5.7.6.1 General

5.7.6.1.1 Over ISO/IEC 8208 Mobile Subnetworks, the subnetwork service described in 5.7.2 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 5.7.6.3;*
- *Data Stream Mode Compression as specified in 5.7.6.5.*

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 5.7.6.3.1) 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).

5.7.6.1.2 All ATN Intermediate Systems using Mobile ISO/IEC 8208 subnetworks for communication with other Intermediate Systems shall implement the LREF compression procedure.

5.7.6.1.3 **Recommendation**.— *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.*

5.7.6.2 Call Setup

5.7.6.2.1 Calling DTE Procedures

5.7.6.2.1.1 General

5.7.6.2.1.1.1 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.

5.7.6.2.1.1.2 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 to to 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.

5.7.6.2.1.1.3 The Call Request user data shall be formatted as specified in 5.7.6.2.1.5.

5.7.6.2.1.2 The Priority Facility

5.7.6.2.1.2.1 The mapping of ATN network layer priorities to ATN mobile subnetwork priorities shall be as defined in 1.3.8 for those mobile subnetworks subject to ICAO standards.

5.7.6.2.1.2.2 For mobile subnetworks not subject to ICAO standards, the Priority Facility shall be used if the subnetwork provider supports prioritisation of Virtual Circuits and specifies the mapping of Network Service to Subnetwork Service priorities.

5.7.6.2.1.2.3 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.

5.7.6.2.1.2.4 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 prioritisation 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.

5.7.6.2.1.3 Non-Standard Default Packet Size Facility and Flow Control Parameter Negotiation Facility

5.7.6.2.1.3.1 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.

5.7.6.2.1.4 The Fast Select Facility

5.7.6.2.1.4.1 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.

5.7.6.2.1.4.2 No restriction on response shall be indicated.

Note 1.— This permits the responding DTE 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.

5.7.6.2.1.5 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.

5.7.6.2.1.5.1 The Call Request User Data format shall be as illustrated in Figure 5.7-2.

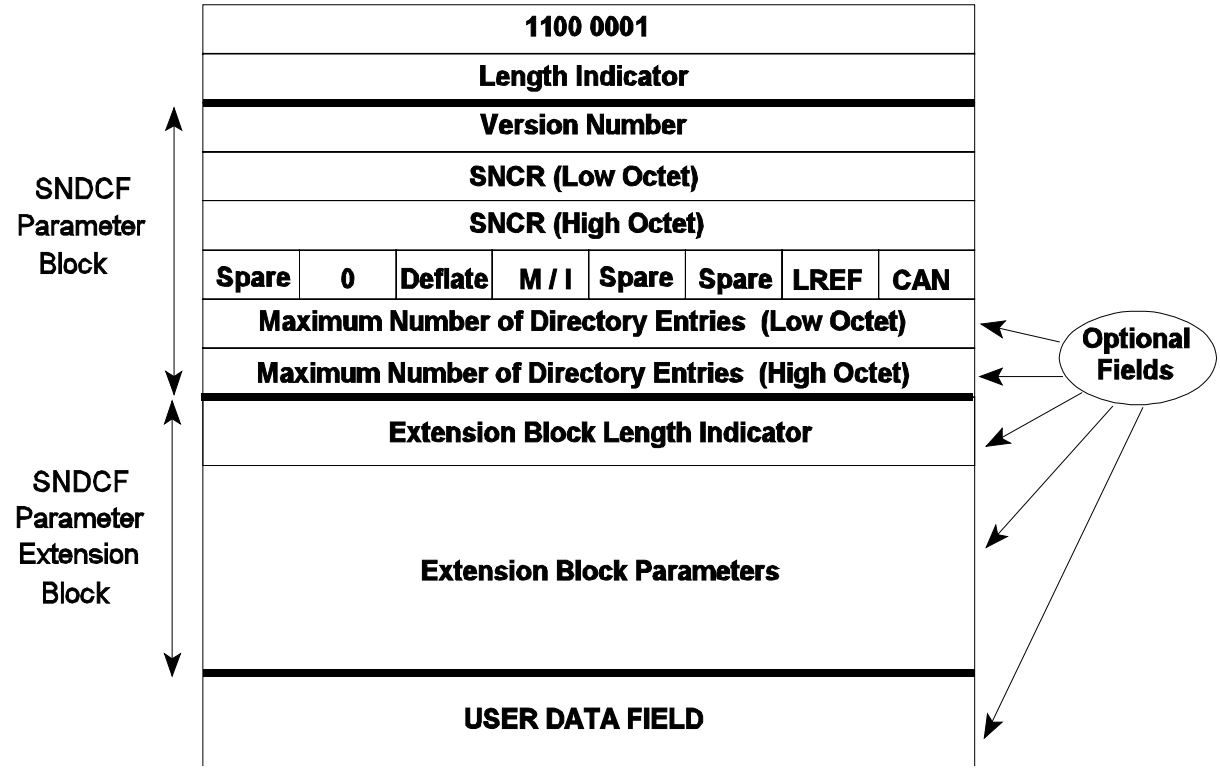


Figure 5.7-2 Format for Call Request User Data

5.7.6.2.1.5.2 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.

5.7.6.2.1.5.3 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).

5.7.6.2.1.5.4 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 parameters 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.

5.7.6.2.1.5.4.1 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 5.7.6.2.1.5.5), 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 3rd edition of this specification.

5.7.6.2.1.5.4.1.1 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 formated 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".

5.7.6.2.1.5.4.1.2 ***Recommendation.—*** *The version number of the SNDCF protocol used by the calling DTE when initiating a Call Request should be configurable.*

5.7.6.2.1.5.4.2 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).

5.7.6.2.1.5.4.3 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.

5.7.6.2.1.5.4.4 The fourth octet of the SNDCF Parameter Block shall indicate the compression techniques offered by the calling DTE, according to Table 5.7-2 and Figure 5.7-2.

5.7.6.2.1.5.4.5 Those bits of Table 5.7-2 and Figure 5.7-2 which are marked as 'Spare' are reserved for future use by this specification and shall always be set to zero.

Table 5.7-2 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 5.7-4).*
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

5.7.6.2.1.5.4.6 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.

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.

5.7.6.2.1.5.4.7 Bit 1 of the fourth octet of the SNDCF Parameter Block shall only be set if bit 2 is also set.

5.7.6.2.1.5.4.8 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.

5.7.6.2.1.5.4.9 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.

5.7.6.2.1.5.4.10 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.

5.7.6.2.1.5.4.11 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).

5.7.6.2.1.5.4.12 Bit 2 of the fourth octet of the SNDCF Parameter Block shall be set to zero.

5.7.6.2.1.5.5 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.

5.7.6.2.1.5.5.1 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.

5.7.6.2.1.5.5.2 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.

5.7.6.2.1.5.5.3 Each parameter contained within the SNDCF Parameter Extension Block shall be structured as illustrated in Figure 5.7-3.

Octets	**Semantics**
1	Parameter Code
2	Parameter Length Indication
3 ... m	Parameter Value

Figure 5.7-3 Format of Parameters in the SNDCF Parameter Extension Block

5.7.6.2.1.5.5.4 The Parameter Code field shall be coded in binary.

5.7.6.2.1.5.5.5 There shall be no more than one parameter with the same Parameter Code in the SNDCF Parameter Extension Block.

5.7.6.2.1.5.5.6 The Parameter Length Indication field shall indicate the number of octets of the Parameter Value field.

5.7.6.2.1.5.5.7 Dictionaries List Parameter

5.7.6.2.1.5.5.7.1 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.

5.7.6.2.1.5.5.7.2 The Dictionaries List Parameter shall be encoded as defined in 5.7.6.2.1.5.9.

5.7.6.2.1.5.5.8 Deflate Maintenance Parameter

5.7.6.2.1.5.5.8.1 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.

5.7.6.2.1.5.5.8.2 The Deflate Maintenance Parameter shall be encoded as defined in 5.7.6.2.1.5.10.

5.7.6.2.1.5.6 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.

5.7.6.2.1.5.7 Otherwise, the octet following the SNDCF Parameter Block shall be the first octet of the User Data field, if present.

5.7.6.2.1.5.8 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.

5.7.6.2.1.5.9 Encoding of the Dictionaries List Parameter

5.7.6.2.1.5.9.1 The Dictionaries List Parameter shall be structured as illustrated in Figure 5.7-3.

5.7.6.2.1.5.9.2 The Parameter Code field of the Dictionaries List Parameter shall be set to [0000 0001].

5.7.6.2.1.5.9.3 The Parameter Value field of the Dictionaries List Parameter shall consist of one or more Dictionary Tags, as defined in 5.7.6.2.1.5.9.7, identifying the latest supported version of the Data Stream Compression Dictionaries supported by the calling DTE.

5.7.6.2.1.5.9.4 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.

5.7.6.2.1.5.9.5 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.

5.7.6.2.1.5.9.6 Within the Dictionaries List Parameter Value field, there shall be no duplication of a Dictionary Tag.

5.7.6.2.1.5.9.7 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.

5.7.6.2.1.5.9.7.1 A Dictionary Tag shall be two octets in length.

5.7.6.2.1.5.9.7.2 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 5.7-3.

Table 5.7-3 Encoding of the First Octet of a Dictionary Tag

Bit 8	Bit 7	Registration Authority
0	0	ICAO
0	1	IATA
1	0	Reserved

Bit 8	Bit 7	Registration Authority
1	1	Reserved

5.7.6.2.1.5.9.7.3 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.

5.7.6.2.1.5.9.7.4 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.

5.7.6.2.1.5.10 Encoding of the Deflate Maintenance Parameter

5.7.6.2.1.5.10.1 The Deflate Maintenance Parameter shall be structured as illustrated in Figure 5.7-3.

5.7.6.2.1.5.10.2 The Parameter Code of the Deflate Maintenance Parameter shall be set to [0000 0010].

5.7.6.2.1.5.10.3 The Parameter Length field of the Deflate Maintenance Parameter shall be set to 4.

5.7.6.2.1.5.10.4 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.

5.7.6.2.1.5.10.5 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 5.7.6.5.9.3.

5.7.6.2.1.5.11 Procedure Associated with the Use of the Deflate Maintenance Parameter

5.7.6.2.1.5.11.1 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.

5.7.6.2.1.6 Receipt of “Call Confirm Packet”

5.7.6.2.1.6.1 Fast Select Facility In Use

5.7.6.2.1.6.1.1 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 5.7.6.2.2.4.3) 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.

5.7.6.2.1.6.1.2 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.

5.7.6.2.1.6.1.3 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.

5.7.6.2.1.6.1.4 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.

5.7.6.2.1.6.1.5 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).

5.7.6.2.1.6.1.6 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.

5.7.6.2.1.6.1.7 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 5.7.6.2.1.6.1.11.

5.7.6.2.1.6.1.8 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 5.7-4) 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.

5.7.6.2.1.6.1.9 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.

5.7.6.2.1.6.1.10 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.

5.7.6.2.1.6.1.11 Processing of SNDCF Parameter Extension Block

5.7.6.2.1.6.1.11.1 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.

5.7.6.2.1.6.1.11.2 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).

5.7.6.2.1.6.1.11.3 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.

5.7.6.2.1.6.1.11.4 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.

5.7.6.2.1.6.1.11.5 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.

5.7.6.2.1.6.1.11.6 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.

5.7.6.2.1.6.1.11.7 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 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 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.

5.7.6.2.1.6.1.11.8 If a Dictionary Selection Parameter is present in the SNDCF Parameter Extension Block, the following cases are error conditions:

a) The preceeding 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).

5.7.6.2.1.6.1.11.9 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.

5.7.6.2.1.6.2 Fast Select Facility not in Use

5.7.6.2.1.6.2.1 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.

5.7.6.2.1.7 Call Rejection by the DCE or Called DTE

5.7.6.2.1.7.1 General

5.7.6.2.1.7.1.1 **Recommendation.—** *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 5.7-4), then the call should be re-attempted with the minimum directory size (see 5.7.6.3.1.3).*

Note.— This is to ensure that the call is not rejected again due to the requested directory size being too big.

5.7.6.2.1.7.1.2 If the diagnostic indicates Call Collision resolution then no further attempt shall be made to re-establish the call.

5.7.6.2.1.7.1.3 When a DTE originated ISO/IEC 8208 Call Clearing packet is received with a diagnostic value indicating "Version number not supported" (see Table 5.7-4), then the call shall be re-attempted with a version number in the SNDCF Parameter Block of the Call Request User Data (see 5.7.6.2.1.5.4.1) 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.

5.7.6.2.1.7.2 Fast Select Facility Requested

5.7.6.2.1.7.2.1 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.

5.7.6.2.1.7.3 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.

5.7.6.2.1.7.3.1 When a DTE originated ISO/IEC 8208 Call Clearing Packet is received with a diagnostic indicating *LREF Compression not Supported* (see Table 5.7-4), the call shall be re-attempted without offering LREF Compression.

5.7.6.2.1.7.3.2 When a DTE originated ISO/IEC 8208 Call Clearing Packet is received with a diagnostic indicating *Local Reference Cancellation not Supported* (see Table 5.7-4), the call shall be re-attempted without offering Local Reference Cancellation.

5.7.6.2.1.7.3.3 When a DTE originated ISO/IEC 8208 Call Clearing Packet is received with a diagnostic indicating *Deflate compression not Supported* (see Table 5.7-4), the call shall be re-attempted without offering Deflate compression.

5.7.6.2.2 Called DTE Procedures

5.7.6.2.2.1 Incoming Call Processing

5.7.6.2.2.1.1 When an ISO/IEC 8208 Incoming Call Packet is received, the called SNDCF first shall check for a call collision.

5.7.6.2.2.1.2 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.

5.7.6.2.2.1.3 The called SNDCF shall then determine whether to accept the call.

5.7.6.2.2.1.4 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.

5.7.6.2.2.1.5 The call shall then be rejected using a Call Clearing Packet, with the appropriate diagnostic code, as listed in Table 5.7-4.

5.7.6.2.2.1.6 If the call is to be accepted then the Called SNDCF shall perform the ISO/IEC 8208 procedures associated with accepting a call.

5.7.6.2.2.2 Call Acceptance with the Fast Select Facility in Use

5.7.6.2.2.2.1 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 5.7-4.

5.7.6.2.2.2.2 Paragraph has been deleted.

5.7.6.2.2.2.3 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.

5.7.6.2.2.2.4 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 5.7.6.2.2.2.10), 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.

5.7.6.2.2.2.5 If there is additional user data beyond the SNDCF Parameter Block or the SNDCF Parameter Extension Block respectively (see Figure 5-7.2) 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.

5.7.6.2.2.2.6 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.

5.7.6.2.2.2.7 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.

5.7.6.2.2.2.8 If an SNDCF Parameter Extension Block (see Figure 5-7.2) is present in the received Incoming Call Packet, then it shall be processed by the called SNDCF as specified in 5.7.6.2.2.2.9.

5.7.6.2.2.2.9 Processing of Received SNDCF Parameter Extension Block

5.7.6.2.2.2.9.1 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.

5.7.6.2.2.2.9.2 ***Recommendation***.*— The order of preference of compression options should be configurable.*

5.7.6.2.2.2.9.3 Processing of Received Deflate Maintenance Parameter

5.7.6.2.2.2.9.3.1 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.

5.7.6.2.2.2.9.3.2 If a Deflate Maintenance Parameter is present in the SNDCF Parameter Extension Block and none of the above conditions are true, then the newly established Virtual Circuit shall be inserted into the Subnetwork Connection Group.

5.7.6.2.2.2.9.3.3 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.

5.7.6.2.2.2.9.3.4 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.

5.7.6.2.2.2.9.3.5 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.

5.7.6.2.2.2.9.3.6 The Called DTE shall then insert a Deflate Maintenance Parameter in the SNDCF Parameter Extension Block of the Call Accept User Data.

5.7.6.2.2.2.9.3.7 The Deflate Maintenance Parameter shall be encoded as defined in 5.7.6.2.1.5.10.

5.7.6.2.2.2.9.3.8 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 5.7.6.5.9.3.

5.7.6.2.2.2.9.3.9 No more than one Deflate Maintenance Parameter shall be inserted in the SNDCF Parameter Extension Block of the Call Accept User Data.

5.7.6.2.2.2.9.4 Processing of a Dictionaries List Parameter

5.7.6.2.2.2.9.4.1 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, neither at the proposed version nor any earlier version, are supported.

5.7.6.2.2.2.9.4.2 If a Dictionaries List Parameter is present in the SNDCF Parameter Extension Block and none of the above conditions are 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.

5.7.6.2.2.2.9.4.3 The Called DTE shall then insert a Dictionary Selection Parameter in the SNDCF Parameter Extension Block of the Call Accept User Data.

5.7.6.2.2.2.9.4.4 The Dictionary Selection Parameter shall be encoded as defined in 5.7.6.2.2.4.7.

5.7.6.2.2.2.9.4.5 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.

5.7.6.2.2.3 Call Acceptance without the Fast Select Facility in Use

5.7.6.2.2.3.1 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 5.7.6.2.2.1.4.

5.7.6.2.2.4 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.

5.7.6.2.2.4.1 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.

5.7.6.2.2.4.2 The Call Accept User Data format shall be as illustrated in Figure 5.7-4.

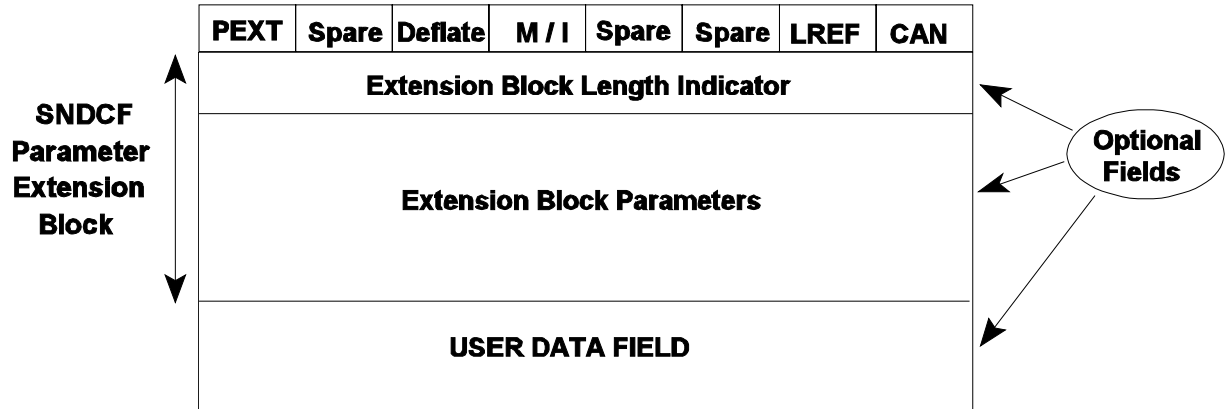


Figure 5.7-4 Format for Call Accept User Data

5.7.6.2.2.4.3 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 5.7-2).

5.7.6.2.2.4.4 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 5.7-4) 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.

5.7.6.2.2.4.5 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.

5.7.6.2.2.4.5.1 If present, the SNDCF Parameter Extension Block shall start at the second octet of the Call Accept User Data.

5.7.6.2.2.4.5.2 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.

5.7.6.2.2.4.5.3 Each parameter contained within the SNDCF Parameter Extension Block shall be structured as illustrated in Figure 5.7-3 and as specified in 5.7.6.2.1.5.5.4 through 5.7.6.2.1.5.5.6.

5.7.6.2.2.4.6 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 5.7.6.2.3.1), the optional NPDU in the Call Accept User Data, if present, is sent uncompressed.

5.7.6.2.2.4.7 Encoding of the Dictionary Selection Parameter

5.7.6.2.2.4.7.1 The Dictionary Selection Parameter shall be structured as illustrated in Figure 5.7-3.

5.7.6.2.2.4.7.2 The Parameter Code of the Dictionary Selection Parameter shall be set to [0000 0011].

5.7.6.2.2.4.7.3 The Parameter Length field of the Dictionary Selection Parameter shall be set to 2.

5.7.6.2.2.4.7.4 The Parameter Value field of the Dictionaries Selection Parameter shall consist of one and only one Dictionary Tag as defined in 5.7.6.2.1.5.9.7, identifying the Data Stream Compression Dictionary selected by the called DTE.

5.7.6.2.3 Data Transfer Phase

5.7.6.2.3.1 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.

5.7.6.2.3.2 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.

5.7.6.2.3.3 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.

5.7.6.2.4 Call Clearing

5.7.6.2.4.1 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.

5.7.6.2.4.2 Items b) or c) above shall only apply to those virtual circuits that have been established following an SN-UNITDATA.request.

5.7.6.2.4.3 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.

5.7.6.2.4.4 All packets subsequently received other than a Clear Confirm or a Clear Indication shall be ignored.

5.7.6.2.4.5 The same actions shall apply to the receipt of a Clear Indication.

5.7.6.2.4.6 The Clearing Cause octet in the ISO/IEC-8208 Cause/Diagnostic field shall be set to [1000 0000].

5.7.6.2.4.7 The reason for clearing the call shall be placed in the Diagnostic field using the appropriate diagnostic values according to Table 5.7-4.

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.

5.7.6.3 Local Reference Compression Procedures

5.7.6.3.1 Local Directory Initialization

5.7.6.3.1.1 Both calling and called SNDCFs shall create a local directory to be associated with each newly established Subnetwork Connection Group.

5.7.6.3.1.2 This directory shall consist of entries numbered from zero to a maximum of 32767, 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.

5.7.6.3.1.3 The directory shall be initially empty. The Mobile SNDCF shall support a minimum directory size of 128 entries.

Table 5.7-4 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

	Binary value	Decimal value	Diagnostic Code
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

5.7.6.3.2 Action following an SN-UNITDATA Request

5.7.6.3.2.1 General

5.7.6.3.2.1.1 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.

5.7.6.3.2.1.2 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.

5.7.6.3.2.1.3 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.

5.7.6.3.2.1.4 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.

5.7.6.3.2.1.5 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.

5.7.6.3.2.2 Identification of Network Layer Protocol

5.7.6.3.2.2.1 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.

5.7.6.3.2.2.2 If the IPI contains binary [1000 0001] indicating ISO/IEC 8473, then the procedures in 5.7.6.3.2.3 shall be performed.

5.7.6.3.2.2.3 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.

5.7.6.3.2.2.4 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.

5.7.6.3.2.3 Identification of Option Parameter and Local Directory Look-up

5.7.6.3.2.3.1 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.

5.7.6.3.2.3.2 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.

5.7.6.3.2.3.3 If an entry is found, then the NPDU shall be sent in the compressed form constructed according to 5.7.6.3.3, using the local directory entry number as the local reference.

5.7.6.3.2.3.4 If no entry is found, then a new directory entry shall be created and the SN-Userdata shall be modified as specified in 5.7.6.3.2.4.

5.7.6.3.2.4 Establishing a New Local Reference

5.7.6.3.2.4.1 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.

5.7.6.3.2.4.2 The value of the protocol version number, and the security parameter, if present, shall also be placed in this entry.

5.7.6.3.2.4.3 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..16447] if the SNDCF is the initiator of the first virtual circuit in a Subnetwork Connection Group, or [64..127] or [16448..32767], if the SNDCF is the responder for such a virtual circuit.

5.7.6.3.2.4.4 When a directory size greater than 128 but less than 32767 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

16447 + (n -128) / 2

where 'n' is the agreed maximum directory size.

5.7.6.3.2.4.5 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.

5.7.6.3.2.4.6 **Recommendation.**— *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.*

5.7.6.3.2.4.7 The PDU, which may be either a DT PDU or an ER PDU, shall have an additional options field added to the PDU header.

5.7.6.3.2.4.8 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.

5.7.6.3.2.4.9 This Local Reference option parameter shall be included as the first parameter in the Option Part of the DT or ER PDU header.

5.7.6.3.2.4.10 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.

5.7.6.3.2.4.11 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.

5.7.6.3.2.4.12 The Total Length, if present, shall be left unmodified.

5.7.6.3.2.5 Reference Cancellation Option

5.7.6.3.2.5.1 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.

5.7.6.3.2.5.2 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 5.7.6.3.6 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.

5.7.6.3.2.6 Transfer of the Modified ISO/IEC 8473 PDU

5.7.6.3.2.6.1 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.

5.7.6.3.3 Compression of SN-Userdata

5.7.6.3.3.1 General

5.7.6.3.3.1.1 An Initial DT NPDU shall be compressed according to the procedures specified in 5.7.6.3.3.2.

5.7.6.3.3.1.2 A Derived DT NPDU shall be compressed according to the procedures specified in 5.7.6.3.3.3.

5.7.6.3.3.1.3 An ER NPDU shall be compressed according to the procedures specified in 5.7.6.3.3.4.

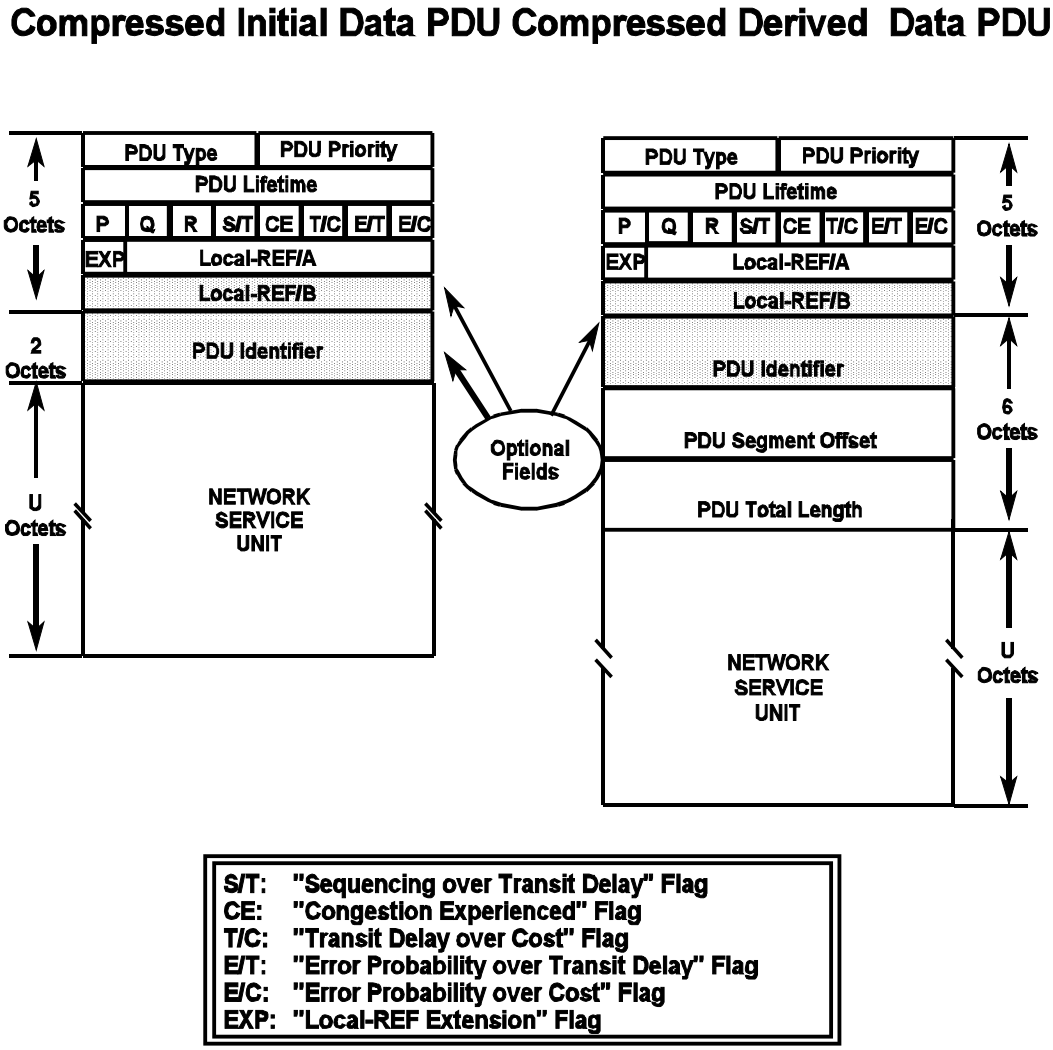


Figure 5.7-5 Compressed Initial and Derived Formats

5.7.6.3.3.2 Initial DT PDU Compression

5.7.6.3.3.2.1 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.

5.7.6.3.3.2.1.1 The original Initial DT PDU shall be compressed into the Compressed Initial Data PDU as shown in Figure 5.7-5.

5.7.6.3.3.2.1.2 The fields of the Compressed Initial Data PDU shall be set as follows.

5.7.6.3.3.2.2 Type Field

5.7.6.3.3.2.2.1 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 5.7-5.

Table 5.7-5 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

5.7.6.3.3.2.3 PDU Priority Field

5.7.6.3.3.2.3.1 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.

5.7.6.3.3.2.4 PDU Lifetime Field

5.7.6.3.3.2.4.1 The PDU Lifetime field value shall be set to the eight bits of the original NPDU lifetime field.

5.7.6.3.3.2.5 P bit Field

5.7.6.3.3.2.5.1 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.

5.7.6.3.3.2.6 Q bit Field

5.7.6.3.3.2.6.1 The Q field value shall be set to one if the original uncompressed PDU contained the QoS Maintenance option.

5.7.6.3.3.2.6.2 This field shall be set to zero otherwise.

5.7.6.3.3.2.7 R bit Field

5.7.6.3.3.2.7.1 The R field value shall be set to one if the original uncompressed PDU contains a non-zero checksum.

5.7.6.3.3.2.7.2 This field shall be set to zero otherwise.

5.7.6.3.3.2.8 S/T, CE , T/C, E/T, and E/C Fields

5.7.6.3.3.2.8.1 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.

5.7.6.3.3.2.8.2 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.

5.7.6.3.3.2.8.3 The CE field shall be set to the value of bit 4 in the Quality of Service Maintenance parameter value field.

5.7.6.3.3.2.8.4 The T/C field shall be set to the value of bit 3 in the Quality of Service Maintenance parameter value field.

5.7.6.3.3.2.8.5 The E/T field shall be set to the value of bit 2 in the Quality of Service Maintenance parameter value field.

5.7.6.3.3.2.8.6 The E/C field shall be set to the value of bit 1 in the Quality of Service Maintenance parameter value field.

5.7.6.3.3.2.9 EXP, Local-REF/A and Local-REF/B Fields

5.7.6.3.3.2.9.1 If the value of the Local Reference determined according to the procedure specified in 5.7.6.3.2.4 is less than 128, then the EXP field shall be set to zero.

5.7.6.3.3.2.9.2 In this case, only the Local-REF/A field shall be present in the PDU.

5.7.6.3.3.2.9.3 The Local-REF/A field value shall be set to the value of the Local Reference encoded as an unsigned integer.

5.7.6.3.3.2.9.4 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.

5.7.6.3.3.2.9.5 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.

5.7.6.3.3.2.10 PDU Identifier

5.7.6.3.3.2.10.1 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.

5.7.6.3.3.2.10.2 The PDU Identifier field shall contain the Data Unit Identifier as provided in the segmentation part of the Initial DT PDU.

5.7.6.3.3.2.10.3 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.

5.7.6.3.3.2.11 PDU Segment Offset

5.7.6.3.3.2.11.1 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.

5.7.6.3.3.2.12 PDU Total Length

5.7.6.3.3.2.12.1 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.

5.7.6.3.3.2.13 Network Service Data Unit Field

5.7.6.3.3.2.13.1 This field shall contain the Data Part of the original Initial DT PDU.

5.7.6.3.3.3 Derived DT PDU Compression

5.7.6.3.3.3.1 General

5.7.6.3.3.3.1.1 The original Derived DT PDU shall be compressed into the Compressed Derived Data PDU as shown in Figure 5.7-5.

5.7.6.3.3.3.1.2 The fields of the Compressed Derived Data PDU shall be set as defined in the following sections.

5.7.6.3.3.3.2 Type Field

5.7.6.3.3.3.2.1 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 5.7-6.

Table 5.7-6 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

PDU Type Values	CLNP NPDU ER Value	CLNP NPDU SP Value	CLNP NPDU MS Value
1 0 1 0	1	1	1

5.7.6.3.3.3.3 PDU Priority Field

5.7.6.3.3.3.3.1 This field shall be set as defined in 5.7.6.3.3.2.3.

5.7.6.3.3.3.4 PDU Lifetime Field

5.7.6.3.3.3.4.1 This field shall be set as defined in 5.7.6.3.3.2.4.

5.7.6.3.3.3.5 P bit Field

5.7.6.3.3.3.5.1 This field shall be set as defined in 5.7.6.3.3.2.5.

5.7.6.3.3.3.6 Q bit Field

5.7.6.3.3.3.6.1 This field shall be set as defined in 5.7.6.3.3.2.6.

5.7.6.3.3.3.7 S/T, CE , T/C, E/T, and E/C Fields

5.7.6.3.3.3.7.1 These fields shall be set as defined in 5.7.6.3.3.2.8.

5.7.6.3.3.3.8 EXP, Local-REF/A and Local-REF/B Fields

5.7.6.3.3.3.8.1 These fields shall be set as defined in 5.7.6.3.3.2.9.

5.7.6.3.3.3.9 PDU Identifier Field

5.7.6.3.3.3.9.1 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.

5.7.6.3.3.3.10 PDU Segment Offset Field

5.7.6.3.3.3.10.1 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.

5.7.6.3.3.3.11 PDU Total Length Field

5.7.6.3.3.3.11.1 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.

5.7.6.3.3.4 Error Report PDU Compression

5.7.6.3.3.4.1 General

5.7.6.3.3.4.1.1 The original ER PDU shall be compressed into the Compressed Error Report PDU as shown in Figure 5.7-6.

5.7.6.3.3.4.1.2 The fields of the Compressed Error Report PDU shall be set as defined in the following sections.

5.7.6.3.3.4.2 PDU Type Field

5.7.6.3.3.4.2.1 The PDU Type field value shall be set to [1101].

5.7.6.3.3.4.3 PDU Priority Field

5.7.6.3.3.4.3.1 This field shall be set as defined in 5.7.6.3.3.2.3.

5.7.6.3.3.4.4 PDU Lifetime Field

5.7.6.3.3.4.4.1 This field shall be set as defined in 5.7.6.3.3.2.4.

5.7.6.3.3.4.5 P bit Field

5.7.6.3.3.4.5.1 This field shall be as defined in 5.7.6.3.3.2.5.

5.7.6.3.3.4.6 Q bit Field

5.7.6.3.3.4.6.1 This field shall be set as defined in 5.7.6.3.3.2.6.

5.7.6.3.3.4.7 S/T, CE , T/C, E/T and E/C Fields

5.7.6.3.3.4.7.1 These fields shall be set as defined in 5.7.6.3.3.2.8.

5.7.6.3.3.4.8 EXP, Local-REF/A, Local-REF/B Fields

5.7.6.3.3.4.8.1 These fields shall be set as defined in 5.7.6.3.3.2.9.

5.7.6.3.3.4.9 Discard Reason Field

5.7.6.3.3.4.9.1 This field shall be set to the value of the Reason for Discard Parameter Value field contained in the original NPDU header.

5.7.6.3.3.4.10 Header of Discarded NPDU Field

5.7.6.3.3.4.10.1 This field shall contain the value of the Error Report Data Part if provided in the original Error Report PDU.

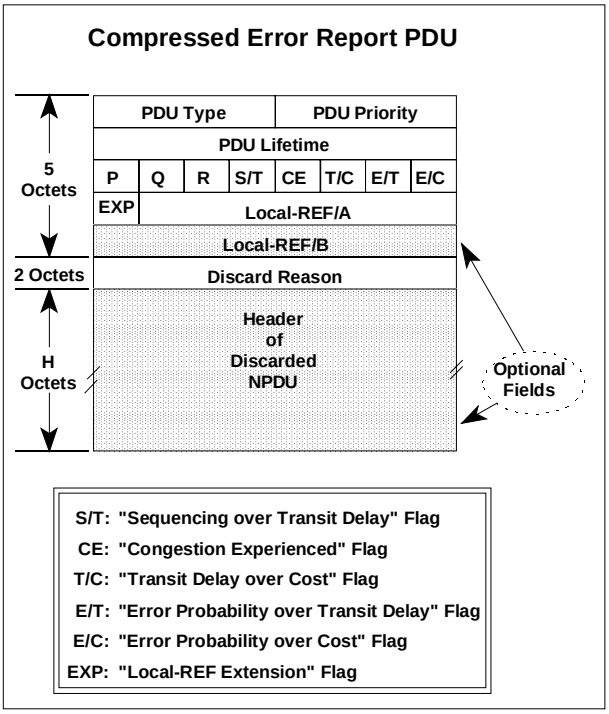


Figure 5.7-65 Compressed Error Report PDU |

5.7.6.3.3.4.11 Transfer of Compressed ISO/IEC 8473 PDUs

5.7.6.3.3.4.11.1 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.

5.7.6.3.4 Processing of Packets Received from the Subnetwork Service Provider

Note.— The following sections specify the processing of packets received from the Subnetwork Service provider.

5.7.6.3.4.1 Initial Processing of NPDU

5.7.6.3.4.1.1 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 5.7-7).

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 5.7.6.3.4.2.2.

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 5.7.6.3.4.3.

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 5.7.6.3.4.3.

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 5.7.6.3.4.4.

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 5.7.6.3.4.5, 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 5.7.6.3.6 and no SN-UNITDATA.indication generated.

Table 5.7-7 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

5.7.6.3.4.1.2 In all other cases, the PDU shall be discarded and an SNDCF Error Report Generated (see 5.7.6.3.5).

5.7.6.3.4.2 Incoming ISO/IEC 8473 PDU with Uncompressed Header

5.7.6.3.4.2.1 General

5.7.6.3.4.2.1.1 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.

5.7.6.3.4.2.2 Processing of Unmodified ISO/IEC 8473 PDUs

5.7.6.3.4.2.2.1 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.

5.7.6.3.4.2.3 Processing of Modified ISO/IEC 8473 PDUs

5.7.6.3.4.2.3.1 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.

5.7.6.3.4.2.3.2 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.

5.7.6.3.4.2.3.3 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.

5.7.6.3.4.2.3.4 An SNDCF Error Report (see 5.7.6.3.5) 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.

5.7.6.3.4.2.3.5 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.

5.7.6.3.4.2.3.6 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.

5.7.6.3.4.3 Incoming Compressed Data PDU

5.7.6.3.4.3.1 General

5.7.6.3.4.3.1.1 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.

5.7.6.3.4.3.1.2 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.

5.7.6.3.4.3.1.3 Upon receipt, the SNDCF shall examine and validate the Local-REF in the compressed PDU.

5.7.6.3.4.3.1.4 The value of the Local Reference shall be extracted from the compressed header and the corresponding entry in the local directory located.

5.7.6.3.4.3.1.5 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.

5.7.6.3.4.3.1.6 If the Local-REF is valid, the original uncompressed NPDU shall be recreated by the procedures defined in 5.7.6.3.4.3.2 through 5.7.6.3.4.3.6.

5.7.6.3.4.3.1.7 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.

5.7.6.3.4.3.2 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.

5.7.6.3.4.3.2.1 Network Layer Protocol Identifier

5.7.6.3.4.3.2.1.1 This field shall be set to binary [1000 0001] to identify this Network Layer Protocol as ISO/IEC 8473.

5.7.6.3.4.3.2.2 Length Indicator

5.7.6.3.4.3.2.2.1 This field shall be set to the length of the uncompressed NPDU header in octets.

5.7.6.3.4.3.2.3 Version/Protocol Identifier Extension

5.7.6.3.4.3.2.3.1 The Version/Protocol Identifier Extension field shall be set to the values provided in the corresponding entry of the local directory.

5.7.6.3.4.3.2.4 PDU Lifetime

5.7.6.3.4.3.2.4.1 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.

5.7.6.3.4.3.2.5 Segmentation Permitted, More Segments, Error Report Flags

5.7.6.3.4.3.2.5.1 The values of these flags shall be derived from the value of the Protocol ID field and Type field of the Compressed Data PDU.

5.7.6.3.4.3.2.5.2 These flag values shall be determined according to Table 5.7-5 for an Initial Data PDU and Table 5.7-6 for a Derived Data PDU.

5.7.6.3.4.3.2.6 Type Code

5.7.6.3.4.3.2.6.1 This field shall be set to binary [11100] to indicate a DT PDU.

5.7.6.3.4.3.2.7 Segment Length

5.7.6.3.4.3.2.7.1 This field shall indicate the entire length in octets of the PDU, including both header and data.

5.7.6.3.4.3.2.7.2 The value of this field shall be computed by the SNDCF.

5.7.6.3.4.3.2.7.3 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.

5.7.6.3.4.3.2.8 PDU Checksum

5.7.6.3.4.3.2.8.1 The value of this field shall be set to zero if the R bit in the compressed header is zero.

5.7.6.3.4.3.2.8.2 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.

5.7.6.3.4.3.3 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.

5.7.6.3.4.3.3.1 Destination and Source Address Length Indicators and Addresses

5.7.6.3.4.3.3.1.1 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.

5.7.6.3.4.3.3.1.2 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.

5.7.6.3.4.3.3.1.3 The Length fields shall contain the length of each address in octets.

5.7.6.3.4.3.4 Segmentation Part

5.7.6.3.4.3.4.1 General

5.7.6.3.4.3.4.1.1 If the ISO/IEC 8473 SP field is set to one, then the Segmentation Part shall be generated.

5.7.6.3.4.3.4.1.2 The Segmentation Part shall consist of the Data Unit Identifier, Segment Offset, and Total Length field as defined in ISO/IEC 8473.

5.7.6.3.4.3.4.2 Data Unit Identifier

5.7.6.3.4.3.4.2.1 This field shall contain the value of the PDU Identifier field as provided in the compressed DT PDU.

5.7.6.3.4.3.4.3 Segment Offset

5.7.6.3.4.3.4.3.1 For an Initial DT PDU, this field shall be set to zero.

5.7.6.3.4.3.4.3.2 For a Derived DT PDU, this field shall be set to the PDU Segment Offset field as provided in the compressed DT PDU.

5.7.6.3.4.3.4.4 PDU Total Length

5.7.6.3.4.3.4.4.1 For a Derived DT PDU, this field shall contain the value of the PDU Total Length field as provided in the Compressed DT PDU.

5.7.6.3.4.3.4.4.2 For an Initial PDU, the entire length of the PDU in octets shall be calculated by the SNDCF and stored in this field.

5.7.6.3.4.3.5 Options Part

5.7.6.3.4.3.5.1 General

5.7.6.3.4.3.5.1.1 If the Q bit field is set to one, the Globally Unique QoS option shall be recreated according to 5.7.6.3.4.3.5.3.

5.7.6.3.4.3.5.1.2 If the Security option is present in the local reference directory entry, the Security option shall be recreated according to 5.7.6.3.4.3.5.4.

5.7.6.3.4.3.5.1.3 If the P bit field is set to one, the Priority option shall be recreated according to 5.7.6.3.4.3.5.2.

5.7.6.3.4.3.5.2 Priority

5.7.6.3.4.3.5.2.1 For the Priority option, the Parameter Code shall be set to binary [1100 1101] and the Parameter Length set to one octet.

5.7.6.3.4.3.5.2.2 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.

5.7.6.3.4.3.5.3 Quality of Service Maintenance

5.7.6.3.4.3.5.3.1 For the Quality of Service Maintenance option, the Parameter Code shall be set to binary [1100 0011], the Parameter Length set to one octet.

5.7.6.3.4.3.5.3.2 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.

5.7.6.3.4.3.5.4 Security

5.7.6.3.4.3.5.4.1 This field shall be set to the value of the Security parameter contained in the corresponding Local Reference directory entry.

5.7.6.3.4.3.6 Data Part

5.7.6.3.4.3.6.1 The Data Part shall be copied from the Compressed Data PDU data part.

5.7.6.3.4.4 Incoming Compressed Error Report PDU

5.7.6.3.4.4.1 General

5.7.6.3.4.4.1.1 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.

5.7.6.3.4.4.2 Fixed Part

5.7.6.3.4.4.2.1 The Fixed Part of the ER PDU shall be composed in the same manner as defined in 5.7.6.3.4.3.2 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.

5.7.6.3.4.4.3 Address Part

5.7.6.3.4.4.3.1 The Address Part of the ER PDU shall be composed in the same manner as defined in 5.7.6.3.4.3.3.

5.7.6.3.4.4.4 Options Part

5.7.6.3.4.4.4.1 The Options Part of the ER PDU shall be composed in the same manner as defined in 5.7.6.3.4.3.5 for an Initial DT PDU.

5.7.6.3.4.4.5 Reason for Discard

5.7.6.3.4.4.5.1 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.

5.7.6.3.4.4.6 Error Report Data Part

5.7.6.3.4.4.6.1 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.

5.7.6.3.4.5 Incoming SNDCF Error Report

5.7.6.3.4.5.1 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.

5.7.6.3.4.5.2 On receipt of an SNDCF Error Report with reason other than “compressed NPDU with unrecognized local reference” (see Table 5.7-8), the virtual circuit shall be reset (see 5.7.6.3.7) 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.

5.7.6.3.4.5.3 **Recommendation**.— *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 5.7.6.3.5).

5.7.6.3.5 SNDCF Error Report

5.7.6.3.5.1 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.

5.7.6.3.5.2 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 5.7-8:

Table 5.7-8 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

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.

5.7.6.3.5.3 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.

5.7.6.3.5.4 The Error Report PDU shall be sent as an ISO/IEC 8208 DATA packet(s) and, if needed, segmented using the M-bit procedures.

5.7.6.3.6 Local Reference Cancellation Option

5.7.6.3.6.1 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.

5.7.6.3.6.1.1 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.

5.7.6.3.6.1.2 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.

5.7.6.3.6.1.3 When a Cancellation Accept PDU is received, the corresponding directory entries shall be cleared, and the Local References therefore become available for re-use.

5.7.6.3.6.1.4 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.

5.7.6.3.6.1.5 If any one of them is not, then an SNDCF error report shall be returned, and the request ignored.

5.7.6.3.6.1.6 Otherwise, the directory entries corresponding to the indicated local references shall be cleared, and a cancellation accept PDU be formatted and returned, in order to accept cancellation of these local references.

5.7.6.3.6.2 The Cancellation Request PDU

5.7.6.3.6.2.1 The PDU format shall be as illustrated in Figure 5.7-7. 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.

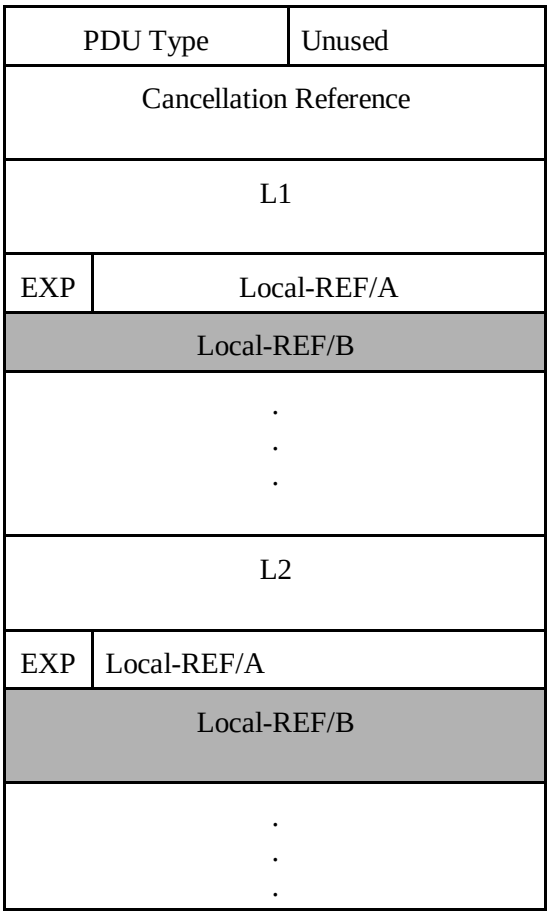


Figure 5.7-7 Cancellation Request PDU

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.

5.7.6.3.6.2.2 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.

5.7.6.3.6.2.3 The extended Local Reference octet shall not be present.

5.7.6.3.6.2.4 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.

5.7.6.3.6.3 The Cancellation Accept PDU

5.7.6.3.6.3.1 The PDU format shall be as illustrated in Figure 5.7-8.

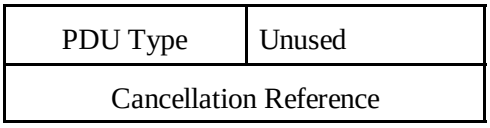


Figure 5.7-8 Cancellation Accept PDU

5.7.6.3.6.3.2 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.

5.7.6.3.7 Call Reset Provisions

5.7.6.3.7.1 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.

5.7.6.3.7.2 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.

5.7.6.3.8 Call Clearing and LREF Procedures

5.7.6.3.8.1 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.

5.7.6.4 Paragraph has been deleted.

5.7.6.5 **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 re-occurring 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 optimises 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.

5.7.6.5.1 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 5.7-9.

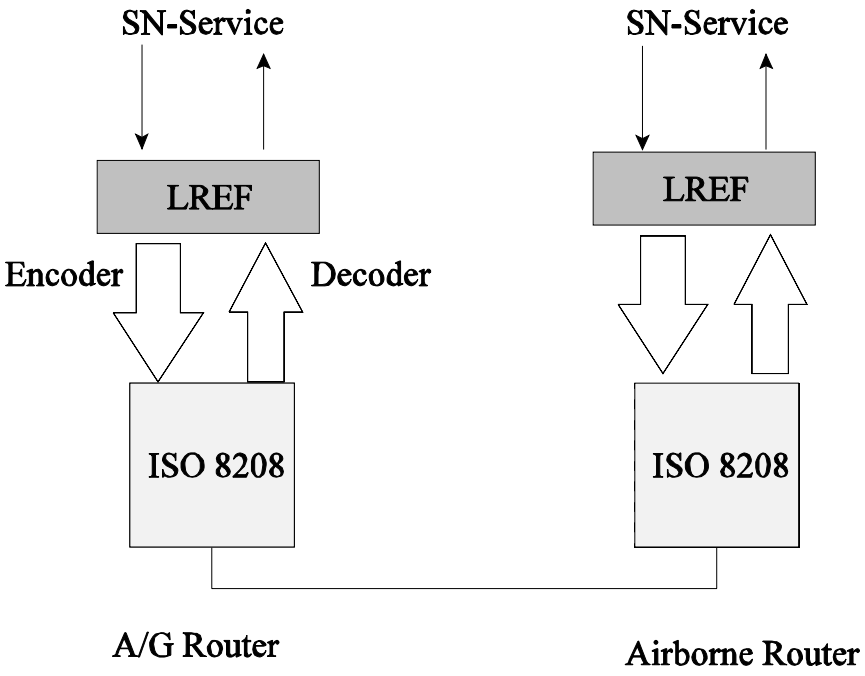


Figure 5.7-9 Relationship of the Deflate Encoder and Decoder to ISO/IEC 8208 and LREF Functions

5.7.6.5.1.1 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.

5.7.6.5.2 Encoded Packet Format

5.7.6.5.2.1 Each NPDU shall be encoded into the compressed representation shown in Figure 5.7-10.

Figure 5.7-10 Compressed Packet Format

5.7.6.5.2.2 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.

5.7.6.5.2.3 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.

5.7.6.5.2.4 The encoded representation of the NPDUs shall be a data stream that is subdivided into a number of bit-aligned blocks of arbitrary length.

5.7.6.5.2.5 Each such block shall be in the format shown in Figure 5.7-11.

Figure 5.7-11 Format of Deflate Data Blocks

5.7.6.5.2.6 Each Deflate Data Block shall comprise:

a) A 3-bit header (H), and

b) A stream of self-delimited compressed data.

5.7.6.5.2.7 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.

5.7.6.5.2.8 The remaining two bits of the header shall be used to indicate the compression type according to Table 5.7-9.

Table 5.7-9 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

5.7.6.5.2.9 When a compressed data block is not wholly transmitted as the final compressed data block of the encoded data (see Figure 5-7.9) 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 5.7.6.5.2.3 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.

5.7.6.5.3 Uncompressed Deflate Data Blocks

5.7.6.5.3.1 When the encoder determines that no benefit can be derived by data compression of a given string, then that string shall be sent uncompressed.

5.7.6.5.3.2 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 5.7-12.

Figure 5.7-12 Format of Uncompressed Deflate Data Blocks

5.7.6.5.3.3 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.

5.7.6.5.3.4 The two length fields (LEN and NLEN) shall be encoded and sent least significant octet first.

5.7.6.5.3.5 The literal data shall be encoded in the same byte order as encountered in the uncompressed data stream.

Note 5.— 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 6.— 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.

5.7.6.5.4 Compressed Deflate Data Blocks using Fixed Huffman Codes

5.7.6.5.4.1 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.

5.7.6.5.4.1.1 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.

5.7.6.5.4.1.2 The Huffman Codes used to encode the literal/length code in the LZ77 compressed data stream shall be as specified in Table 5.7-10.

Note.— Although Table 5.7-10 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 5.7-10 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

5.7.6.5.4.1.3 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 5.7-10. For example, the "Huffman Encoded Value 145" is encoded as a 9-bit bit string "110010001".

5.7.6.5.4.1.4 The Hufman 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.

5.7.6.5.4.1.5 The Huffman codes shall be encoded (packed) into the compressed data block, most significant bit first.

5.7.6.5.4.2 Length/Distance Codes

5.7.6.5.4.2.1 Length Codes

5.7.6.5.4.2.1.1 Huffman-encoded values in the range 257 to 285 shall represent a length code and shall always be followed by an associated distance code.

5.7.6.5.4.2.1.2 Each length code shall represent a particular string length, as specified in Table 5.7-11.

5.7.6.5.4.2.2 Extra Bits for Length Codes

5.7.6.5.4.2.2.1 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.

5.7.6.5.4.2.2.2 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.

5.7.6.5.4.2.2.3 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 5.7-11 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			

5.7.6.5.4.2.3 Distance Codes

5.7.6.5.4.2.3.1 Each length code in the encoded data stream shall be followed by a Huffman-encoded distance code according to Table 5.7-12.

5.7.6.5.4.2.3.2 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.

5.7.6.5.4.2.4 Extra Bits for Distance Codes

5.7.6.5.4.2.4.1 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.

5.7.6.5.4.2.4.2 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.

5.7.6.5.4.2.4.3 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.

5.7.6.5.4.2.5 Semantic

5.7.6.5.4.2.5.1 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.

5.7.6.5.4.2.5.2 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 5.7-12 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

5.7.6.5.5 Compressed Deflate Data Blocks using Dynamically Determined Huffman Codes

5.7.6.5.5.1 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.

5.7.6.5.5.1.1 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.

5.7.6.5.5.1.2 The sequences of code length shall themselves be compressed using a Huffman code and the alphabet for code lengths specified in Table 5.7-13.

Table 5.7-13 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.

5.7.6.5.5.1.3 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.

5.7.6.5.5.2 Block Format

5.7.6.5.5.2.1 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 5.7-13, 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.

5.7.6.5.5.3 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.

5.7.6.5.5.3.1 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*

5.7.6.5.6 Frame Check Sum (FCS)

5.7.6.5.6.1 A two-octet, octet-aligned, frame checksum shall be appended to the end of each encoded packet.

5.7.6.5.6.2 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.

5.7.6.5.6.3 The two octets of the frame checksum shall be the two partial sums C0 and C1 as specified in ISO/IEC 8073 Annex D.

5.7.6.5.6.4 The value of C0 shall be the first octet of the frame checksum parameter and the value of C1 shall be the second octet.

5.7.6.5.6.5 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 Check Sum may be used by the decompression procedure to verify correct decompression of the NPDU.

5.7.6.5.7 Compression Procedure

5.7.6.5.7.1 General

5.7.6.5.7.1.1 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 5.7-10 and specified in section 5.7.6.5.2.

5.7.6.5.7.1.2 The resulting data block shall be a complete encoded representation of the NPDU.

5.7.6.5.7.1.3 **Recommendation.—** *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 optimise 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.

5.7.6.5.7.2 NPDU Encoding

5.7.6.5.7.2.1 The NPDU shall be encoded in the same sequence in which it would have been transmitted if it had not been compressed.

5.7.6.5.7.2.2 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).

5.7.6.5.7.2.3 Octet sequences for which a match has been found within the last 32KB of encoded data shall be encoded as length/distance pairs.

5.7.6.5.7.2.4 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.

5.7.6.5.7.2.5 The distance to the duplicate string shall similarly be encoded using the Huffman Code specified in Table 5.7-11 for the required distance, where necessary also followed by the appropriate extra bits needed to fully define the distance.

5.7.6.5.7.2.6 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).

5.7.6.5.7.2.7 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.

5.7.6.5.7.2.8 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.

5.7.6.5.7.2.9 The Frame Check Sum (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.

5.7.6.5.8 Decompression Procedures

5.7.6.5.8.1 General

5.7.6.5.8.1.1 NPDUs shall be decompressed in exactly the same order that they have been received from the ISO/IEC 8208 subnetwork.

5.7.6.5.8.1.2 Each data packet received from an ISO/IEC 8208 subnetwork shall be assumed to be in the format given by Figure 5.7-10, and thus comprises one or more Deflate Data Blocks.

5.7.6.5.8.2 Compressed Deflate Data Block

5.7.6.5.8.2.1 Each compressed Deflate Data Block shall be interpreted as a sequence of Huffman-encoded symbols.

5.7.6.5.8.2.2 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.

5.7.6.5.8.2.3 The Huffman-encoded value 256 shall be taken as end-of-block indication and not appended to the NPDU that is decompressed.

5.7.6.5.8.2.4 Huffman-encoded values in the range 257..285 shall be taken as length indicators and as introducing a length/distance pair.

5.7.6.5.8.2.5 The length and distance values shall be decoded and the referenced string shall be appended to NPDU that is being decompressed.

5.7.6.5.8.3 Uncompressed Deflate Data Block

5.7.6.5.8.3.1 Octets from uncompressed Deflate Data Blocks shall be appended to the NPDU in the order in which they are encoded.

5.7.6.5.8.4 FCS Verification

5.7.6.5.8.4.1 The Frame Check Sum for the uncompressed NPDU shall be the last two octets of the received packet and shall be verified for all received NPDUs.

5.7.6.5.8.4.2 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.

5.7.6.5.8.4.3 In this case, the call reset procedures specified in 5.7.6.5.9 shall be performed.

5.7.6.5.8.4.4 **Recommendation.—** *The error should be notified to System Management.*

5.7.6.5.9 Call Reset Provisions

5.7.6.5.9.1 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.

5.7.6.5.9.2 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.

5.7.6.5.9.3 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.

5.7.7 ATN Mobile SNDCF Protocol Requirements List

5.7.7.1 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 5.7.7.8.

5.7.7.2 Paragraph has been deleted.

5.7.7.3 Paragraph has been deleted.

5.7.7.4 Paragraph has been deleted.

5.7.7.5 Paragraph has been deleted.

5.7.7.6 Paragraph has been deleted.

5.7.7.7 Paragraph has been deleted.

5.7.7.8 ATN Requirements for Mobile SNDCFs

5.7.7.8.1 Major Capabilities

Item	Capability	ATN SARPs Reference	ATN Support
mcNego	Negotiation of Compression Algorithm	5.7.6.2	M
mcLocRef	Local Reference Header Compression	5.7.6.3	M
mcCan	Local Reference Cancellation	5.7.6.3.6	O
mcM/I	Local Reference directory maintenance	5.7.6.3	Snvdl:M ^Snvdl:O
mcVer2	Version 2 of ISO/IEC 8208 Mobile SNDCF	5.7.6.2	M
mcDict	Negotiation of use of pre-stored dictionaries	5.7.6.2.1, 5.7.6.2.2	mcVer2:O ^mcVer2:-
mcDefMaint	Negotiation of maintenance of Deflate history windows	5.7.6.2.1, 5.7.6.2.2	mcVer2:O ^mcVer2:-
mcDeflate	Deflate Compression	5.7.6.5	O

Note.— Snvdl is true when the VDL SNDCF is implemented.

5.7.7.8.2 Call Setup and Clearing Procedures

Item	Function	ATN SARPs Reference	ATN Support
clInit	Call Initiator	5.7.6.2	O.1
clRspd	Call Responder	5.7.6.2	O.1
csDynam	Dynamic Call Setup	5.7.6.2.1.1.1	clInit:O.2
csSys	Call Setup by Systems Management	5.7.6.2.1.1	clInit:O.2
csDef	Use of non-standard default packet size	5.7.6.2.1.3	clInit:O.3
csNeg	Use of flow control parameter negotiation	5.7.6.2.1.3	clInit:O.3
csFast	Use of Fast Select	5.7.6.2.1.4	M
csM/I	Local Reference directory maintenance request/acceptance	5.7.6.2.1.5.13 5.7.6.2.2.2.3	^csFast: - mcM/I:M
csOther	Use of other optional User Facilities and CCITT-specified DTE facilities	5.7.6.2.1.1.3	O
csCol	Call collision resolution	5.7.6.2.2.1.2	clInit:M
csAcp	Call acceptance procedures	5.7.6.2.1.6	clRspd:M
csRej	Call rejection procedures	5.7.6.2.1.7	clRspd:M
csOrd	Order of compression procedures	5.7.6.2.3.2	M
csDiag	Use of call rejection diagnostic codes	5.7.6.2.1.7.3	clInit:M
csClear	Call clearing procedures	5.7.6.2.4	M

Note.— Fast Select only required if supported by subnetwork.

5.7.7.8.3 Negotiation of Compression Algorithm

Item	Function	ATN SARPs Reference	ATN Support
caMaxd	Indication of the maximum of directories entries in the call user Data	5.7.6.2.1.5.4.11	mcNego:O
caDict	Request/acceptance of use of pre-stored dictionaries	5.7.6.2.1.5.5.7, 5.7.6.2.1.6.1.10, 5.7.6.2.2.2.9.4	mcDict:M ^mcDict:-

Item	Function	ATN SARPs Reference	ATN Support
caDefMaint	Request/acceptance of maintenance of Deflate history windows	5.7.6.2.1.5.5.8, 5.7.6.2.1.6.1.10, 5.7.6.2.2.2.9.3	mcDefMaint:M ^mcDefMaint:-

5.7.7.8.4 Local Reference Header Compression

Item	Function	ATN SARPs Reference	ATN Support
lrVC	Opening additional virtual circuits	5.7.6.3.2.1.2	M
lrDirSize	Local Directory with more than 128 entries	5.7.6.3.1	O
lrProt	Identification of Network Layer Protocol	5.7.6.3.2.2	M
lrMod	Processing of SN-UnitData Requests	5.7.6.3.2	M
lrEst	Establishment of new local reference	5.7.6.3.2.4	M
lrTransfer	Transfer of modified ISO 8473 PDU	5.7.6.3.2.6	M
lrInitial	Initial DT PDU Compression	5.7.6.3.3.2	M
lrDerived	Derived DT PDU Compression	5.7.6.3.3.3	M
lrError-s	Generation of Error PDU Compression	5.7.6.3.3.3	M
lrDiscard	Compression of discarded PDU encapsulated within Error PDU	5.7.6.3.3.4	lrError-s:M
lrCompTr	Transfer of compressed PDUs	5.7.6.3.3.4.1 1	M
lrReceived	Processing of received PDUs	5.7.6.3.4	M
lrUncomp-r	Processing of received uncompressed PDUs	5.7.6.3.4.2	M
LrReset	Purging directories entries on Reset	5.7.6.3.7	mcLocRef:M
lrUnMod-r	Processing of received unmodified PDUs	5.7.6.3.4.2.2	M
lrComp-r	Processing of received compressed data PDUs	5.7.6.3.4.3	M
lrError-r	Processing of received compressed Error PDUs	5.7.6.3.4.4	M
lrSNDCFerr-s	Generation of SNDCF Error Report	5.7.6.3.5	M
lrSNDCFerr-r	Processing of received SNDCF Error Report	5.7.6.3.4.5	M

5.7.7.8.5 Local Reference Cancellation

Item	Function	ATN SARPs Reference	ATN Support
lrcMgmt	Management of local references	5.7.6.3.2.5	mcCan:M
lrcRequest-s	Generation of Cancellation Request PDU	5.7.6.3.6	mcCan:M
lrcRequest-r	Processing of incoming Cancellation Request PDU	5.7.6.3.6	mcCan:M
lrcReliable	Reliable transfer of Cancellation Request	5.7.6.3.6	mcCan:M
lrcAccept-s	Generation of Cancellation Accept PDU	5.7.6.3.6	mcCan:M
lrcAccept-r	Processing of incoming Cancellation Accept PDU	5.7.6.3.6	mcCan:M

5.7.7.8.6 Paragraph has been deleted.

5.7.7.8.7 PDU Formats

5.7.7.8.7.1 Call Request User Data

Item	Description	ATN SARPs Reference	ATN Support
crLen	Length Indicator	5.7.6.2.1.5.3	M
crVersion	Version Indicator	5.7.6.2.1.5.4.1	M
crSNCR	Subnetwork Connection Reference (SNCR)	5.7.6.2.1.5.4.2	M
crComp	Offerred Compression Techniques	5.7.6.2.1.5.4.4	M
crDir	Maximum Directory Size *Note.—Dynamically, this field is only generated if Local Reference Compression is offered.*	5.7.6.2.1.5.4.11	M
crExtBlock	SNDCF Parameter Extension Block	5.7.6.2.1.5.5	mcVer2:M
crDictList	Dictionaries List Parameter	5.7.6.2.1.5.5.7	mcDict:M ^mcDict:-
crDefMaint	Deflate Maintenance Parameter	5.7.6.2.1.5.5.8	mcDefMaint:M ^mcDefMaint:-

Item	Description	ATN SARPs Reference	ATN Support
crAdd-s	Additional User Data on send	5.7.6.2.1.5.6	O
crAdd-r	Additional User Data on receive	5.7.6.2.1.5.6.	O
MaxDir	Maximum number of directory entries supported	5.7.6.2.1.5.4.11	≥ 128

5.7.7.8.7.2 Call Accept User Data

Item	Description	ATN SARPs Reference	ATN Support
caComp	Offerred Compression Techniques	5.7.6.2.2.4.3	mcNego:M
caAdd-s	Additional User Data on send	5.7.6.2.2.4.6	mcNego:O
caAdd-r	Additional User Data on receive	5.7.6.2.2.4.6	mcNego:O
caExtBlock	SNDCF Parameter Extension Block	5.7.6.2.2.4.5	mcVer2:M
caDictSel	Dictionaries Selection Parameter	5.7.6.2.2.4.7	mcDict:M ^mcDict:-
caDefMaint	Deflate Maintenance Parameter	5.7.6.2.1.5.5.8	mcDefMaint:M ^mcDefMaint:-

5.7.7.8.7.3 Modified ISO/IEC 8473 NPDU

Item	Description	ATN SARPs Reference	ATN Support
npLocRef-s	Local Reference Option field	5.7.6.3.2.3	M

5.7.7.8.7.4 Compressed Initial PDU

Item	Description	ATN SARPs Reference	ATN Support
inType	PDU Type	5.7.6.3.3.2.2	M
inPri	Priority	5.7.6.3.3.2.3	M
inLifetime	Lifetime	5.7.6.3.3.2.4	M

Item	Description	ATN SARPs Reference	ATN Support
inFlags	Flag Bits	5.7.6.3.3.2.5 to 5.7.6.3.3.2.9	M
inLocRef	Local Reference (1 octet)	5.7.6.3.3.2.9	M
inLocRef2	Local Reference (2 octet)	5.7.6.3.3.2.9	lrDirSize:M ^lrDirsize:X
inPDUId	PDU Identifier	5.7.6.3.3.2.10	M
inNSDU	User Data	Figure 5.7-5	M

5.7.7.8.7.5 Compressed Derived PDU

Item	Description	ATN SARPs Reference	ATN Support
drType	PDU Type	5.7.6.3.3.3.2	M
drPri	Priority	5.7.6.3.3.3.3	M
drLifetime	Lifetime	5.7.6.3.3.3.4	M
drFlags	Flag Bits	5.7.6.3.3.3.5 to 5.7.6.3.3.3.8	M
drLocRef	Local Reference (1 octet)	5.7.6.3.3.2.8	M
drLocRef2	Local Reference (2 octet)	5.7.6.3.3.2.8	lrDirSize:M ^lrDirsize:X
drPDUId	PDU Identifier	5.7.6.3.3.3.9	M
drSegOff	Segment Offset	5.7.6.3.3.3.10	M
drTotalLen	Total Length	5.7.6.3.3.3.11	M
drNSDU	User Data	Figure 5.7-5	M

5.7.7.8.7.6 Compressed Error PDU

Item	Description	ATN SARPs Reference	ATN Support
erType	PDU Type	5.7.6.3.3.4.2	M
erPri	Priority	5.7.6.3.3.4.3	M
erLifetime	Lifetime	5.7.6.3.3.4.4	M
erFlags	Flag Bits	5.7.6.3.3.4.5 to 5.7.6.3.3.4.8	M
erLocRef	Local Reference (1 octet)	5.7.6.3.3.2.8	M
erLocRef2	Local Reference (2 octet)	5.7.6.3.3.2.8	lrDirSize:M ^lrDirsize:X
erReason	Discard Reason	5.7.6.3.3.4.9	M
erNSDU	Compressed Header of discarded PDU	5.7.6.3.3.4	M

5.7.7.8.7.7 SNDCF Error Report PDU

Item	Description	ATN SARPs Reference	ATN Support
sfType	PDU Type	5.7.6.3.5	M
sfReason	Discard Reason	5.7.6.3.5	M
sfLocRef	Local Reference	5.7.6.3.5	M
sfLocRef2	Local Reference (2 octet)	5.7.6.3.3.2.9	lrDirSize:M ^lrDirsize:X

5.7.7.8.7.8 Cancellation Request

Item	Description	ATN SARPs Reference	ATN Support
cqType	PDU Type	5.7.6.3.6	mcCan:M
cqRef	Cancellation Reference	5.7.6.3.6	mcCan:M
cqLocRef	Local Reference	5.7.6.3.6	M

Item	Description	ATN SARPs Reference	ATN Support
cqLocRef2	Local Reference (2 octet)	5.7.6.3.3.2.9	lrDirSize:M ^lrDirsize:X

5.7.7.8.7.9 Cancellation Accept

Item	Description	ATN SARPs Reference	ATN Support
ccType	PDU Type	5.7.6.3.6	mcCan:M
ccRef	Cancellation Reference	5.7.6.3.6	mcCan:M

5.7.8 SNDCF for Frame Mode Mobile Subnetworks

5.7.8.1 Architecture

Note 1.— The architecture of the Frame Mode SNDCF is more than an SNDCF as normally understood and includes its own data link management protocol. As illustrated in Figure 5.7-13, the specification is provided in two parts: the SNDCF proper and an Air/Ground Communications Sublayer (A/GCS). The A/GCS comprises the multiplexing of many logical channels, the DLCP and the Deflate compression (which operates across channels). The SNDCF itself is responsible for providing the SN-Service over the A/GCS and also incorporates LREF compression, which is CLNP specific. A separate Data Link Manager (DLM) actions data link management requests on behalf of the SNDCF and any other A/GCS users.

Note 2.— The underlying Data Link Layer is assumed to provide:

a) A unicast communications service that provides reliable delivery and preservation of frame transfer sequence order. It may thus be a connection mode service (e.g. VDL2 AVLC) or an acknowledged connectionless service (e.g. VDL3);

b) optionally a broadcast ground-to-air unacknowledged connectionless service;

c) Join and Leave events to signal contact with a new ground station/aircraft, and loss of contact, respectively.

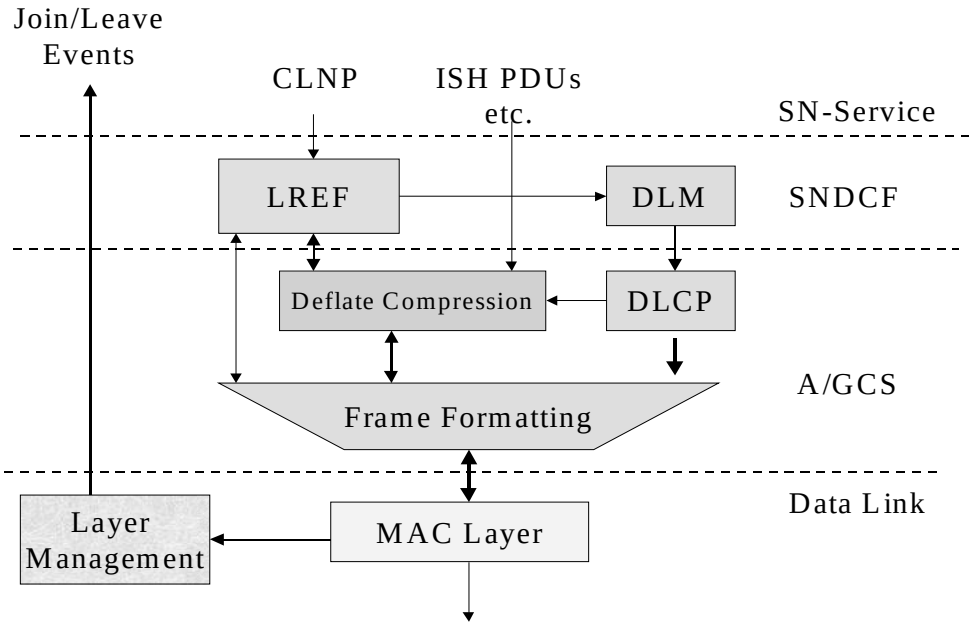


Figure 5.7-13 Frame Mode SNDCF Architecture

5.7.8.1.1 The A/GCS shall provide:

a) a (DLCP supported) Data Link Management service to the DLM and a data communications service, and

b) channel oriented Data Communications service, with channel assignment performed through the Data Link Management interface.

5.7.8.1.2 The data communications service provided by the underlying data link shall be packet oriented and guaranteed to maintain packet delivery order.

Note.— There is no requirement on the underlying data link to guarantee to deliver all packets.

5.7.8.2 Provision of the SN-Service

Note.— The SNDCF provides the required SN-Service. It uses the Data Link Manager (DLM) provided Service to maintain at least one channel for ISH PDUs, and CLNP PDUs that cannot be compressed using LREF. The SNDCF will also use the DLM to assign a new channel to transfer LREF compressed CLNP PDUs.

5.7.8.2.1 General Requirements

5.7.8.2.1.1 In an aircraft, a separate instance of this SNDCF shall be created for each type of subnetwork supported.

5.7.8.2.1.2 When multiple Service Providers are to be accessed concurrently over the same type of subnetwork, then a separate instance shall also be created for each Service Provider.

Note.—Compression state information for the LREF compression algorithm is retained when a data link is terminated for possible use on a later data link connection with a ground station operated by the same Service Provider or an associate. Therefore SNDCF implementation instances are persistent rather than being created and deleted for each data link connection.

5.7.8.2.1.3 In a ground station, instances of this SNDCF shall be created on demand and deleted when no longer required.

Note.—A ground station may be in contact with many different aircraft simultaneously and it needs to balance its resources against demand. Hence, it is unlikely to be practicable to retain an SNDCF instance in the hope that the same aircraft may re-connect – although some implementations may choose to do just this. On the other hand, LREF compression state information will need to be saved so that it can be restored later by the same or a different ground station. Most likely this will be to a file or memory buffer.

5.7.8.2.1.4 The A/GCS shall be used to support communications over the data link service provided by the Air/Ground subnetwork.

5.7.8.2.1.5 The DLM shall be used to initiate data link communications and to manage the use of A/GCS channels.

Note.—DLM data link initiation is usually in response to a Join Event. The IS-SME is responsible for handling Join Events and will typically contact the DLM directly. There is thus no explicit involvement of the SNDCF in data link initiation except that it needs to be aware that a data link now exists so that it can properly respond to SN-Service requests.

5.7.8.2.2 SN Service

5.7.8.2.2.1 The Frame Mode SNDCF shall provide the SN-Unitdata.request and SN-Unitdata.indication service required by CLNP.

5.7.8.2.2.2 The Frame Mode SNDCF shall also provide a data link management interface for use by the IS-SME. This interface shall support:

a) Requests to establish data link communications (airborne systems only);

b) Requests to terminate data link communications.

5.7.8.2.3 Data Transfer

5.7.8.2.3.1 SN-UNITDATA.Request

5.7.8.2.3.1.1 An SN-UNITDATA.Request service shall be provided.

5.7.8.2.3.1.2 This shall take two parameters:

a) the NPDU to be sent to the remote system;

b) the NPDU priority.

5.7.8.2.3.1.3 If an SN-UNITDATA.Request is received and no data link connection exists, the NPDU shall be queued for transmission, in strict priority order, waiting for a data link connection to be established.

Note.—It is a local matter as to how long the NPDU will be queued awaiting a data link connection. However, this retention period should be related to the NPDU's expected lifetime in the network.

5.7.8.2.3.1.4 If an SN-UNITDATA.Request is received and a data link connection does exist, the NPDU shall be queued for transmission, in strict priority order, waiting for a data link to be available.

5.7.8.2.3.1.5 When the data link is available for use and NPDUs are queued for transmission then the NPDU with the highest priority shall be selected for transmission using the A/GCS.

Note.—A/GCS channels may be assigned to LREF format, CLNP Reformatted Headers or ISO TR 9577 format NPDUs, i.e. uncompressed CLNP, ES-IS, etc. When LREF and CLNP Reformatted headers are

both available, it is a local matter as to which is used. Otherwise, the NPDU has to be sent uncompressed. Either way, an A/GCS channel has to be established.

5.7.8.2.3.1.6 If:

a) neither LREF nor CLNP Reformatted headers are supported by the data link, or

b) the NPDU selected for transmission is not a CLNP NPDU, or

c) LREF compression is in use and the CLNP NPDU is a CLNP Echo PDU, or

d) LREF compression is in use and the CLNP NPDU is not compressible by LREF because it satisfies one of the conditions listed in 5.7.6.3.2.3.1,

then if a channel has not already been allocated for sending ISO TR 9577 format NPDUs, the DLCP shall be used to allocate such a channel.

5.7.8.2.3.1.7 The NPDU shall be sent as a user data packet over such a channel.

Note.— For efficiency, it is expected that the Channel Start and NPDU are concatenated into the same transmission frame.

5.7.8.2.3.1.8 If LREF or CLNP Reformatted headers are supported by the data link and the NPDU selected for transmission is a CLNP Data or Error PDU then:

a) Either LREF or CLNP Header reformatting shall be used to transfer the NPDU over the data link. The choice shall be a local decision of the sender;

b) If a channel has not already been allocated for the chosen data format then such a channel shall be allocated using the DLCP;

c) If LREF is the chosen transmission format then the NPDU shall be compressed using the LREF compression procedure and the resulting compressed NPDU transmitted using a channel assigned to the LREF data format;

d) If CLNP Reformatted Headers is the chosen transmission format then the NPDU header shall be reformatted as specified in 5.7.8.2.4.2 and the resulting reformatted NPDU transmitted using a channel assigned to the CLNP Reformatted Headers data format.

Note.—The above procedure can result in both sides simultaneously allocating a channel to the same data format. This is not an error nor is it particularly inefficient.

5.7.8.2.3.2 SN-UNITDATA.Indication

5.7.8.2.3.2.1 If an NPDU is received on a channel assigned to ISO TR 9577 format NPDUs then the NPDU shall be passed to the service user as the user data parameter of an SN-UNITDATA.Indication.

5.7.8.2.3.2.2 If an NPDU is received on a channel assigned to the LREF Data Format, then the NPDU shall be assumed to be in LREF compressed format and decompressed using the LREF decompression procedures specified in 5.7.8.2.4.1.1.

5.7.8.2.3.2.3 The resulting NPDU shall be passed to the service user as the user data parameter of an SN-UNITDATA.Indication.

5.7.8.2.3.2.4 If an NPDU is received on a channel assigned to the CLNP Reformatted Headers Data Format, then the NPDU shall be restored to the proper CLNP Header format by applying the procedures specified in 5.7.8.2.4.2.

5.7.8.2.3.3 The resulting NPDU shall be passed to the service user as the user data parameter of an SN-UNITDATA.Indication.

5.7.8.2.4 Data Compression

5.7.8.2.4.1 LREF Compression

5.7.8.2.4.1.1 General

Note.— The LREF compression algorithm was previously specified for use with an ISO/IEC 8208 communications service. The same algorithm is specified for use here except that the DLCP is used to negotiate the use of LREF (instead of the ISO/IEC 8208 Call setup) and Channel Reset is used instead of an ISO/IEC 8208 Network Reset. Uncompressible PDUs are also sent using a separate channel rather than as part of the same data stream as compressed NPDUs.

5.7.8.2.4.1.1.1 The procedures specified in 5.7.6.3 shall be applied except that:

1) NPDUs are transferred using a channel assigned to the LREF data format instead of an ISO/IEC 8208 virtual circuit;

2) Channel Reset is used instead of Network Reset, and the User Diagnostic parameter of the Channel Reset shall contain the SNDCF Error Report Diagnostic code;

3) When more than one channel is assigned to the LREF data format between the same aircraft and ground station, they shall share a common LREF directory;

4) A Channel Reset on one channel assigned to the LREF data format implicitly applies to the other channels also assigned to the LREF data format.

5.7.8.2.4.1.2 DLCP User Parameters supporting LREF Compression

5.7.8.2.4.1.2.1 Maximum LREF Directory Size

Parameter Code	1000 0000
Parameter Length	variable
Parameter Value	Maximum LREF Directory Size

5.7.8.2.4.1.2.1.1 This parameter shall contain the Maximum LREF Directory Size supported encoded as an unsigned binary number.

5.7.8.2.4.1.2.1.2 The length of the parameter shall be the minimum number of octets needed to express the value.

5.7.8.2.4.1.2.1.3 If this parameter is omitted then a default of 128 shall be assumed.

5.7.8.2.4.1.2.2 LREF Compression State Restored

Parameter Code	1000 0001
Parameter Length	0
Parameter Value	empty

5.7.8.2.4.1.2.2.1 The presence of this parameter shall indicate that the LREF compression state has been restored.

5.7.8.2.4.1.2.3 Local Reference Cancellation Supported

Parameter Code	1000 0010
Parameter Length	0
Parameter Value	empty

5.7.8.2.4.1.2.3.1 The presence of this parameters shall imply the support of the Local Reference cancellation option.

5.7.8.2.4.1.3 Negotiation of the Maximum LREF Directory Size

5.7.8.2.4.1.3.1 During Data Link Initialisation, the initiator shall include a "Maximum LREF Directory Size" parameter in its DLS packet in order to propose a non-default LREF Directory Size.

Note.— The default LREF Directory is 128 as defined above.

5.7.8.2.4.1.3.2 The responder shall examine the proposed Maximum Directory Size proposed by the initiator, which shall be assumed to be the default value if no a "Maximum LREF Directory Size" parameter is present in the received DLS packet.

5.7.8.2.4.1.3.3 The responder shall determine whether or not is it able to support the proposed LREF directory size and, if not shall determine a lower maximum LREF directory size that it can support.

5.7.8.2.4.1.3.4 If the maximum LREF directory size that the responder can support is not the default directory size, then in its DLS response packet, the responder shall include a "Maximum LREF Directory Size" parameter indicating the maximum LREF Directory size that it can support.

5.7.8.2.4.1.3.5 The maximum LREF Directory size used for the data link shall be value of the "Maximum LREF Directory Size" parameter in the responder's DLS packet, or the default value if no such parameter is present.

5.7.8.2.4.1.3.6 If this value is greater than the value initially proposed by the initiator then this a protocol error and the data link shall be terminated by sending a DLE packet with a "Protocol Error" diagnostic code.

5.7.8.2.4.1.4 Restoring the LREF Compression State

5.7.8.2.4.1.4.1 A ground station that receives an incoming data link connection from an aircraft that reports a previous data link connection with an identified ground station shall optionally chose to recover the LREF Compression State, provided that the A/GCS has been able to restore the channel assignments for LREF.

5.7.8.2.4.1.4.2 The previous Ground Endpoint Identifier and Aircraft address shall be used to determine the source of this information.

5.7.8.2.4.1.4.3 The LREF compression state information shall comprise the LREF directory.

5.7.8.2.4.1.4.4 If the LREF compression state has been successfully restored then the DLCP user parameter "LREF compression state restored" shall be returned in the DLS.

Note.—If the ground station is the same as the previous ground station – which is very likely when a single ground station is connected to several ground stations in a given geographical error, the restoring the compression state should be trivial. When the ground station is remote then a communications protocol will be needed to recover the directory information. This could, for example be the Hypertext Transfer Protocol (http) with the Ground Endpoint ID and aircraft address used to construct a conventional URL from where the required compression state will be found.

5.7.8.2.4.2 CLNP Header Reformatting

5.7.8.2.4.2.1 The Reformatted CLNP Header format is specified in 5.7.8.2.4.2.3. The header of an outgoing CLNP NPDU shall be reformatted by changing the encoding of the CLNP header to the header formatted illustrated in Figure 5.7-14.

5.7.8.2.4.2.2 The header of an incoming CLNP NPDU shall be restored to its correct format by parsing the reformatted header and then recreating a proper CLNP Header from this information.

Note.—Note.—The reconstituted header will not necessarily be syntactically identical to the original although the semantics will be unchanged.

5.7.8.2.4.2.3 Reformatted CLNP Data Format

5.7.8.2.4.2.3.1 The reformatted CLNP packet format shall be as illustrated below in Figure 5.7-14.

Note.—The parameter order has been revised in order to optimise Deflate compression by ordering the fields according to increased probability of change from packet to packet.

<table>
<tr><td colspan="4">Version/Protocol Id Extension</td></tr>
<tr><td>sec</td><td>pri</td><td colspan="2">Source address Length Indicator</td></tr>
<tr><td colspan="4">Source Address</td></tr>
<tr><td>rrc</td><td>qos</td><td colspan="2">Destination Address Length Indicator</td></tr>
<tr><td colspan="4">Destination Address</td></tr>
<tr><td colspan="4">Security Parameter (if present)</td></tr>
<tr><td colspan="4">Priority Parameter (if present)</td></tr>
<tr><td colspan="4">The Length Indicator</td></tr>
<tr><td>SP</td><td>Check</td><td>E/R</td><td>Type</td></tr>
<tr><td colspan="4">Data Unit Identifier (if SP set)</td></tr>
<tr><td colspan="4">Total Length (if SP set)</td></tr>
<tr><td colspan="4">Lifetime</td></tr>
<tr><td colspan="4">Route Recording Parameter (if present)</td></tr>
<tr><td colspan="4">QoS Maintenance parameter (if present)</td></tr>
<tr><td>MS</td><td colspan="3">Segment length</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Segment offset (if SP set)</td></tr>
<tr><td colspan="4">Any other options</td></tr>
<tr><td colspan="4">Reason For Discard (for ER PDU only)</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Figure 5.7-14 Reformatted CLNP Packet

5.7.8.2.4.2.3.2 When a CLNP PDU is reformatted as above, the value of each header field is transferred unchanged into the order expressed above.

5.7.8.2.4.2.3.3 The "sec", "pri", "rrc" and "qos" flag shall indicate respectively the presence or absence of the security, priority, route recording and QoS maintenance parameters.

5.7.8.2.4.2.3.4 If the flag is set to one then this shall indicate that the corresponding parameter is present.

5.7.8.2.4.2.3.5 If set to zero then this shall indicate that the parameter is absent.

5.7.8.2.4.2.3.6 The "check" flag shall indicate whether the checksum was used in the original NPDU.

Note.— The value of the checksum is not conveyed within the reorganised PDU format. This is because, as a result of the reorganisation reconstitution process, the rebuilt CLNP PDU while semantically identical may not be syntactically identical to the original CLNP PDU. For example, the order of options may change.

5.7.8.3 The Data Link Manager (DLM)

5.7.8.3.1 DLM Service

5.7.8.3.1.1 The Data Link Manager shall provide Data Link Management services to the Frame Mode SNDCF and any other A/GCS data communications service users.

5.7.8.3.1.2 The DLM Service shall comprise:

1) A Data Link Initiation Service;

2) A Data Link Termination Service;

3) A Channel Management Service.

5.7.8.3.2 Data Link Initiation

5.7.8.3.2.1 Initiator Procedures

5.7.8.3.2.1.1 The Data Link Initiation service shall support the following parameters:

1) Data Link Identifier;

2) User Data.

Note 1.—The Data Link Identifier is a local identifier provided in a Join Event from the underlying data link service provider. It is used to select the air/ground data link connection that will be used for exchange of A/GCS frames. This may be a data link connection that has already been established prior to issuing the Join Event, or it may be a potential data link for which a Join Event has been issued but will not actually be established until a frame (e.g. a DLCP DLS) is available to downlink.

Note 2.—Multiple Air/Ground Data link connections may be concurrently available over the same or via different air/ground networks. All A/GCS services have thus to be invoked in the context of a given data link identifier which is then used to select the correct data link connection.

5.7.8.3.2.1.2 On receipt of a Data Link Initiation request from the DLS User:

a) If a DLCP connection already exists using this Data Link Identifier, then the request shall be ignored;

b) The A/GCS shall be used to initialise data communications with the ground station implicitly identified by the Data Link Identifier;

c) If User Data was provided with the Data Link Initialisation request then this shall be included in the DLCP DLS;

d) The Ground Endpoint Identifier of the ground station with which the SNDCF last had or currently has a data link connection, if any, shall be included as the value of the "Previous Ground Endpoint ID" DLCP parameter;

e) If LREF is supported then this shall be included in the list of Data Link Capabilities provided on the DLCP DLS, and the maximum LREF directory size other than the default of 128 shall be indicated to the remote system by including this as a DLS user parameter as specified in 5.7.8.2.4.1.2.1;

f) Other data link capabilities shall be included if supported and when local policy requires them to be offered;

g) If LREF Local Reference Cancellation is also supported then the DLCP user parameter "Local Reference Cancellation supported" shall be included in the DLCP DLS;

h) If CLNP Header reformatting is supported then this shall be included in the list of data link capabilities.

5.7.8.3.2.1.3 If the A/GCS DLCP successfully establishes a DLCP connection then:

a) If user data was returned on the DLCP DLS then this shall be assumed to be an NPDU and passed to the sn-service user using an SN-UNITDATA.indication;

b) If LREF is supported and the DLCP user parameter providing the maximum LREF directory size is included in the DLS then this shall used as the maximum directory size, otherwise the default of 128 shall be used as the maximum directory size. If the maximum directory size thereby determined is greater than that offered on the aircraft's DLS then the data link connection shall be terminated with a protocol error diagnostic;

c) If the DLCP user parameter "Local Reference Cancellation supported" is present then the LREF Local Reference Cancellation option shall be available for use, unless the parameter was not included in the aircraft's DLS when the data link shall be terminated with a protocol error diagnostic;

d) If the DLCP user parameter indicating "LREF compression state restored" is present then the LREF directory from the previous data link connection shall be retained and used for this data link connection. If the parameter is not present then the LREF directory shall be re-initialised to its empty state.

Note.— It is possible that the DLM Data Link Initiation procedures may be started by a A/GCS service user other than the Frame Mode SNDCF. However, LREF parameter exchanges will still take place as long as the Frame Mode SNDCF is supported by the implementation and this information may be used later by the Frame Mode SNDCF if CLNP packets are also exchanged over the data link.

5.7.8.3.2.2 Responder Procedures

5.7.8.3.2.2.1 The responder procedures shall be implemented by a ground based system implementing this specification.

5.7.8.3.2.2.2 When the A/GCS indicates that a DLS has been received from an aircraft:

a) The receiving System shall, optionally, make a local decision as to whether to accept or reject the data link connection, and, if the data link connection is accepted;

b) If any user data is provided on the DLS this shall be assumed to be an NPDU and passed to the sn-service user using an SN-UNITDATA.indication;

c) If LREF compression is included in the list of data link capabilities and LREF is also supported by the responding system then the DLCP user parameter providing the maximum LREF directory size shall be extracted if present and a default of 128 assumed if it is not present;

d) If the DLCP user parameter "Local Reference Cancellation supported" is present and the LREF Local Reference Cancellation option is also supported by the responding system then this option shall be available for use on the data link;

e) If a Previous Ground Endpoint ID parameter is included in the DLS and LREF compression state restoration is supported by the responding system, then it shall attempt to recover the LREF compression state as specified in 5.7.8.2.4.1.3.

5.7.8.3.2.2.3 If the data link connection is rejected then the DLCP data link connection rejection procedure shall be invoked.

5.7.8.3.2.2.4 If the data link connection is accepted then the DLCP data link connection acceptance procedures shall be invoked to return a DLS to the aircraft.

5.7.8.3.2.2.5 This shall include:

a) A user data parameter, if available;

Note.— The user data typically contains the responding system's ISH PDU.

b) If LREF is supported and was also listed in the Data Link Capabilities parameter provided by the aircraft, a DLCP user parameter, as specified in 5.7.8.2.4.1.2.1, shall be provided indicating the maximum directory size that may be used, and calculated as the smaller of the maximum directory sizes supported by the aircraft and ground station, respectively;

c) If the LREF Local Reference Cancellation option is available for use (i.e. the DLCP user parameter "Local Reference Cancellation supported" was present in the aircraft's DLS and the option is also supported by the ground station) then the DLCP user parameter "Local Reference Cancellation supported" shall be included;

d) If the LREF Compression state has been successfully restored, then the DLCP User Parameter "LREF Compression State restored" (see 5.7.8.2.4.1.2.2) shall be included.

5.7.8.3.2.3 Data Link Termination

5.7.8.3.2.3.1 If a data link termination request is received then the data link connection, if any, shall be terminated using the DLCP.

Note.— The data link service provider will normally be requested to terminate the underlying data link connection itself. However, this will depend upon the type of data link.

5.7.8.3.2.3.2 If a Leave Event is received from the data link service provider then the associated DLCP connection shall be implicitly terminated (i.e. no protocol exchanges take place).

5.7.8.3.2.3.3 If LREF is supported and in use, the LREF compression state shall be retained following the DLCP connection termination.

5.7.8.3.2.4 Channel Management

5.7.8.3.2.4.1 The DLM shall provide Channel Management service to users of the A/GCS data communciations service supporting Channel Start, Channel Reset and Channel End services.

5.7.8.3.2.4.2 An GCS data communciations service. shall be permitted to establish more than one channel with the same data type.

Note.— This may be (e.g.) to take advantage of different Deflate dictionaries for different subtypes of the identified data type. For example, both ATC and AOC data are CLNP LREF compressed data but may required different Deflate Dictionaries.

5.7.8.3.2.4.3 When a Channel Start is received from the peer system then the A/GCS data communications service known to be responsible for the associated data type shall be notified.

5.7.8.4 The Air/Ground Communications Sublayer (A/GCS)

5.7.8.4.1 General

Note.— This specification applies to mobile subnetworks having the following characteristics:

a) data packets are sent unicast over a data link layer service that is generally reliable. Examples include an acknowledged connectionless procedure that notifies the sender if the packet has been successfully delivered or not, and a connection mode service that guarantees delivery until failure is notified;

b) The Data Link Service is assumed to have a low probability of packet loss or duplication;

c) In the air- to-ground direction a single ground station receives all downlinks. In the ground-to-air direction, a specific aircraft is identified as the packet's destination;

d) Data packets are subject to a specified maximum packet size.

5.7.8.4.2 Architecture

Note 1.— The A/GCS communications model is that of a lightweight protocol dividing communications between a given aircraft and the ground station into a number of separate prioritised channels. One channel is reserved for control packets; the purpose of the remaining channels is determined through an exchange of control packets.

Note 2.— The architecture of the A/GCS is presented in Figure 5.7-15.

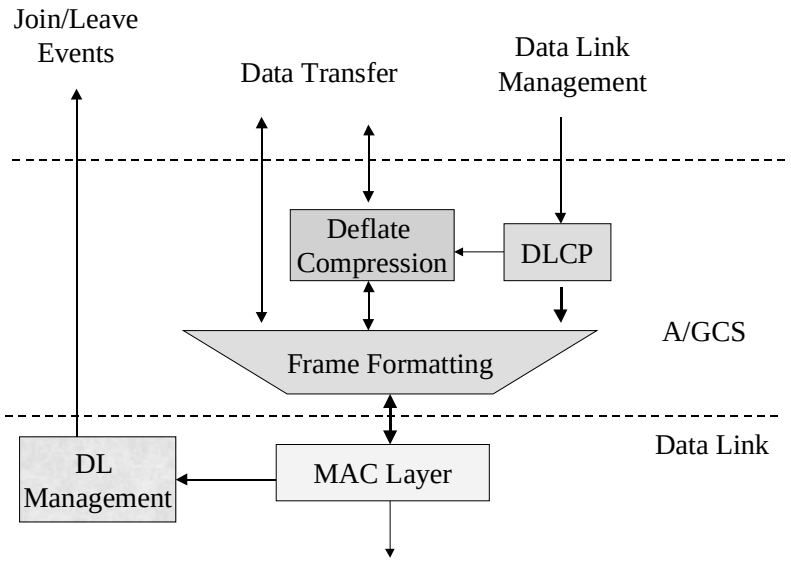


Figure 5.7-15 A/GCS Architecture

Note.—The A/GCS assumes direct access to a MAC layer communications service. A Data Link (DL) Management entity also provides Join and Leave events to the IS-SME.

5.7.8.4.2.1 In an aircraft, a separate instance of the A/GCS shall be created for each type of subnetwork supported.

5.7.8.4.2.2 When multiple Service Providers are to be accessed concurrently over the same type of subnetwork, then a separate instance shall also be created for each Service Provider.

Note 1.—Compression state information is retained on Handoff between ground stations on the same subnetwork which either belong to the same Service Provider or its associates. Therefore, instances of the airborne A/GCS are not created and deleted for each individual data link connection but are instead persistent so that compression state is retained across data link handoff.

Note 2.— When multiple instances of the A/GCS are supported on the same data link in order to support access to multiple data link service providers, some local means will be necessary to relate incoming frames to the appropriate A/GCS instance.

5.7.8.4.2.3 In a ground station, instances of the A/GCS shall be created and deleted on demand for each data link connection with a given aircraft.

Note.—A ground station may be in contact with many different aircraft simultaneously and it needs to balance its resources against demand. Hence, it is unlikely to be practicable to retain an A/GCS instance in the hope that the same aircraft may re-connect – although some implementations may choose to do just this. On the other hand, compression state information will need to be saved so that it can be restored later by the same or a different ground station. Most likely this will be to a file or memory buffer.

5.7.8.4.3 Logical Channels

5.7.8.4.3.1 Frames

Note 1.—Each transmitted frame is assigned to a logical channel. Channel number zero is reserved for Data Link Control messages. All other logical channels may be compressed using Deflate, although the protocol is flexible enough to be extended in a backwards compatible manner to support other compression schemes (e.g. voice compression). One deflate compressed channel is typically assigned to ISO TR 9577 identified packets (e.g. ES-IS and CLNP). This is used for ISH PDUs and any CLNP PDUs that cannot be compressed by LREF. Another channel may be assigned for LREF compressed PDUs and a further, experimental, channel may be assigned for CLNP PDUs with re-ordered header fields. The protocol design is aimed at both minimising bandwidth and providing the flexibility for future extension.

Note 2.—Multiple frames may also be concatenated into a single transmission frame in order to minimise transmission overheads. On receipt, the transmission frame is broken up into the frames contained within it which are then processed in the order in which they were concatenated into the transmission frame i.e. the transmission order within the frame determines the processing order. Each frame is then processed depending upon its logical channel.

5.7.8.4.3.1.1 Each frame shall be formatted as illustrated in Figure 5.7-16. There shall be four fields:

a) The Logical Channel (LC) field (12 bits);

b) The Priority field (4 bits);

c) The Length field (16 bits);

d) The User Data field (all remaining octets in the frame).

5.7.8.4.3.1.2 This four field group shall be repeated one or more times within the maximum transmission frame size.

Figure 5.7-16 Frame Format

5.7.8.4.3.2 Field Definitions

5.7.8.4.3.2.1 The LC field comprises the first 12 bits of the frame transmitted and shall identify the logical channel on which the frame is sent.

5.7.8.4.3.2.2 The first octet transmitted shall comprise the high order 8 bits and the most significant four bits of the second octet shall comprise the low order 4 bits of the 12 bit channel number.

5.7.8.4.3.2.3 Channel number zero shall be reserved for data link control. Channel numbers in the range FF0h to FFFh are not available for use and shall not be assigned to any channel.

5.7.8.4.3.2.4 The Pr field comprises the low order 4 bits of the second octet of the frame and shall identify the frame's priority as an unsigned binary number in the range zero to 15. Zero shall represent the lowest priority.

5.7.8.4.3.2.5 The Len field comprises the next 16 bits of the frame transmitted and shall identify the length of the subsequent user data field in octets.

5.7.8.4.3.2.6 The first octet of the length field shall contain the most significant byte and the second octet shall contain the least significant byte.

5.7.8.4.3.2.7 The user data field shall follow the Len field.

5.7.8.4.3.2.7.1 This shall always a whole number of binary octets (as given by the Len field), and each octet is transmitted least significant bit first.

5.7.8.4.3.3 Concatenation

5.7.8.4.3.3.1 Multiple frames addressed to the same destination may be concatenated together for transmission in a single data link "burst" (i.e. transmission frame) up to the maximum frame size supported by the communications media.

5.7.8.4.3.3.2 Frames of different priorities shall not be concatenated together unless:

a) the sender controls access to the medium and there are no unfulfilled requests for access to the medium for packets of a higher priority than the lowest priority frame in the concatenated frame;

b) the sender has already been given permission to send a frame with a priority equal to the lowest priority frame in the concatenated frame;

c) the transmission medium does not support priority based access.

Note.—In VDL Mode 3, the ground station controls access to the medium and gives permission to send based on data priority.

5.7.8.4.3.3.3 On receipt, the received frames shall be processed in strict order of receipt.

5.7.8.4.3.4 Data Transfer

5.7.8.4.3.4.1 Once a channel has been assigned to a given purpose using the DLCP, user data may be transferred as a series of frames sent with that channel number included in the frame header.

5.7.8.4.3.4.2 The frame priority shall be set to reflect the priority of the data contained within the frame.

5.7.8.4.3.4.3 The frames on a given channel shall comprise a continuous data stream fragmented and then re-assembled in strict transmission order. Each channel shall support bi-directional data transfer.

Note.—A given data format may specify that frame boundaries are significant in determining packet boundaries. However, this is a feature of the data format and not the channel concept.

5.7.8.4.3.4.4 On reception the channel number shall be used to determine the format of the data contained in the frame and how it is processed.

5.7.8.4.3.4.5 If a frame is received containing an unknown channel number, the frame shall be discarded and the problem reported to the peer system by using the DLCP to send a Channel Reset packet identifying the problem.

5.7.8.4.3.4.6 If the channel has been assigned to a data compression algorithm then the user data field of each frame sent over the channel shall be compressed using that algorithm.

5.7.8.4.3.4.7 The compression shall take place immediately prior to transmission and in the order in which multiple frames sharing the same compression algorithm are concatenated into a transmission frame.

5.7.8.4.3.4.8 On reception, the user data shall be decompressed using the corresponding decompression algorithm and in the order in which the frames were received and/or concatenated into the same data link frame.

Note.—It is important that the compression takes place immediately prior to transmission as data using the same compression algorithm can be sent at different priorities and hence may overtake each other in a transmission queue.

5.7.8.4.3.5 Congestion Handling

5.7.8.4.3.5.1 When an implementation becomes congested it shall delete sufficient low priority frames in its outgoing queues in order to return to an uncongested state.

Note.—The definition of congested and uncongested are a local matter. However, a typical strategy is to specify a "high water mark" for the number of used buffers that signals when the congested state is entered, and a "low water mark" for the number of used buffers that signals when the uncongested state has been reached.

5.7.8.4.3.6 Data Compression Procedures

5.7.8.4.3.6.1 Deflate Compression

Note 1.—The Deflate Compression procedures are specified in 5.7.6.5.

Note 2.—The A/GCS permits the concurrent use of multiple Deflate compressed data streams each associated with a different dictionary including the empty dictionary. Each such Deflate compressed data stream is unidirectional and is associated with one or more channels. Data on each such channel is compressed as part of the same data stream. Although the compressed data streams in each direction of data transfer are unidirectional, when Deflate compression is applied to a channel in one direction, it is also applied on the same channel in the other direction and using the same dictionary.

Note 3.—A Deflate Dictionary is an octetstring of frequently used symbols and may be up to 32KB long. A Deflate Dictionary Identifier uniquely identifies a such a dictionary. A different octetstring may apply to the uplink direction compared with the downlink direction.

5.7.8.4.3.6.1.1 Deflate Data Compression with a given dictionary, or with no dictionary, shall only be used when the corresponding compression algorithm identifier has been included in both an aircraft and ground station’s DLS/DLR packet and the exchange of DLS/DLR packets has been completed.

5.7.8.4.3.6.1.2 Initialisation

5.7.8.4.3.6.1.2.1 When the use of the Deflate data compression algorithm has been agreed on data link initialisation or restart, the compressor and decompressor in each direction shall be initialised prior to their use on any channel.

5.7.8.4.3.6.1.2.2 If the use of multiple Deflate dictionaries has been agreed then a separate compressor/decompressor shall be used for each dictionary.

5.7.8.4.3.6.1.2.3 The compressor/decompressor for a given dictionary shall be initialised by:

a) applying the contents of the dictionary into the compressor and discarding the result;

b) initialising the history buffer of the decompressor with the dictionary contents.

5.7.8.4.3.6.1.2.4 When Deflate is re-initialised following a Link Reset, the applicable dictionary, if any, shall also be initialised as specified above.

5.7.8.4.3.6.1.3 Data Transfer

Note 1.—A data stream compressed using Deflate may be modelled as a byte stream starting at byte zero and with each successive byte identified by its relative position in the data stream expressed as an offset from the start of the stream. The first byte is at offset zero.

Note 2.—Deflate maintains an active window on this data stream which may be up to 32KB wide. The stream offset to the start of this window is known as the lower window edge and the stream offset to the end of this window is known as the higher window edge. As the data stream is transferred from one system to another both lower and higher window edges follow the data transfer with the higher window edge always positioned at the current end of the stream and the lower window edge position at the start of the stream or "window size" bytes before the higher window edge. Compression is partly achieved by replacing repeated strings by backwards references to an earlier occurrence within this window.

Note 3.—If there is a data transfer error then the sender's higher window edge will be in advance of the receiver's higher window edge. A reset procedure is needed to reset it to the receiver's higher window edge. Although the sender's lower window edge will also be in advance of the receiver's lower window edge there is no need to adjust this.

5.7.8.4.3.6.1.3.1 If the use of Deflate and optionally a Deflate dictionary was specified in the Channel Start DLCP packet for a given channel, Deflate compression shall apply to all data sent on that channel in both directions of data transfer.

Note.—There is no requirement to re-initialise an existing data compression stream when a Channel Start is issued identifying a dictionary that is already in use. The identified channel simply joins the list of channels using the compressor/decompressor.

5.7.8.4.3.6.1.3.2 The User Data of a channel frame shall be compressed as a single packet as specified in 5.7.6.5.2.

5.7.8.4.3.6.1.3.3 Frames shall be compressed in strict transmission order regardless of the channel with which they are associated.

5.7.8.4.3.6.1.3.4 The resulting compressed frame shall include the FCS.

Note.—The channel header is not compressed – only the user data.

5.7.8.4.3.6.1.3.5 When a frame is received on a channel assigned for use with Deflate compression then the user data shall be decompressed using the Deflate decompressor associated with the Deflate Dictionary assigned to the channel, if any.

5.7.8.4.3.6.1.3.6 Frames shall be decompressed in strict order of reception regardless of the channel with which they are associated.

5.7.8.4.3.6.1.3.7 A compressor shall not use a backwards reference greater than the Deflate Compression Window size agreed when the data link is initialised or restarted.

5.7.8.4.3.6.1.4 Error Recovery

5.7.8.4.3.6.1.4.1 If an FCS failure is detected following decompression then the DLCP Reverse Link Reset procedure shall be invoked in order to report and recover from the problem.

5.7.8.4.3.6.1.4.2 The sender shall indicate using the Compressed Data Stream Resync DLCP parameters:

a) the data compression algorithm to which the reset applies (i.e. Deflate) and the associated dictionary, if any, and

b) the data stream position of the last successfully received packet, expressed as the offset of the last received octet after decompression from the start of the data stream, i.e. when the decompressor was last initialised.

Note.—Link Reset applies only to one direction of data transfer at any one time.

5.7.8.4.3.6.1.4.3 If an FCS error occurs immediately after a link reset or the recovery of compression state information on handoff, then the Reverse Link Reset procedure shall again be invoked in order to reset the compression stream to the initial state.

Note.—This is because there is a high probability that there is a more fundamental problem, and re-initialisation of the compressed data stream is appropriate in such a case.

5.7.8.4.3.6.1.5 Receiving a Link Reset

5.7.8.4.3.6.1.5.1 When a DLCP Link Reset packet is received indicating resync of a Deflate compressed stream, the indicated compressor shall be reset.

5.7.8.4.3.6.1.5.2 The compressor shall be set so that either:

a) the Deflate Compression Window now ends with the last octet that was correctly received by the peer system, as indicated by the Link Reset, or

b) the Deflate Compressor is re-initialised with the associated Deflate Dictionary, if any, loaded into the compressor.

5.7.8.4.3.6.1.5.3 A DLCP Link Reset packet shall be returned with the Compressed Data Stream Resync Parameter indicating whether the compressor was reset to the requested position or re-initialised.

5.7.8.4.3.6.1.5.4 The AK Sequence number parameter shall be included to indicate that this is a confirmation of reset by identifying the sequence number of the Link Reset Request.

5.7.8.4.3.6.1.5.5 If the indicated last octet received is in advance of the current compressor position then the compressed data stream shall always be reset to the initial state.

Note 1.— This error is indicative of a software error in the sender or receiver and appropriate diagnostic information may also need to be logged.

Note 2.— The term "in advance of" needs to be treated with caution as stream offsets are 32-bit numbers that wrap around to zero.

5.7.8.4.3.6.1.6 Completing the Error Recovery Procedure

5.7.8.4.3.6.1.6.1 When a DLCP Link Reset packet is received in response to a Link Reset, the decompressor shall be re-initialised to the indicated position in the data stream.

5.7.8.4.3.6.1.6.2 If the indicated position to which the data stream has been reset is in advance of the current decompressor position then the Data Link Restart procedures shall be invoked to restore the data link to a defined state.

Note 1.— This error is indicative of a software error in the sender or receiver and appropriate diagnostic information may also need to be logged.

Note 2.— The term "in advance of" needs to be treated with caution as stream offsets are 32-bit numbers that wrap around to zero.

5.7.8.4.3.6.1.6.3 Any compressed data packets received on a given Deflate compressed data stream between the transmission of a Link Reset and the receipt of a Link Reset acknowledgement shall be ignored.

5.7.8.4.3.6.1.7 Restoring the Deflate Compression State

Note.—Restoring the compression state is largely a ground based problem. The aircraft still has its active window onto the Deflate data stream. The ground side must obtain a copy of the active window for both directions and synchronise the upper window edge with the aircraft's active window onto the data stream.

5.7.8.4.3.6.1.7.1 When an aircraft sends a DLS to a ground station and the sending A/GCS instance used Deflate compression for one or more channels on the data link to the previous ground station, if any, it shall include the Deflate Compression State parameter in the DLS for each Deflate compressor that was active and for which the ground-to-air compression state is still available.

5.7.8.4.3.6.1.7.2 The parameter value shall include the position of the data stream, i.e. the Higher Windows Edge.

5.7.8.4.3.6.1.7.3 When a DLS is received from an aircraft, a ground station shall perform restoration of the Deflate compression state by:

a) obtaining the current Deflate compression state from the previous ground station, if any, and

b) loading the appropriate Deflate Compressor and Decompressor with the compression state, and

c) indicating the stream positions (both ground-to-air and air-to-ground) of the restored compression state in the Compression State Restored parameter.

5.7.8.4.3.6.1.7.4 The restored stream position for the ground-to-air direction shall be the stream position indicated by the aircraft in the Deflate Compression State Information parameter.

Note.— This may require adjustment of the Deflate Upper Windows edge in the retrieved compression state information to match the current stream position of the aircraft decompressor.

5.7.8.4.3.6.1.7.5 If the aircraft stream position is in advance of the stream position obtained from the previous ground station then the data stream shall be re-initialised and this indicated on the Compressed State restored parameter.

5.7.8.4.3.6.1.7.6 An airborne system shall carry forward the compression state from the previous data link connection.

Note.— This may require adjustment of the Deflate Upper Windows edge in the carried forward compression state information to match the current stream position of the restored ground station's decompressor.

5.7.8.4.3.6.1.7.7 If the aircraft is unable to accept an indicated stream position in the ground-to-air direction, then the aircraft shall use the Reverse Link Reset procedure to return the data stream to the initial state.

5.7.8.4.3.6.1.7.8 If the aircraft is unable to accept an indicated stream position in the air-to-ground direction, then the aircraft shall invoke the Forward Link Reset procedures to indicate that the affected data stream is being returned to its initial state.

5.7.8.4.4 The Data Link Control Protocol (DLCP)

5.7.8.4.4.1 General

Note 1.—The purpose of the DLCP is to manage the assignment and use of the remaining channels and the data compression functions.

Note 2.— Channel zero is dedicated to the Data Link Control Protocol (DLCP). However, following Data Link Initiation, all other channels are unassigned.

Note 3.— The DLCP is specified as a robust protocol designed to recover from packet loss in the MAC layer.

5.7.8.4.4.1.1 Channel zero shall be dedicated to the Data Link Control Protocol (DLCP).

5.7.8.4.4.1.2 The Data Link Control Protocol (DLCP) shall comprise the following packet formats:

1) DATA LINK START (DLS);
2) DATA LINK RESTART (DLR);
3) DATA LINK END (DLE);
4) CHANNEL START (CS);
5) CHANNEL END (CE);
6) CHANNEL RESET (CR);
7) LINK RESET (LR).

5.7.8.4.4.1.3 The format of each DLCP packet shall be as shown below.

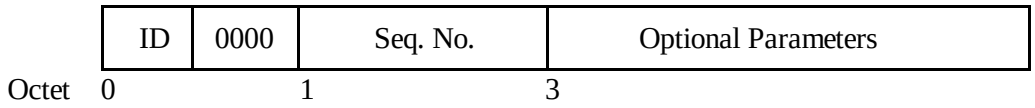


Figure 5.7-17 Channel Independent DLCP Packet Format

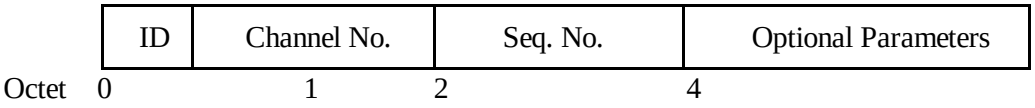


Figure 5.7-18 Channel Dependent DLCP Packet Format

5.7.8.4.4.1.4 The DLCP packet shall comprise:

a) A four bit Identifier field (ID) encoded as an unsigned binary number occupying the most significant four bits of the first byte;

Note.— Conventionally, the most signficant bit of the ID field indicates whether the Channel Independent format (set to 0) or the channel dependent format (set to 1) is used.

b) In the Channel Independent Format the least significant four bits of the first octet shall be set to zero;

c) In the Channel Dependent Format, a 12-bit channel number shall be encoded with the most significant four bits of the channel number occupying the least significant four

bits of the first octet, and the least significant eight bits of the channel number encoded as the second octet;

d) A 16-bit sequence number also encoded as an unsigned binary number. The most significant byte of the sequence number shall be encoded as the first octet of the sequence number field and the least significant byte shall be encoded as the second octet;

e) Zero, one or more optional parameters. The optional parameters are encoded as Type Length Value (TLV) parameters using the same encoding procedures as specified for the options part of the PDU header in ISO/IEC 8473. The permissible set of optional parameters is specified separately for each DLCP packet.

5.7.8.4.4.1.5 The DLS, DLR, CS and CE DLCP packets may have optional user specified parameters that are passed through transparently by the DLCP.

5.7.8.4.4.1.6 Parameter codes in the range 1000 0000 to 1100 1111 shall be reserved for user specified parameters.

5.7.8.4.4.1.7 An implementation receiving an unknown DLCP packet (i.e. with an unknown identifier field value) shall declare a protocol error and invoke the Data Link Restart procedures to return the data link to a defined state.

Note.— The backwards compatible mechanism for the introduction of new features is provided by the DLS packet. Hence, an unidentified DLCP packet will always be a protocol error.

5.7.8.4.4.1.8 On data link initiation, the first DLCP packet sent shall have a sequence number of zero. The sequence number shall be incremented for each subsequent DLCP packet.

5.7.8.4.4.1.9 On reaching the maximum value (i.e. 216-1), the sequence number shall wrap round to zero.

5.7.8.4.4.1.10 An implementation receiving a DLCP packet with a lower sequence number than that previously received shall ignore the packet.

Note 1.— Because of wrap around, implementers should treat the term "lower" with a certain degree of caution.

Note 2.— As a local matter, an implementation may limit the number of acceptable protocol errors from a specific peer system and terminate the data link if that limit is exceeded.

5.7.8.4.4.1.11 Both aircraft and ground stations shall maintain a variable tracking the last received sequence number from the peer system.

5.7.8.4.4.1.12 This shall be set to zero on data link initiation, and thereafter set to the value of the sequence number in each received and processed frame.

5.7.8.4.4.1.13 With the exception of a DLS with a sequence number of zero, an incoming frame shall be ignored if its sequence number is the same or less than the last received sequence number.

5.7.8.4.4.1.14 All DLCP packets shall be sent using the highest priority, i.e. priority 15.

Note.— A DLCP packet exchange may be an essential preliminary to the sending of high priority data and hence some DLCP packets have to be sent at the highest priority i.e. 15. As the DLCP also requires that packets are sent and received in sequence number order, it does not make sense to differentiate DLCP packet priorities as this could result in unnecessary protocol errors.

5.7.8.4.4.2 DLCP Procedures

5.7.8.4.4.2.1 Data Link Initialisation

5.7.8.4.4.2.1.1 Data Link Initialisation shall be performed by an aircraft only.

5.7.8.4.4.2.1.2 When initialising a data link, the aircraft shall mark all channels other than channel zero as unassigned and send a DLS packet.

5.7.8.4.4.2.1.3 On receipt of a DLS packet. the ground station shall also mark all channels other than channel zero as unassigned.

5.7.8.4.4.2.1.4 It shall then apply the Compression State recovery procedures specified in 5.7.8.4.3.6.2.6, and return its own DLS packet in acknowledgement.

5.7.8.4.4.2.1.5 The DLS's sequence number shall be set to zero on data link initialisation. The DLS sent in acknowledgement to a received DLS shall have the same sequence number as in the received DLS.

5.7.8.4.4.2.1.6 A timer t_1 shall be started whenever a DLS is sent, and reset when the DLS is acknowledged.

5.7.8.4.4.2.1.7 If timer t_1 expires before the DLS is acknowledged then the sequence number shall be incremented, the DLS shall be sent and timer t_1 restarted.

5.7.8.4.4.2.1.8 Each time timer t_1 is restarted the timer duration shall be increased by 50%.

Note.— The purpose of this procedure is to ensure that a timer set to an unrealistically short interval does not prevent communication.

5.7.8.4.4.2.1.9 If a ground station receives a further DLS initialising the data link (i.e. with higher sequence number), it shall:

a) deallocate any channel allocations it had made since the receipt of the previous DLS, and

b) again return its own DLS packet in acknowledgement.

5.7.8.4.4.2.1.10 A DLS with the same or lower sequence number than a previously received DLS shall be ignored.

5.7.8.4.4.2.1.11 No other packet may be sent by the aircraft until a valid DLS has been received in response.

5.7.8.4.4.2.1.12 Any other packets received from the ground station other than a responding DLS or a DLE shall be silently discarded.

5.7.8.4.4.2.1.13 A ground station may send further DLCP packets as soon as it has responded to the DLS.

Note.— The User Data parameter permits the DLS to contain an uncompressed ISH PDU.

5.7.8.4.4.2.1.14 If an aircraft receives a DLS with a lower sequence number from the ground station than the last DLS it sent, then it shall ignore that DLS.

5.7.8.4.4.2.1.15 The aircraft shall not discard any channel assignments it made itself.

5.7.8.4.4.2.1.16 If an aircraft receives a DLE in response to its DLS then the Data Link Initialisation procedure shall be terminated and a failure indication returned to the initiating user.

5.7.8.4.4.2.1.17 The following parameters shall be included in the DLS:

Parameter	**Included by**		**Purpose**
	Aircraft	**Ground Station**	
Data Link Capabilities	M	M	To declare the implemented capabilities.
Compression Algorithm Identifier	O	O	To identify the data compression algorithms.
Deflate Compression Window	O	O	To identify the largest backwards reference that will be made by the sender's Deflate compressor.
Highest Channel Number	O	O	To identify the highest channel number that the sender can use.
Previous Ground Endpoint ID	O	-	When present, to identify a ground station from which the current compression state may be recovered.
Deflate Compression State Information	O	-	When present, to identify the current stream position of the aircraft's identified Deflate decompressor.

Parameter	Included by Aircraft	Included by Ground Station	Purpose
Ground Endpoint ID	-	M	To identify uniquely the ground station as a data link endpoint.
Compression State Restored	-	O	When present, to indicate that the compression state was recovered from the identified ground station.
Uncompressed Channels Restored	-	O	When present, to indicate that all uncompressed channels have been restored.
User Data	O	O	To exchange a user data packet, e.g. an ISH PDU, on the DLS.

Note.— When LREF is used to compress CLNP PDUs, the user parameters specified in 5.7.8.2.4.1.2 may also be present in the DLS.

5.7.8.4.4.2.1.18 On completion of the exchange of DLS packets:

a) Only those capabilities in common between aircraft and ground station shall be used on the Data Link;

b) The highest channel number available for allocation shall be the lower of the Highest Channel Numbers supported by aircraft and ground station.

Note.— Initialisation of the Deflate Compressor/Decompressor is specified in 5.7.8.4.3.6.1.

5.7.8.4.4.2.1.19 If a user data parameter is present in an incoming DLS, the user packet contained within it shall be passed to the service user.

5.7.8.4.4.2.1.20 Negotiation of Data Link Capabilities

5.7.8.4.4.2.1.20.1 An aircraft shall identify its supported data link capabilities by including a Data Link Capabilities parameter in its DLS and setting the appropriate bits.

5.7.8.4.4.2.1.20.2 A ground station shall inspect the Data Link Capabilities parameter in a received DLS and determine the common set of availability data link capabilities.

5.7.8.4.4.2.1.20.3 The ground station shall return this common set in its DLS response by including a Data Link Capabilities parameter and setting the bits that correspond to the common set of capabilities.

5.7.8.4.4.2.1.20.4 Any unrecognised Data Link Capabilities shall be ignored by the ground station.

5.7.8.4.4.2.1.21 Negotiation of Compression Algorithms

5.7.8.4.4.2.1.21.1 An aircraft shall identify the compression algorithms and versions it supports by including a "Compression Algorithm identifier" parameter for each such algorithm in its DLS.

5.7.8.4.4.2.1.21.2 Each such parameter shall identify the algorithm and version supported.

5.7.8.4.4.2.1.21.3 A ground station shall determine the common set of supported compression algorithms and versions by comparing the list of compression algorithms given in the aircraft's DLS with those compression algorithms it supports.

5.7.8.4.4.2.1.21.4 The ground station shall list this common set in its DLS response by including a Compression Algorithm Identifier parameter for each such algorithm identifying both algorithm and version supported.

5.7.8.4.4.2.1.21.5 When the ground station supports an earlier version to that supported by the aircraft, then this earlier version shall be that included in the common set of supported algorithms.

5.7.8.4.4.2.1.21.6 Any unknown Compression Algorithms shall be ignored by the ground station.

Note.— Version numbers are intended to be used incrementally and if a given version is supported then all earlier versions are also supported. The ground station may therefore respond with an earlier version number if the version proposed is not supported. It is implicitly assumed that the aircraft will support this earlier version.

5.7.8.4.4.2.1.22 Restoring the Compression State

Note.— The procedures for restoring the Deflate Compression State are specified in 5.7.8.4.3.6.2.6.

5.7.8.4.4.2.1.22.1 If the aircraft's A/GCS instance has retained compression state information from a previous data link connection, it shall include:

a) The Previous Ground Endpoint ID parameter in its DLS. This shall contain the Ground Endpoint Identifier that had been uplinked in the DLS from the ground station with which the previous data link connection had been established;

b) Optionally, the Deflate Compression State Information parameter for each Deflate compressor. This shall contain the algorithm id for the compressor followed by the current position of the ground-to-air data stream compressed by Deflate.

5.7.8.4.4.2.1.22.2 If supported by the ground station, the ground station shall use a "Previous Ground Endpoint ID" parameter in the aircraft's DLS to contact the identified ground station and to obtain from it:

a) The compression state for each compression algorithm supported by both ground station and aircraft, and

b) The current channel assignments, including those of channels not associated with any compressor.

5.7.8.4.4.2.1.22.3 If the compression state is successfully obtained, then ground station shall restore the current channel assignments including those channels not associated with any compressor and set its own A/GCS compression/decompression functions to the obtained state.

5.7.8.4.4.2.1.22.4 The ground station shall include a "Compression State Restored" parameter in the returned DLS for each compression algorithm restored, indicating the stream position for which compression was restored.

Note 1.— The compression state may include Deflate compression state information and state information from any other A/GCS compression algorithm. it also includes the current channel allocations for each compression algorithm, which are implicitly restored. This is because compression algorithms are linked to channels.

Note 2.—LREF state is restored separately (see section 5.7.8.2.4.1.3). However, LREF compression cannot be restored unless the channel assigned to LREF is also restored.

Note 3.— It is possible to restore the channel assignments only by including a Compression State Restored parameter restoring the stream to the initial state.

5.7.8.4.4.2.1.22.5 The ground station shall include an "Uncompressed Channels Restored" parameter in the returned DLS if it is able to restore channel assignments for channels not associated with any compressor.

Note 1.— Channel zero is always available and there is no need to include this parameter if there is no uncompressed channel other than channel zero .

Note 2.— It is possible to restore the uncompressed channel assignments only.

5.7.8.4.4.2.1.22.6 When an aircraft receives a DLS response that includes a "Compression State Restored" parameter it shall restore the indicated compression functions and channels to their state when the data link with the previous ground station was terminated.

Note.— If the ground station is the same as the previous ground station – which is very likely when a single ground station is connected to several ground stations in a given geographical error, then restoring the compression state should be trivial (i.e. the information is available locally). When the ground station is remote then a communications protocol will be needed to recover the compression state. This could, for example be the Hypertext Transfer Protocol (http) with the Ground Endpoint ID and aircraft address used to construct a conventional URL from where the required compression state will be found.

5.7.8.4.4.2.1.23 Data Link Initiation Refusal

5.7.8.4.4.2.1.23.1 A ground station that is unable to accept a Data Link Initiation request from an Aircraft shall respond to the DLS packet with a DLE packet with an appropriate diagnostic code.

Note.— If a transient problem is signalled then it is a local matter as to whether a further attempt is made to establish a data link after some back off period or whether an alternative ground station is contacted, if available.

5.7.8.4.4.2.2 Data Link Restart

5.7.8.4.4.2.2.1 The Data Link Restart procedures shall be performed in order to recover from a serious protocol error as specified by this specification.

5.7.8.4.4.2.2.2 The Data Link Restart procedure may be initiated by either the aircraft or the ground station.

5.7.8.4.4.2.2.3 To initiate a Data Link Restart, the initiator shall send a DLR packet. The packet's sequence number shall be the next sequence number in the series.

5.7.8.4.4.2.2.4 When a system receives a DLR packet which is not in response to a Data Link Restart that it initiated itself, the system shall deallocate all allocated channels and re-initialise all compression functions.

5.7.8.4.4.2.2.5 It shall respond with a DLR packet acknowledging the restart.

Note.— The AK Sequence number parameter is used to indicate that this is a response and to which DLR it is a response.

5.7.8.4.4.2.2.6 Once a system has initiated a Data Link Restart, it shall ignore and discard all received packets on all channels except for another DLR.

5.7.8.4.4.2.2.7 When it receives a DLR acknowledging its own Data Link Restart, the system shall deallocate all allocated channels and re-initialise all compression functions.

Note.— Exceptionally Data Link Restart procedures may be initiated by both systems simultaneously. 5.7.8.4.4.2.2.4 above applies even when a system is waiting for a response to its own DLR.

5.7.8.4.4.2.2.8 A timer t_1 shall be started whenever a DLR is sent, and reset when the DLR is acknowledged.

5.7.8.4.4.2.2.9 If timer t_1 expires before the DLR is acknowledged then the DLR shall be sent again and timer t_1 restarted. On retransmission, the sequence number shall be the next sequence number in the series.

5.7.8.4.4.2.2.10 Each time timer t_1 is restarted the timer duration shall be increased by 50%.

Note.— The purpose of this procedure is to ensure that a timer set to an unrealistically short interval does not prevent communication.

5.7.8.4.4.2.2.11 The procedures for negotiation of data link capabilities and compression algorithm negotiation shall be as specified for Data Link Initiation.

Note 1.— There is no mechanism for restoring the compression state or channel assignments on a Data Link Restart.

Note 2.— There is no change to shared session key on a Data Link Restart.

5.7.8.4.4.2.2.12 The following parameters shall be included in the DLR for a Data Link Restart:

Parameter	**Included by**		**Purpose**
	Aircraft	**Ground Station**	
Data Link Capabilities	M	M	To declare the implemented capabilities.
Compression Algorithm Identifier	O	O	To identify the supported data compression algorithms.
Deflate Compression Window	O	O	To identify the largest backwards reference that will be made by the sender's Deflate compressor.
Highest Channel Number	O	O	To identify the highest channel number that the sender can use.
AK Sequence Number	M	M	To acknowledge the received DLR. Required on a response only.
Diagnostic	M	M	To indicate the reason for the restart.

5.7.8.4.4.2.2.13 On completion of the exchange of DLR packets for a Data Link Restart:

a) Only those capabilities in common between aircraft and ground station shall be used on the data link;

b) The highest channel number available for allocation shall be the lower of the Highest Channel Numbers supported by aircraft and ground station.

Note.— The data link is now in its initial state except for any shared session key which remains unchanged.

5.7.8.4.4.2.2.14 If a DLR is received apparently in response to a DLR that had been sent previously but which is unexpected, then the Data Link Restart procedures shall be invoked to restore the data link to a defined state.

5.7.8.4.4.2.3 Data Link Termination

5.7.8.4.4.2.3.1 The data link shall be implicitly terminated either:

a) when the underlying data link reports loss of communications, or

b) when a DLS packet is received. The DLS packet shall be processed as specified in 5.7.8.4.4.2.1.

5.7.8.4.4.2.3.2 The data link shall be explicitly terminated by either airborne or ground station sending a DLE packet.

5.7.8.4.4.2.3.3 Once a DLE packet has been sent, any further packet received from the peer system shall be silently discarded and the DLE re-sent.

5.7.8.4.4.2.3.4 On receipt of a DLE packet a system shall regard the data link as being terminated.

5.7.8.4.4.2.3.5 Once a data link has been terminated no further data transfers shall be initiated.

5.7.8.4.4.2.3.6 However, channel allocation and compression state shall be retained for possible use on the next data link connection.

Note.— The implicit termination of a data link when a DLS is received is compatible with the retransmission of a DLS (see 5.7.8.4.4.2.1).

5.7.8.4.4.2.4 Channel Allocation

5.7.8.4.4.2.4.1 The CS packet shall be used to assign the purpose and use of a logical channel, as indicated by the packet's parameters.

5.7.8.4.4.2.4.2 A Data Format parameter shall always be present in the CS packet and shall indicate the type of data for which the channel is assigned.

5.7.8.4.4.2.4.3 A Compression Algorithm Identifier shall be present when the channel is to be associated with a compression algorithm.

5.7.8.4.4.2.4.4 The Compression Algorithm Identifier shall be used to identify the compressor and decompressor with which the channel is associated.

5.7.8.4.4.2.4.5 If a CS packet is received for a channel that is already assigned and:

a) the assignment had been previously made by the sender of the CS packet, then the CS packet shall re-assign the channel to the new purpose and use;

b) the assignment had been previously made by the receiver of the CS packet, then the CS packet is in error and a Channel Reset shall be sent in response.

Note.— If the channel assignment or re-assignment is accepted then no response is expected.

5.7.8.4.4.2.4.6 The sender of the CS packet shall be the channel initiator and the receiver shall be the channel responder.

5.7.8.4.4.2.4.7 When choosing a logical channel to assign, an aircraft shall choose the highest numbered logical channel available for assignment while a ground station shall choose the lowest numbered logical channel available.

5.7.8.4.4.2.4.8 If no channel is available, a lesser importance channel shall be selected out of those previously assigned by the sender of the CS packet, and re-assigned to the new purpose and use.

5.7.8.4.4.2.4.9 If no such channel is available, the request for a new channel assignment shall fail and the service user notified.

Note.— It is a local matter as to what constitutes "lesser importance".

5.7.8.4.4.2.4.10 In order to prevent channel assignment race conditions, there shall be at least one channel that remains unassigned at all times.

5.7.8.4.4.2.4.11 A single compression algorithm may be specified for the channel out of those in common between initiator and responder.

5.7.8.4.4.2.4.12 If a CS packet is received attempting to assign a channel number greater than that which the receiving system declared as the "highest channel number" in its DLS or DLR packet, then the channel assignment shall be rejected by returning a Channel Reset, with an appropriate diagnostic code.

5.7.8.4.4.2.4.13 An unknown parameter code or the use of an unrecognised data format shall be rejected as an error and a Channel Reset packet returned in order to report the error, with an appropriate diagnostic code. The channel shall return to the unassigned state.

5.7.8.4.4.2.5 Channel Deallocation

5.7.8.4.4.2.5.1 The Channel End (CE) packet is sent in order to return a channel to the unassigned state. It shall be sent only by the channel initiator.

5.7.8.4.4.2.5.2 Receipt of a CE by the channel initiator shall be regarded as a protocol error and the DLR procedure shall be used to re-initialise the data link.

5.7.8.4.4.2.5.3 A CE received for an unassigned channel shall be silently ignored.

5.7.8.4.4.2.6 Link Reset Procedures

5.7.8.4.4.2.6.1 The Link Reset procedures shall be used by a data compression function that operates on data from one or more channels, in order to recover from errors in the compression procedure that affect those channels.

Note 1.—Either system may perform a link reset.

Note 2.—The only data compression procedure currently specified to use this procedure is Deflate.

5.7.8.4.4.2.6.2 Forward Link Reset Procedure

5.7.8.4.4.2.6.2.1 The Forward Link Reset Procedure shall be used to announce that the compressed data stream from the initiator of the procedure to the receiver is being reset to its initial state.

5.7.8.4.4.2.6.2.2 To invoke the Forward Link Reset Procedure, the initiator shall send a Link Reset packet to the receiver.

5.7.8.4.4.2.6.2.3 The Compression Algorithm Identifier parameter shall be present and identifies the affected data compression algorithm and hence the affected data stream and channels.

5.7.8.4.4.2.6.2.4 The Diagnostic parameter shall be present and indicates the reason for the Link Reset.

5.7.8.4.4.2.6.2.5 When a Forward Link Reset is sent, the affected data stream compressor is re-initialised.

5.7.8.4.4.2.6.2.6 When a Forward Link Reset is received, the affected data stream decompressor is re-initialised.

Note.—No acknowledgement of receipt is required.

5.7.8.4.4.2.6.3 Reverse Link Reset Procedure

5.7.8.4.4.2.6.3.1 To initiate a Reverse Link Reset, the initiator shall send an LR packet containing the following parameters:

Compressed Data Stream Resync	To identify the affected compression algorithm and by implication the affected channels, and to indicate the postion in the data stream to which a reset may take place.
Diagnostic Reason	To identify the reason for the link reset.

5.7.8.4.4.2.6.3.2 Additional optional parameters may be specified for the specific compression algorithm.

5.7.8.4.4.2.6.3.3 When a Data Link Reset is received, the identified data compression function shall be alerted, and a Link Reset message returned acknowledging the Link Reset.

5.7.8.4.4.2.6.3.4 This shall include the following parameters:

Compressed Data Stream Resync	To identify the affected compression algorithm and by implication the affected channels, and to indicate the postion in the data stream to which a reset may take place.
AK Sequence Number	To indicate the sequence number of the LR packet that initated the link reset.

5.7.8.4.4.2.6.3.5 Additional optional parameters may be specified for the specific compression algorithm.

5.7.8.4.4.2.6.3.6 When such a Data Link Reset Response is received the identified data compression function shall be re-synchronised to the indicated stream position.

Note.—The procedures carried out by the data compression function in response to a Data Link Reset are specific to that function.

5.7.8.4.4.2.6.3.7 A timer t_1 shall be started whenever an LR is sent to initiate a link reset, and reset when the LR is acknowledged.

5.7.8.4.4.2.6.3.8 If timer t_1 expires before the LR is acknowledged, then the LR shall be sent again and timer t_1 restarted.

Note.—The sequence number is incremented for each retransmission.

5.7.8.4.4.2.6.3.9 Each time timer t_1 is restarted the timer duration shall be increased by 50%.

Note.—The purpose of this procedure is to ensure that a timer set to an unrealistically short interval does not result in a communications failure.

5.7.8.4.4.2.6.3.10 If a Forward Link Reset is received for the same compression algorithm while awaiting a response to a Reverse Link Reset, the Reverse Link Reset procedures shall be abandoned and the Forward Link Reset processed as described in5.7.8.4.4.2.6.2.

5.7.8.4.4.3 DLCP Packet Formats

Note.—The DLCP procedures are specified in 5.7.8.4.4.2. Only the packet formats are specified here.

5.7.8.4.4.3.1 Data Link Start (DLS)

Identifier (ID) 1

5.7.8.4.4.3.1.1 The DLS packet shall be sent to initialise a data link.

5.7.8.4.4.3.1.2 The following optional parameters are specified for the DLS packet:

1) Data Link Capabilities;
2) Compression Algorithm Identifier;
3) Deflate Compression Window;
4) Highest Channel Number;
5) Previous Ground Endpoint ID;
6) Ground Endpoint ID;
7) Compression State Restored;
8) Deflate Compression State Information;
9) Security Algorithm ID;
10) Random Value;
11) Public Key;
12) Public Key Certificate;
13) User Data.

5.7.8.4.4.3.1.3 The parameter codes for these parameters shall be as specified for each parameter.

5.7.8.4.4.3.1.4 On receipt an unrecognised parameter shall be silently ignored.

5.7.8.4.4.3.2 Data Link Restart (DLR)

Identifier (ID) 10

5.7.8.4.4.3.2.1 The DLR packet shall be sent to restart a data link after an error has occurred.

5.7.8.4.4.3.2.2 The following optional parameters are specified for the DLR packet:

1) Data Link Capabilities;
2) AK Sequence Number;
3) Compression Algorithm Identifier;
4) Deflate Compression Window;
5) Highest Channel Number;
6) Previous Ground Endpoint ID;
7) Ground Endpoint ID;
8) Diagnostic (to indicate the restart reason).

5.7.8.4.4.3.2.3 The parameter codes for these parameters shall be as specified for each parameter.

5.7.8.4.4.3.2.4 On receipt an unrecognised parameter shall be silently ignored.

5.7.8.4.4.3.3 Data Link End (DLE)

Identifier (ID) 11

5.7.8.4.4.3.3.1 The DLE packet shall be sent to terminate or reject the initiation of a data link.

5.7.8.4.4.3.3.2 The following optional parameters are specified for the DLE packet:

1) Diagnostic.

5.7.8.4.4.3.3.3 The parameter codes for these parameters shall be as specified for each parameter.

5.7.8.4.4.3.3.4 On receipt, an unrecognised parameter shall be silently ignored.

5.7.8.4.4.3.4 Channel Start (CS)

Note.— The purpose of the CS packet is to assign the use of a previously unassigned channel and to define its operational parameters.

Identifier (ID) 1000

5.7.8.4.4.3.4.1 The CS packet header shall include the logical channel number to which the CS applies.

5.7.8.4.4.3.4.2 The following parameters are specified for the CS packet:

1) Compression Algorithm Identifier (optional);
2) Data Format.

5.7.8.4.4.3.4.3 The parameter codes for these parameters shall be as specified for each parameter.

5.7.8.4.4.3.4.4 On receipt an unrecognised parameter shall be rejected as a protocol error.

5.7.8.4.4.3.5 Channel End (CE)

Note.— The purpose of the CE packet is to restore a channel to the unassigned state.

Identifier (ID) 1001

5.7.8.4.4.3.5.1 The CE packet header shall include the logical channel number to which the CE applies.

5.7.8.4.4.3.6 Channel Reset (CR)

Note.— The purpose of the CR packet is to signal a problem in channel assignment or use, and to restore the channel to a defined state.

Identifier (ID) 1010

5.7.8.4.4.3.6.1 The CR packet header shall include the logical channel number to which the CR applies.

5.7.8.4.4.3.6.2 The parameter codes for these parameters shall be as specified for each parameter.

5.7.8.4.4.3.6.3 On receipt an unrecognised parameter shall be rejected as a protocol error.

5.7.8.4.4.3.6.4 The CR packet shall be sent only:

a) when required by this specification in order to signal a problem with a channel assignment, or

b) on the request of the service user in order to report a problem in the data sent over the channel.

5.7.8.4.4.3.6.5 When a CR packet has been sent on the request of the service user:

a) The Diagnostic parameter shall indicate "User Problem";

b) The User Diagnostic parameter shall be present and set to a value specified by the service user.

5.7.8.4.4.3.6.6 The following optional parameters are specified for the CR packet:

1) Diagnostic;
2) User Diagnostic;
3) AK Sequence Number.

5.7.8.4.4.3.6.7 If no User Diagnostic parameter is present then a Channel Reset results in the channel becoming unassigned.

5.7.8.4.4.3.6.8 If a User Diagnostic parameter is present then a timer t_1 shall be started by the sender.

5.7.8.4.4.3.6.9 All user data received on the same channel shall be discarded until a Channel Reset is returned by the peer system acknowledging receipt of the Channel Reset by including an AK Sequence number parameter containing the sequence number of the original Channel Reset.

5.7.8.4.4.3.6.10 If timer t_1 expires before such a Channel Reset is received, the Channel Reset shall be sent again, and timer t_1 restarted.

Note.— The DLCP protocol requires that the sequence number is incremented for each retransmission.

5.7.8.4.4.3.6.11 Each time timer t_1 is restarted the timer duration shall be increased by 50%.

Note.—The purpose of this procedure is to ensure that a timer set to an unrealistically short interval does not result in communications failure.

5.7.8.4.4.3.6.12 When a Channel Reset is received from a peer system with a User Diagnostic parameters but without an AK Sequence Number parameter, the Channel Reset and Diagnostic shall be reported to the service user and a Channel Reset returned in response.

5.7.8.4.4.3.6.13 This shall include the AK Sequence Number parameter containing the sequence number of the received Channel Reset.

5.7.8.4.4.3.6.14 No other parameters shall be included.

5.7.8.4.4.3.6.15 When a Channel Reset is received from a peer system an AK Sequence Number parameter that is not in acknowledgement of the last sent Channel Reset, the Channel Reset shall be ignored.

5.7.8.4.4.3.7 Link Reset (LR)

Note 1.— The purpose of the LR packet is to re-initialise a compressed data stream or to restart it at an identified point.

Note 2.— A Link Reset affects all channels using the affected compressed data stream.

Identifier (ID) 111

5.7.8.4.4.3.7.1 The Link Reset packet shall be sent when an error is detected in a received Deflate compressed data stream, in order to return the data stream to a defined state.

5.7.8.4.4.3.7.2 The following optional parameters are specified for the Link Reset packet:

1) Compressed Data Stream Resync;
2) Compression Algorithm ID;
3) Diagnostic;
4) AK Sequence Number.

5.7.8.4.4.3.7.3 The parameter codes for these parameters shall be as specified for each parameter.

5.7.8.4.4.3.7.4 On receipt, an unrecognised parameter shall be rejected as a protocol error.

5.7.8.4.4.4 DLCP Optional Parameters

5.7.8.4.4.4.1 Data Link Capabilities Parameter

Parameter Code	0000 0001
Parameter Length	variable
Parameter Value	see below

5.7.8.4.4.4.1.1 The parameter shall be interpreted as a variable length bitmap indicating support of data link capabilities specified in this and subsequent standards.

Note.—An important purpose of this parameter is to provide for the introduction of new capabilities in a backwards compatible manner. Therefore this specification requires implementations to ignore capabilities that they do not understand and to handle longer length parameters than they would otherwise expect.

5.7.8.4.4.4.1.2 For the purposes of this specification, the bits in the bitmap shall be numbered b_0 through to b_n where b_0 is the least significant bit in the bitmap and b_n is the most significant bit.

5.7.8.4.4.4.1.3 The sender shall send the minimum number of octets in order to transmit all non-zero bits in the bitmap.

5.7.8.4.4.4.1.4 A receiver shall be able to accept any length bitmap up to the maximum length permitted by the encoding rules.

5.7.8.4.4.4.1.5 The Data Link Capabilities parameter shall be interpreted as follows:

Bit No.	Capability
0	ISO TR 9577 Format Data
1	LREF Data Format
2	Reformatted CLNP Headers
3	IPv4

5.7.8.4.4.4.1.6 The sender shall set the corresponding bit to one in order to claim support of the associated capability.

5.7.8.4.4.4.1.7 The data link capabilities that are used for communication between the sender and receiver shall be those in common between those declared in the sender's DLR and those declared in the DLR sent back in response.

5.7.8.4.4.4.1.8 Any unrecognised bits in the capabilities bitmap shall be ignored.

Note.—LREF Data Compression is listed here as a capability for efficiency reasons. Formally, it is a capability of the service user.

5.7.8.4.4.4.2 Compression Algorithm Identifier

Parameter Code	0000 0010
Parameter Length	0, 2 or 3 octets
Parameter Value	Algorithm ID and version

Note 1.— The purpose of the Compression Algorithm Identifier is to identify a Compression Algorithm supported by the sender of the DLS or DLR, and the version supported.

Note 2.—Currently Deflate is the only compression algorithm that will be identified. However, it is intended that each Deflate dictionary supported is identified by a unique Algorithm ID.

5.7.8.4.4.4.2.1 The parameter value shall be either:

a) an unsigned 16-bit unsigned binary number that is a unique identifier for a compression algorithm. Compression Algorithm identifiers shall be globally known and the registry of Compression Algorithm identifiers shall be maintained by ICAO, or

b) a Compression Algorithm identifier as defined above followed by an 8-bit unsigned binary number that is the version number of the algorithm.

5.7.8.4.4.4.2.2 If no version number is present then version zero shall be assumed for a DLS or DLR.

5.7.8.4.4.4.2.3 Otherwise, the negotiated version, as agreed on data link initialisation or restart, shall be assumed.

5.7.8.4.4.4.2.4 This parameter may occur more than once in a DLS or DLR and is repeated for each compression algorithm supported.

5.7.8.4.4.4.2.5 A compression algorithm ID of zero is defined by this specification to identify the Deflate stream compression algorithm with no initialisation dictionary.

5.7.8.4.4.4.2.6 If the parameter length is zero and no parameter value is present then this shall equate to a parameter value of zero.

Note.—Version number are allocated incrementally and support for a given version number implies support for all earlier versions. For example, support for version 2 implies that versions 1 and 0 are also supported.

5.7.8.4.4.4.3 Deflate Compression Window

Parameter Code	0000 0011
Parameter Length	1 octet
Parameter Value	An unsigned binary number in the range 10 to 15

Note.—The purpose of this parameter is to declare the largest backwards reference that will be made in the Sender's a Deflate compressed data steam. The receiver can use this information to reduce the size of the decompression buffer.

5.7.8.4.4.4.3.1 This parameter shall be included in a DLR in order to signal the largest backwards reference that will be made in the Sender's a Deflate compressed data steam.

5.7.8.4.4.4.3.2 The parameter value shall be a number n in the range 10 to 15.

5.7.8.4.4.4.3.3 The largest backwards reference shall be calculated as 2^n-1.

5.7.8.4.4.4.3.4 If the parameter is omitted, then a value of n shall default to 15.

Note.— There is no requirement for the Default Compression Window to be the same in both directions.

5.7.8.4.4.4.4 Highest Channel Number

Parameter Code	0000 0100
Parameter Length	2 octets
Parameter Value	Highest assignable Channel Number

Note.—The purpose of this parameter is to indicate the maximum number of channels supported by the sender. The actual number of channels available will be the lower of the maximum supported by both sides.

5.7.8.4.4.4.4.1 This parameter shall be included in a DLR to indicate the highest assignable channel number.

5.7.8.4.4.4.4.2 The sending system will not attempt to assign a channel number greater than the parameter value, nor will it accept a channel number greater than the parameter value.

5.7.8.4.4.4.4.3 If this parameter is not included then the highest assignable channel number shall default to 15.

5.7.8.4.4.4.5 Ground Endpoint ID

Parameter Code	0000 0101
Parameter Length	variable
Parameter Value	Ground Endpoint Identifier

Note.—The purpose of the parameter is to enable the ground station to provide the aircraft with some unique identifier that can be used on a subsequent data link to restore the compression state.

5.7.8.4.4.4.5.1 The Ground Endpoint ID parameter shall be included in every DLS sent to an aircraft.

5.7.8.4.4.4.5.2 The Ground Endpoint ID parameter shall provide a unique identifier for the ground station.

Note.—An example of a unique identifier is the NET of the ATN Router.

5.7.8.4.4.4.6 Previous Ground Endpoint ID

Parameter Code	0000 0110
Parameter Length	variable
Parameter Value	Previous Ground Endpoint Identifier

Note.—The purpose of this parameter is to identify the previous ground station on the same type of Air/Ground Subnetwork which the aircraft used for data communications using the procedures specified by this SNDCF. It is used as a hint to the receiver that it may be possible to transfer the compression state from the previous connection to the new one.

5.7.8.4.4.4.6.1 The Previous Ground Endpoint ID shall only be included in the DLS sent by an aircraft to initialise a new data link.

5.7.8.4.4.4.6.2 It shall not be sent by a ground station when performing a Data Link Restart.

5.7.8.4.4.4.7 Compression State Restored

Parameter Code	0000 0111
Parameter Length	2, 6 or 10 octets
Parameter Value	Compression Algorithm ID followed by stream position

Note 1.—This parameter is included by a ground station in order to indicate to an aircraft that it has been able to recover the compression state for the indicated Compression Algorithm. All channel assignments are restored; the compressors and decompressors are in the same state as at when the data link was closed.

Note 2.—It occurs once for each data compression algorithm restored.

Note 3.—This parameter is not used to signal restoration of the LREF Directory. This is formally a service user function and is signalled via a parameter code reserved for user parameters.

Note 4.—There is no need to signal the compression algorithm version as it is not possible to change algorithm versions on handoff. The same version is maintained implicitly.

5.7.8.4.4.4.7.1 The Compression State Restored parameter shall only be included in a DLS sent by a ground station to an aircraft, and to indicate that the compression state has been recovered from the ground station attached to the previous ground station, and for the specified compression algorithm.

5.7.8.4.4.4.7.2 The parameter value shall comprise three fields:

1) A 16-bit compression algorithm identifier;

2) Optionally, the data stream position in the air-to-ground direction;

3) Optionally, the data stream position in the ground-to-air direction.

Note.—This encoding implies that a ground-to-air stream position can only be indicated when an air-to-ground stream position is also indicated.

5.7.8.4.4.4.7.3 In each case, the stream position expressed as a 32-bit unsigned binary number which wraps around to zero on overflow.

5.7.8.4.4.4.7.4 The presence of a given compression algorithm identifier shall indicate that all channels that use that algorithm for data compression have been restored.

5.7.8.4.4.4.7.5 The stream position parameter for the air-to-ground direction shall indicate the data stream position of the last octet of the last packet received on a channel that uses the specified algorithm.

5.7.8.4.4.4.7.6 The stream position parameter for the ground-to-air direction shall indicate the data stream position of the last octet of the last packet sent on a channel that uses the specified algorithm.

5.7.8.4.4.4.7.7 If either or both stream positions are not present, then this shall indicated that the compression state for that data stream has not been restored and that the compressed data stream in that direction has been re-initialised.

Note 1.—Due to wrap around, stream position zero does not indicate re-initialisation.

Note 2.—It is not possible to re-initialise the ground-to-air direction only.

5.7.8.4.4.4.8 Diagnostic

Parameter Code	0000 1000
Parameter Length	1 octet
Parameter Value	Diagnostic Code

Note.—The purpose of this parameter is to convey the reason for a data link restart, or a problem with a channel assignment or use.

5.7.8.4.4.4.8.1 The diagnostic parameter shall convey the reason for the restart, link reset or other problem using one of the reason codes given in Table 5.7-14.

5.7.8.4.4.4.8.2 An invalid reason code shall be ignored on receipt.

Table 5.7-14 Diagnostic Codes

Restart Reason Code	Interpretation
0000 0010	Channel Start Error

0000 0011	Highest channel number exceeded
0000 0100	Unknown parameter code
0000 0101	Unknown compression algorithm requested
0000 0110	Unknown data format requested
0000 0111	Channel not in use
0000 1000	User Reset
0000 1001	Security sequence number overflow
0000 1010	Protocol error
0000 1011	Cannot restore compression state
0000 1100	Deflate stream resync position error
0000 1101	Checksum error
0000 1110	Data link initiation rejected - Permanent problem
0000 1111	Unknown DLC PDU received
0001 0000	User request
0001 0001	Data link initiation rejected - Transient problem

5.7.8.4.4.4.9 AK Sequence Number

Parameter Code	0000 1001
Parameter Length	2 octets
Parameter Value	Sequence Number

5.7.8.4.4.4.9.1 The parameter value AK Sequence number shall identify the sequence number of the DLCP packet that is being acknowledged.

5.7.8.4.4.4.10 Data Format

Parameter Code	0000 1010
Parameter Length	1 octet
Parameter Value	Data Format Identifier

5.7.8.4.4.4.10.1 The Data Format identifier shall be used to indicate the format of the data sent on the channel.

5.7.8.4.4.4.10.2 The parameter value shall be an unsigned 8-bit number interpreted as specified in Table 5.7-15.

Table 5.7-15 Data Format Identifiers

Data Format Identifier	Data Format
0000 0001	Data packets whose type and function can be determined according to ISO TR 9577. *Note.— This includes ISO/IEC 9542 (ES-IS) and ISO/IEC 8473 (CLNP) packets.*
0000 0010	LREF encoded data
0000 0011	Refomatted CLNP
0000 0100	IPv4

5.7.8.4.4.4.10.3 In the absence of this parameter, data format 0000 0001 shall be assumed as the default.

5.7.8.4.4.4.11 User Diagnostic

Parameter Code	0000 1011
Parameter Length	1 octet
Parameter Value	Diagnostic Code

5.7.8.4.4.4.11.1 The User Diagnostic parameter shall indicate that a problem has been detected in the user data and a Channel Reset has been used to report the problem.

5.7.8.4.4.4.11.2 Action following a user generated channel reset shall depend upon the diagnostic returned.

Note.—The diagnostic codes and the action to be taken are specified by the user of the service and are not part of the DLCP specification. The DLCP simply passes the Channel Reset to the service user. For example, it is used by LREF to reset the LREF compressor.

5.7.8.4.4.4.12 Compressed Data Stream Resync Parameter

Parameter Code	0000 1100

Parameter Length	2 or 6 octets
Parameter Value	Compression Algorithm ID followed by stream position

5.7.8.4.4.4.12.1 This parameter shall comprise two fields:

1) A 16-bit compression algorithm identifier;

2) Optionally, a data stream position parameter expressed as an unsigned 32-bit binary number.

5.7.8.4.4.4.12.2 The Compression Algorithm Identifier shall be used to indicate the data compression algorithm to which the parameter applies.

Note.—The version is the current version as agreed on data link initialisation.

5.7.8.4.4.4.12.3 The data position parameter shall be set to either:

a) (Resync Request) the total number of octets received in the data stream, up to and including the last packet received without error on that data stream, or

b) (Resync Response) the position in the data stream to which the compressor has been reset.

Note.—The purpose of this parameter is to signal to the sender a point in the data stream from which valid backwards references can be made.

5.7.8.4.4.4.12.4 In a resync response, the data stream position may be omitted in which case this shall indicated that the data stream has been reset to the initial state.

Note.—Due to wrap around a data stream position of zero is semantically different from the absence of the parameter value.

5.7.8.4.4.4.13 User Data

Parameter Code	0000 1101
Parameter Length	variable
Parameter Value	User Data

5.7.8.4.4.4.13.1 The contents of this parameter shall comprise user data.

5.7.8.4.4.4.13.2 The user data shall be a ISO TR 9577 format packet.

5.7.8.4.4.4.13.3 On receipt, the contents of the packet shall be provided to the service user as data received in the ISO TR 9577 format.

5.7.8.4.4.4.14 Deflate Compression State Information

Parameter Code	0000 1110
Parameter Length	6 octets
Parameter Value	Compression Algorithm ID followed by stream position

5.7.8.4.4.4.14.1 The contents of this parameter shall comprise:

1) A 16-bit Compression Algorithm Identifier;

2) The data stream position in the ground-to-air direction.

5.7.8.4.4.4.14.2 The data stream position shall be expressed as a 32-bit unsigned binary number which wraps around to zero on overflow.

5.7.8.4.4.4.14.3 This parameter shall be used by an aircraft on Data Link Initiation to indicate the current stream positions for the indicated compression algorithm in order to permit restoration of the Deflate compression state on handoff from a previous ground station.

5.7.8.4.4.4.15 Uncompressed Channels Restored

Parameter Code	0000 1111
Parameter Length	0 octets
Parameter Value	None

5.7.8.4.4.4.15.1 This parameter shall be used by a ground station to indicate to an aircraft that it has been able to restore channel assignments for channels not associated with any data compressor.

5.7.8.4.5 Data Transfer Formats

5.7.8.4.5.1 ISO TR 9577 Format Packets

Note.— This class of packets includes ISO/IEC 9542, 8208 and 8473 PDUs. The primary use is expected to be for ISH PDUs. A packet sent in this data stream can be unambiguously identified from its initial octet. Each frame contains a single such packet.

5.7.8.4.5.1.1 A frame sent on a channel assigned to this data format shall contain a single packet that can be identified from its initial octet according to ISO TR 9577.

5.7.8.4.5.1.2 On receipt, the processing of such a packet shall be a local matter.

5.7.8.4.5.2 LREF Formatted Data

5.7.8.4.5.2.1 Data sent over a channel assigned to LREF formatted data shall be formatted in compliance with the LREF CLNP header compression algorithm (see 5.7.8.2.4.1).

5.7.8.4.5.3 Reformatted CLNP Data

5.7.8.4.5.3.1 Data sent over a channel assigned to the reformatted CLNP packet format shall be formatted as specified in 5.7.8.2.4.2.2.

5.7.8.4.5.4 IPv4 Data Format

5.7.8.4.5.4.1 Data sent over a channel assigned to IPv4 formatted data shall be formatted as an IPv4 packet as specified in IETF RFC 791.

5.7.8.4.6 Compatibility with other Frame Formats

Note.— During transition from older protocols, or to provide for lower cost alternatives for small aircraft, other frame formats may used by aircraft operating over the same data link. The A/GCS is designed to permit this to occur and for use of the A/GCS or an alternative frame format to be determined by inspection of the first octet of the first frame received from the aircraft.

5.7.8.4.6.1 If the first octet of the first frame received from an aircraft by a ground station after a data link has been established is non-zero then:

a) If the value of the octet corresponds with a known initial octet value of an alternative frame format that is valid for the data link and supported by the ground station, then the aircraft shall be deemed as supporting that frame format and the A/GCS procedures shall not be applied. The procedures for that other frame format shall be applied instead;

b) If the value of the octet does not correspond with any known initial octet for an alternative frame format supported by the ground station, then the data link shall be terminated or reset, as appropriate, indicating a protocol error as the reason for the problem.

Note 1.— This is possible because the first downlinked frame must start with a DLCP packet on channel zero.

Note 2.— It is not possible for an alternative frame format to start with an initial zero octet and to be compatible with the A/GCS.

5.7.9 VDL Mode 3 Frame Mode SNDCF

Note 1.—This SNDCF and accompanying CLNP Header compression algorithm is specified for use by small aircraft when a low cost ATS service is required over a frame mode link layer service, i.e. a data link service that provides L-Unitdata.req and L-Unitdata.ind service elements. Only the CLNP header is compressed and there is no support for general data compression or other air/ground communications protocols. It is unlikely to be useful for AOC communications as these get the greatest advantage from DEFLATE compression and security labels encoded with an AOC traffic type cannot be compressed using this algorithm. Its use is thus expected to be only for General Aviation aircraft that require a low costs ATS data link service.

Note 2.— This specification is dependent on the subnetwork providing a means to separately convey a 4-bit compression type parameter for each compressed packet.

Note 3.—For example, in VDL Mode 3 this is performed by including this information in a separate "payload" identifier octet that is inserted as the first octet in the frame.

5.7.9.1 Model of Operations

5.7.9.1.1 The model of operations for an SNDCF incorporating this compression algorithm shall be as shown in Figure 5.7-19.

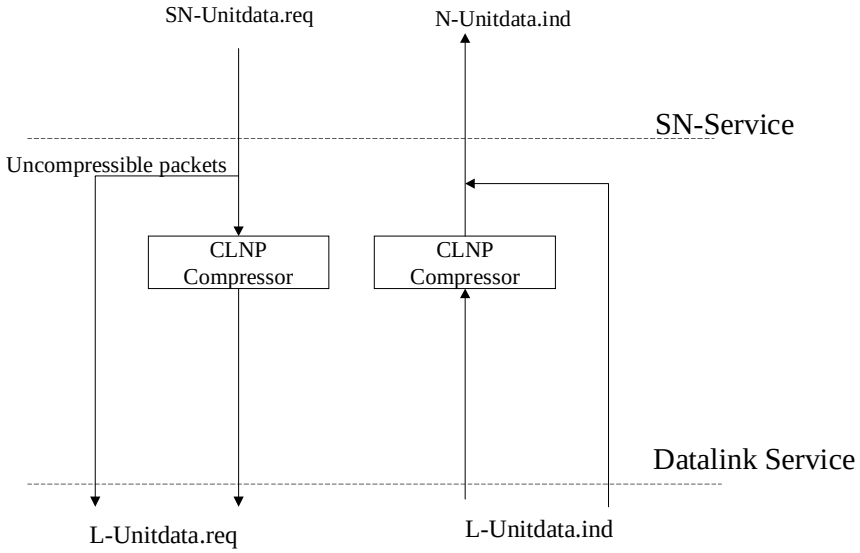


Figure 5.7-19 Model of Operations

5.7.9.1.2 Network Layer PDUs shall be passed to the SNDCF using the SN-Unitdata.req service element.

5.7.9.1.3 Each such PDU shall be inspected to determine if it is a compressible CLNP PDU according to the data compression rules specified in 5.7.9.5.3.

5.7.9.1.4 If so, the PDU shall be passed to the CLNP header compressor. If the PDU is not compressible, then it shall be passed to the data link service, without change and with a data type of TYPE_UNCOMPRESSED_PDU.

Note.— ISH PDUs are always uncompressible.

5.7.9.1.5 CLNP PDUs compressed by the CLNP Header compressor shall be passed to the data link service, and with a data type as indicated by the output of the compressor, and sent using the D-Unitdata.req service.

5.7.9.1.6 When an incoming PDU is received from the data link service:

a) If it has a data type of TYPE_UNCOMPRESSED_PDU, it shall be passed unchanged to the SN Service user by invoking the SN-Unitdata.ind service element;

b) If the incoming PDU has any other data type associated with it, then the PDU shall be passed to the CLNP Header decompressor. The output of the decompressor shall be passed to the SN Service user by invoking the SN-Unitdata.ind service element.

5.7.9.2 Data Type Codes

5.7.9.2.1 The data type codes used by this SNDCF shall be as specified in Table 5.7-16 and are represented as 4-bit unsigned binary numbers.

Note.— These data type codes are used to identify the frame format. In VDL Mode 3, they are included in a payload octet that is prefixed to the frame in each transmission.

Table 5.7-16 Data Type Codes

Code	Semantic
0	TYPE_UNCOMPRESSED_PDU
1	TYPE_RESTART
10	TYPE_UNCOMPRESSED_CLNP
11	TYPE_COMPRESSED_CLNP_LONG_WITH_OPTIONS
100	TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS
101	TYPE_COMPRESSED_CLNP_SHORT
110	TYPE_MULTICAST
111	Reserved

1000 - 1111	Reserved

5.7.9.3 Compressed CLNP Header Format

5.7.9.3.1 The format of the compressed CLNP Header shall be as shown in Figure 5.7-20.

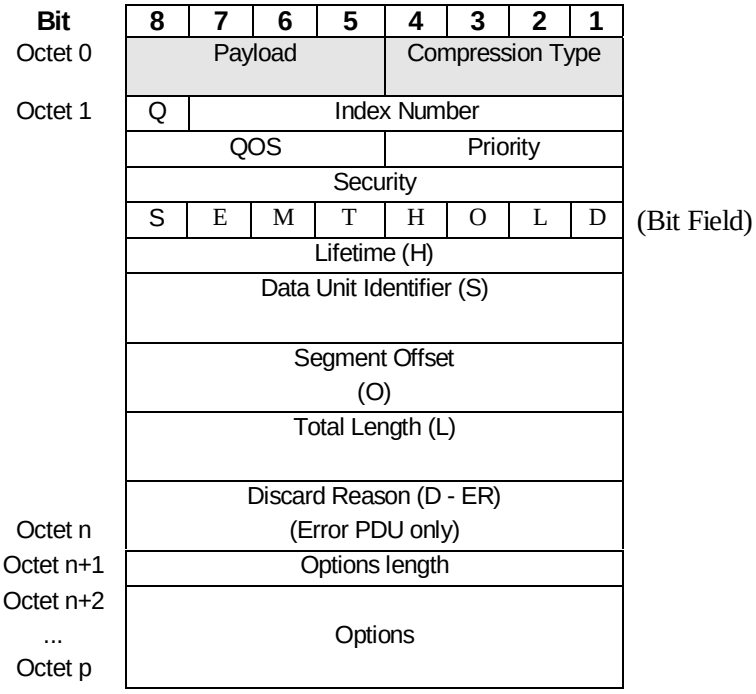


Figure 5.7-20 Compressed CLNP Header Format

Note 1.—Depending on the data type and the value of the S, O, L and D bits, not all indicated fields are present.

Note 2.— The payload field is not formally part of the compressed header and is shown here to illustrate how the data type information is passed when VDL Mode 3 is used as the data link. Other data links using this specification can adopt the same approach but may also define a different scheme to convey the data type information. In VDL Mode 3, the high order 4 bits of the payload field are always set to binary 0001 for data originated by this SNDCF.

5.7.9.3.2 A data type of TYPE_COMPRESSED_CLNP_SHORT or TYPE_MULTICAST shall identify a compressed CLNP Header comprising header fields up to and including the Security field. Such a packet shall contain the Q field, Index Number, QOS, Priority and Security fields. The compressed PDU shall be a compressed CLNP Data PDU.

5.7.9.3.3 A data type of TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS shall identify a compressed CLNP Header comprising header fields as illustrated in Figure 5.7-20 excluding the Options Length and Options fields.

5.7.9.3.3.1 Additionally:

a) If the S-bit is set to a binary 1, then the *DUI* field shall be present;

b) If the O-bit is set to a binary 1, then the *Segment Offset* field shall be present;

c) If the L-bit is set to a binary 1, then the *Total Length* field shall be present;

d) If the H-bit is set to a binary 1, then the *Lifetime* field shall be present;

e) If the value of the D-bit is set to a binary 1, then the *Discard Reason* field shall be present.

5.7.9.3.4 A data type of TYPE_COMPRESSED_CLNP_LONG_WITH_OPTIONS shall identify a CLNP Header comprising the same header fields as for a data type of TYPE_COMPRESSED_ CLNP_LONG_NO_OPTIONS.

5.7.9.3.4.1 Additionally, the compressed CLNP header shall be followed by one or more CLNP options fields copied from the original CLNP header.

5.7.9.3.4.2 The total number of bytes occupied by these options fields shall be given by the value of the Options Length field.

Note.— A data type of TYPE_RESTART implies an empty packet follows and is used as an error recovery mechanism. A data type of TYPE_UNCOMPRESSED_CLNP is used when compression indexes are being defined; the packet has an uncompressed CLNP header.

5.7.9.3.5 The semantics of the compressed CLNP header fields shall be:

a) The single bit Q-field shall indicate the presence of QoS information. If not set (Q=0), no QoS information is present and the value of the QoS field is undefined;

b) The index number shall be indicate the source and destination NSAP Addresses present in the original CLNP Header. The index number shall be in the range 0 to 127 (decimal);

c) The QoS-field shall consist of the CE (bit 8), T/C (bit 7), E/T (bit 6), and E/C (bit 5) bits respectively of the ISO/IEC 8473 QoS Maintenance Parameter;

Note.— The sequencing vs. transit delay (S/T) bit is sent in the T-field (see Figure 5.7-20). This implies that whenever the S/T-bit is set to 1, a long compression format has to be used.

d) The Priority field shall be a 4-bit unsigned binary number representing a priority in the range 0 to 14 decimal. A value of 15 decimal shall imply that no priority has been specified;

Note.— A CLNP PDU with a higher priority than 15 is compressed by including the priority parameter itself in the compressed header.

e) The Security field shall be subdivided into two fields and shall indicate the security parameter of an ATN CLNP packet:

1) The 5 high order bits shall comprise the 5 low order bits of the traffic type security tag of the CLNP security options parameter, and

2) The low order 3 bits shall comprise the 3 low order bits of the security classification tag of the CLNP security options parameter.

A zero value of either or both of the above two fields shall imply that the corresponding security tag is not present in the CLNP Header;

Note.— The traffic type is implicitly ATSC which implies that a CLNP PDU containing any other traffic type (e.g. AOC) is compressed by including the security parameter itself in the compressed header.

f) The bit field comprising the S, E, M, T, H, O, L and D-bits, shall have the following semantics:

Bit	Semantic (Present = 1)
S	SP flag of CLNP Header - Data Unit Identifier present
E	Complement of CLNP ER flag
M	MS-bit of CLNP Header
T	Sequence vs. Transit Delay Bit (from QoS option)
H	Lifetime Field present (Hop Count)
O	Segment Offset present
L	Total Length Field present
D	Type of PDU (Error = 1, Data = 0)

g) The presence of the Lifetime field shall be indicated by the H bit being set to 1. The absence of the Lifetime field shall imply a value for downlink PDUs of decimal 29, and for uplink PDUs, a value of decimal 5;

h) The presence of the Data Unit Identifier field shall be indicated by the S-bit being set to 1. The Data Unit Identifier shall always be present for segmented packets or whenever the SP-bit is set. Absence of this field shall imply that segmentation is not permitted;

i) The presence of the Segment Offset field shall be indicated by the O-bit being set to 1. The Segment Offset shall be sent whenever the SP-bit is set and the Segment Offset is greater than zero. Absence of this field shall imply a value of zero;

j) The presence of the Total Length field shall be indicated by the L bit being set to 1. The Total Length field shall be present the first time a PDU fragment a given DUI is sent only;

Note.— This implies that the value of the field is cached by the receiver by DUI and subsequent fragments with the same DUI are decompressed using the cached total length value.

k) The presence of the Discard Reason field shall be indicated by the D-bit being set to 1. It shall contain the value of the Discard Reason options parameter field;

l) An Options Length field shall contain as its value the number of bytes occupied by the Options field;

m) The value of the Options field shall comprise one or more CLNP options parameters.

5.7.9.4 Data Transmission Procedures

5.7.9.4.1 Determination of whether an NPDU is compressible

5.7.9.4.1.1 An NPDU received as user data of an SN-UnitData.req shall be compressible if and only if:

a) the Network Layer Protocol Identifier is binary 1000 0001 (i.e. it is a CLNP NPDU), and

b) the CLNP version/protocol id extension is set to binary 0000 0001, and

c) the PDU Type is for a Data or Error PDU.

5.7.9.4.1.2 If the NPDU is not compressible, then it shall be passed unchanged to the data link service for transmission, indicating a data type of TYPE_UNCOMPRESSED_PDU.

5.7.9.4.2 Assignment of a Compression Index

5.7.9.4.2.1 The CLNP header compressor shall maintain a local compression directory with up to 128 entries relating an index number in the range 0 to 127, to Source and Destination NSAP Addresses.

5.7.9.4.2.2 ***Recommendation.—****A separate 128 entry directory and index number series should be used for each peer system with which the sending system is in contact.*

5.7.9.4.2.3 When a compressible NPDU has been submitted for transmission, this directory shall be interrogated in order to locate an entry corresponding to the Source and Destination NSAP Addresses of the NPDU.

5.7.9.4.2.4 If such an entry is located, the associated index number shall be retrieved and the procedures specified in 5.7.9.4.3 shall be followed.

5.7.9.4.2.5 Otherwise, an unassigned index number shall be obtained and a local compression directory entry created associating this index number with the NPDU's Source and Destination NSAP Addresses.

5.7.9.4.2.6 The Network Layer Protocol Identifier shall be replaced by the assigned index number encoded as an unsigned 8-bit binary number, and the NPDU passed unchanged to the data link service for transmission, indicating a data type of TYPE_UNCOMPRESSED_CLNP.

5.7.9.4.2.7 If there are no unassigned index numbers available, the NPDU shall be passed otherwise unchanged to the data link service for transmission, indicating a data type of TYPE_UNCOMPRESSED_PDU.

5.7.9.4.3 Creation of the Compressed Header

5.7.9.4.3.1 The CLNP PDU Header including the Network Layer Protocol Identifier shall be removed and replaced with a compressed header in the format illustrated in Figure 5.7-20 applying the following procedures:

a) The Index Number field shall be set to the value of the assigned index number encoded as a 7-bit unsigned binary number;

b) The Q-bit shall be set to 1 if a Globally Unique QoS Maintenance Parameter is present in the original CLNP Header and the QoS field bits and T-bit set according to the value of the Globally Unique QoS Maintenance Parameter and 5.7.9.3. The Q-bit shall be set to 0 otherwise;

c) If a Priority options parameter is present in the original CLNP Header and the priority value is 14 or less then the Priority field shall be set to the low order 4 bits of the Priority options parameter. The Priority field shall be set to zeroes otherwise;

d) If a Security Options parameter is present in the original CLNP Header and the value of the parameter is:

1) an ATN Security Label, and

2) the Traffic Type and Security Classification security tags are the only security tags present, and

3) the Traffic Type is ATSC, then

the value of the Security Field shall be set using the value of the Security Options Parameter and according to 5.7.9.3. Otherwise the Security Field shall be set to zeroes;

e) If the PDU is an Error PDU then the D-bit shall be set to 1. Otherwise the D-bit shall be set to 0;

f) The E-bit shall be set to the complement of the E/R flag in the original CLNP Header;

g) If the value of the Lifetime given in the original CLNP Header is greater than 5 or less than 29 (decimal), then a Lifetime field shall be included in the compressed header and the H bit set to 1. Otherwise the H bit is set to zero. The Lifetime field value shall be identical to the value given in the original CLNP Header;

h) If the SP flag in the original CLNP Header is non-zero, then a Data Unit Identifier (DUI) field shall be present and the S-bit set to 1, and:

1) The M-bit shall be set to the value of the MS-bit in the original CLNP Header;

2) The value of the DUI field shall be set to the Data Unit Identifier contained in the original CLNP Header;

3) If a non-zero Segment offset is present in the original CLNP Header then the O-bit shall be set to 1 and a Segment Offset field shall be present. The value of the Segment Offset field shall be set to the value of the Segment Offset in the original CLNP Header. Otherwise the O-bit shall be zero;

4) If this is the first time that a packet with this DUI has been sent since the index number was assigned, then the L-bit shall be set to 1 and a Total Length Field shall be included and set to the value of the Total Length given in the original CLNP Header. Otherwise the L-bit shall be set to zero.

Otherwise the S and M bits shall be set to zero;

Note 1.— It is not an error to include a Total Length field in more than one compressed header with the same DUI.

Note 2.— This implies caching by the receiver of the value of the Total Length field. The cached information need not be kept longer than the indicated PDU lifetime, and is discarded anyway when the associated index becomes unassigned.

i) If the original CLNP PDU is an Error PDU then the Discard Reason field shall be present and set to the value of the Reason for Discard given in the original CLNP Header;

j) If the original CLNP Header contains:

1) a priority parameter value greater than 14,

2) a security parameter that was uncompressible, i.e. the value of the security field is zero, or

3) any other options parameters other than padding and a Globally Unique QoS Maintenance Parameter, then

such options parameters shall be copied to the compressed header. The Options Length field shall be present and set to the number of bytes in the copied parameters. Otherwise neither the Options Length nor Options shall be present.

5.7.9.4.3.2 The compressed header created above shall replace the original CLNP Header and the resulting compressed header and user data shall be passed to the data link service for transmission. The data type shall be:

a) TYPE_COMPRESSED_CLNP_LONG_WITH_OPTIONS, if options parameters have been copied into the compressed header;

b) TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS, if no options parameters have been copied into the compressed header and the compressed header has a non-zero Bit Field;

c) TYPE_COMPRESSED_CLNP_SHORT otherwise, when the Bit Field shall not be included in the compressed header for this datatype i.e. it is implicitly zero in this data type.

Note.—A zero Bit Field implies that no further fields follow this field as they are all dependent on the Bit Field being non-zero.

5.7.9.4.4 Compression Index Lifetime

5.7.9.4.4.1 For each assigned index number, a timer (CT3) shall be associated.

5.7.9.4.4.2 This timer shall be (re)started every time a packet is sent with that index number.

5.7.9.4.4.3 When the timer expires, the index shall become unassigned.

5.7.9.4.4.4 When an underlying data link is terminated, all associated index numbers become unassigned.

5.7.9.4.4.5 When an index number becomes unassigned, the corresponding local compression directory entry shall be removed.

5.7.9.5 Data Reception Procedures

5.7.9.5.1 Handling of an Incoming Packet

5.7.9.5.1.1 When an incoming packet is recevied from the data link service the indicated data type shall be determined and:

a) If the data type is TYPE_UNCOMPRESSED_PDU, the received packet shall be passed unchanged to the SN Service user using the SN-Unitdata.ind service element;

b) If the data type is TYPE_UNCOMPRESSED_CLNP then the procedures specified in 5.7.9.5.2 shall be applied;

c) If the data type is TYPE_RESTART the procedures specified in 5.7.9.5.6 shall be applied;

d) Otherwise the decompression procedures specified in 5.7.9.5.3 shall be applied.

Note.— TYPE_MULTICAST packets are specified in 5.7.9.6.

5.7.9.5.2 Index Number Assignment

5.7.9.5.2.1 When an incoming packet is received with a data type of TYPE_UNCOMPRESSED_CLNP, the first octet (an unsigned binary number) shall be decoded as the new index number and replaced by the Network Layer Identifier Octet for CLNP (binary 1000 0001).

5.7.9.5.2.2 The PDU shall be passed otherwise unchanged to the SN Service user using the SN-Unitdata.ind service element.

5.7.9.5.2.3 The decompressor shall maintain a local decompression directory for each peer system with which it is currently in communication.

5.7.9.5.2.4 This directory shall comprise a maximum of 128 entries relating an index number in the range 0 to 127, to Source and Destination NSAP Addresses.

5.7.9.5.2.5 This directory shall be interrogated to determine if an entry already exists for this index number.

5.7.9.5.2.6 If such an entry exists and identifies the same Source and Destination NSAP Address pair as encoded into the header of the incoming packet, then no further action shall be taken.

5.7.9.5.2.7 If a different Source and Destination NSAP Address pair is found then the error recovery procedures specified in 5.7.9.5.4 shall be followed.

5.7.9.5.2.8 Otherwise, a new decompression directory entry shall be created associating the received index number with the Source and Destination NSAP Address pair encoded into the header of the incoming packet.

5.7.9.5.3 Decompression Procedures

5.7.9.5.3.1 When an incoming packet is received, then, with reference to the compressed header format given in Figure 5.7-20, a CLNP Header shall be constructed as follows:

a) The Network Layer Protocol Identifier shall be set to binary 1000 0001;

b) The Version/Protocol ID Extension shall be set to binary 0000 0001;

c) The index number shall be decoded from the compressed header and used to determine the Source and Destination NSAP Addresses to be used in the reconstructed CLNP Header by interrogating the local directory specified in 5.7.9.5.2. If no corresponding directory entry can be found then the incoming packet shall be discarded and the error recovery procedures specified in 5.7.9.5.4 shall be applied;

d) If the Q-bit is non-zero, a Globally Unique QoS parameter shall be added to the CLNP Header options parameters and the QoS field bits used to determine the corresponding bits in the parameter value, as specified in 5.7.9.3;

e) If the priority field is non-zero, a priority parameter shall be added to the CLNP Header options parameters and the decimal value of the priority field shall be encoded as the value of the priority parameter;

f) If the security field is non-zero, then a globally unique security parameter shall be added to the CLNP Header, indicating an ATN Security Label:

1) If the most significant 5 bits of the security field are non-zero, then a Traffic Type security tag shall be included in the ATN Security Label; the most significant 3 bits shall indicate a traffic type of ATSC and the least significant 5 bits shall be copied from the most significant 5 bits of the security field;

2) If the least significant 3 bits of the security field are non-zero, then a security classification security tag shall be included in the ATN Security Label; the value of this tag shall be the encoded decimal value of the least significant 3 bits of the security field.

Note.—A padding options parameter may also be included in the CLNP Header.

5.7.9.5.3.2 Decompression of Short Compressed Headers

5.7.9.5.3.2.1 When the data type of the received packet is TYPE_COMPRESSED_CLNP_SHORT, the CLNP Header shall be constructed as above, and:

a) The PDU Type shall be set to indicate a Data PDU;

b) The E/R flag shall be set to 1;

c) The MS and SP flags shall be set to 0, and no segmentation part included in the reconstructed CLNP Header;

d) The Lifetime shall be encoded as decimal 5 if the receiving system is airborne, or as decimal 29 otherwise;

e) The Length Indicator field shall be set to the length of the reconstructed header;

f) The reconstructed header shall replace the compressed header and value of the Segment Length shall be set to the total length to the PDU.

5.7.9.5.3.2.2 The checksum for the reconstructed header shall be recomputed and stored within it.

5.7.9.5.3.2.3 The resulting PDU shall be passed to the SN Service user using the SN-Unitdata.ind service element.

5.7.9.5.3.3 Decompression of Long Compressed Headers with no Options

5.7.9.5.3.3.1 When the data type of the received packet is TYPE_COMPRESSED_CLNP_LONG_ NO_OPTIONS, then the CLNP Header shall be constructed as above in 5.7.9.5.3.

5.7.9.5.3.3.2 The Bit Field shall also be present and used to determine the further additional information in the reconstructed CLNP Header according to the following procedures:

a) If the D-bit is set to 1, then the PDU Type shall be set to indicate an Error PDU. Otherwise the PDU Type shall be set to indicate a Data PDU;

b) The E/R flag shall be set to the complement of the E-bit;

c) If the Q-bit is set, then the value of the S/T-bit in the globally unique QoS Maintenance Parameter shall be set to the value of the T-bit;

d) If the H-bit is set, then the Lifetime in the reconstructed CLNP header shall be set to the value of the Lifetime field in the compressed CLNP Header. If the H-bit is zero, the Lifetime shall be encoded as decimal 5 if the receiving system is airborne, or as decimal 29 otherwise;

e) If the S-bit is set to 0, then the SP and MS flags shall be set to zero and no segmentation part included in the reconstructed CLNP Header. Otherwise, the SP flag shall be set to 1 and a segmentation part included:

1) The MS flag shall be set to the value of the M-bit;

2) The Data Unit Identifier shall be copied from the compressed header to the reconstructed header;

3) If the O-bit is zero, then the Segment Offset shall be set to zero. Otherwise the Segment Offset value shall be copied from the compressed header to the reconstructed header;

4) If the L-bit is set to 1, then the Total Length value shall be copied from the compressed header to the reconstructed header. Additionally:

i. The Total Length shall be cached for use with later packets with the same DUI and index number, and from the same peer system;

ii. If a Total Length with the same DUI and index number, and from the same peer system had already been cached and was a different value, then the PDU shall be discarded and the procedures in 5.7.9.5.4 followed.

5) If the L-bit is set to zero, then the decompressor shall attempt to find a cached Total Length for the same DUI, index number and peer system:

i. If found, then this Total Length shall be copied into the reconstructed CLNP Header;

ii. If not found, then the PDU shall be discarded.

6) ***Recommendation.—*** *The error recovery procedures specified in 5.7.9.5.4 should be followed following the PDU discard.*

Note.—Cached Total Lengths may be discarded when the PDU's lifetime has expired, the index number becomes unassigned, or the data link with the peer system terminated.

f) The Length Indicator field shall be set to the length of the reconstructed header;

g) The reconstructed header shall replace the compressed header and value of the Segment Length shall be set to the total length to the PDU;

h) The checksum for the reconstructed header shall be recomputed and stored within it.

5.7.9.5.3.3.3 The resulting PDU shall be passed to the SN Service user using the SN-Unitdata.ind service element.

5.7.9.5.3.4 Decompression of Long Compressed Headers with Options

5.7.9.5.3.4.1 When the data type of the received packet is TYPE_COMPRESSED_CLNP_LONG_ WITH_OPTIONS, the CLNP Header shall be reconstructed as specified in 5.7.9.5.3.3 above.

5.7.9.5.3.4.2 Additionally, the options parameters contained in the compressed header shall be copied to the reconstructed CLNP Header prior to the recomputation of the Length Indication, Segment Offset and Checksum.

5.7.9.5.4 Error Recovery Procedures

5.7.9.5.4.1 In order to perform error recovery, an empty packet with a data type of TYPE_RESTART shall be sent to the peer system, and the local decompression directory associated with packets received from that peer system shall be cleared i.e. all entries removed.

5.7.9.5.4.2 Received compressed packets shall be discarded but otherwise ignored until a packet is received with a data type of TYPE_UNCOMPRESSED_CLNP.

5.7.9.5.4.3 This shall implicitly acknowledge the restart.

Note.—It is possible to confuse a TYPE_UNCOMPRESSED_CLNP that was sent by the peer system to create a new local reference with a TYPE_UNCOMPRESSED_CLNP sent after re-initialisation of the compression dictionary. However, this will resolve itself following the detection of consequential errors and a further error recovery procedure.

5.7.9.5.5 Index Number Refresh

5.7.9.5.5.1 Whenever a valid packet is received with a given index number, a timer (CT3) shall be (re)started.

5.7.9.5.5.2 When this timer expires the local decompression directory entry for the associated index number shall be removed.

5.7.9.5.6 Processing a TYPE_RESTART Packet

5.7.9.5.6.1 When a TYPE_RESTART packet is received, the local compression directory entries associated when the sending peer system shall be removed.

5.7.9.5.6.2 The associated index numbers shall become unassigned.

5.7.9.6 Multicasting

5.7.9.6.1 The TYPE_MULTICAST data type shall identify a TYPE_CLNP_COMPRESSED_SHORT format packet that is sent multicast to more than one destination NSAP.

Note 1.— An example of the use of TYPE_MULTICAST is a weather broadcast having a destination NSAP which indicates all hosts who want weather information, and a source NSAP indicating that the data originates from a CAA weather processor.

Note 2.—Multicast index numbers may be predefined or dynamically defined. The means to predefine multicast NSAP Addresses and associated index numbers is a local matter and outside the scope of this specification.

5.7.9.6.2 A PDU with a multicast destination NSAP Address that cannot be compressed into the above format shall be sent as TYPE_UNCOMPRESSED_PDU.

5.7.9.6.3 When a ground station uses predefined index numbers, the index numbers used for TYPE_MULTICAST compressed packets shall correspond to a specified and well known Source NSAP Address and Destination Multicast NSAP Address.

5.7.9.6.4 This correspondence shall be known to ground station and all aircraft able to receive the transmission.

5.7.9.6.5 Dynamic Assignment of Index Numbers

5.7.9.6.5.1 When index numbers are dynamically assigned then index numbers shall be assigned and maintained as for singlecast communications

Note.— For example, when a ground station uses dynamically assigned index numbers, the TYPE_UNCOMPRESSED_CLNP packet format is used to assign the meaning of index numbers as specified in 5.7.9.4.2.

5.7.9.6.5.2 ***Recommendation.—****When assigning index numbers to multicast destinations, the ground station should use a different series of index numbers to those used for single cast communications.*

5.7.9.6.5.3 An airborne system shall use a separate local decompression directory for multicast index numbers to that used for singlecast index numbers, and for each ground station.

5.7.9.6.5.4 When a data link is terminated, the index numbers associated with the peer system for multicast communications shall become unassigned.

5.7.9.6.5.5 When a TYPE_UNCOMPRESSED_CLNP packet is sent with a dynamically assigned index number for multicast communications, timers CT1 and CT2 shall be (re)started.

5.7.9.6.5.6 When the CT1 timer expires, the next PDU sent using this index number shall be sent in the TYPE_UNCOMPRESSED_CLNP format even if it is otherwise compressible as a TYPE_MULTICAST.

Note.—The purpose of this procedure is to ensure that aircraft that have recently joined the network have an upper bound on the length of time they are unable to decompress such PDUs.

5.7.9.6.5.7 When the CT2 timer expires, the associated index number shall become unassigned.

5.7.9.6.6 Compression of Multicast PDUs

5.7.9.6.6.1 If a PDU with a multicast Destination NSAP Address is:

a) compressible according to 5.7.9.4.1,

b) may be compressed into the TYPE_COMPRESSED_SHORT format,

c) a suitable index number has been assigned, and

d) the PDU does not have to be sent as a TYPE_UNCOMPRESSED_CLNP (see 5.7.9.6.5 above), then

a compressed packet shall be constructed according to 5.7.9.4.3 and the packet transmitted multicast with a data type of TYPE_MULTICAST.

5.7.9.6.7 Reception of Multicast PDUs

5.7.9.6.7.1 When a TYPE_MULTICAST packet is received, it shall be decompressed according to 5.7.9.5.3 expect that the local decompression directory for multicast index numbers shall be used.

5.7.9.6.7.2 A decompression error shall result in the packet being discarded but the error recovery procedures shall not be followed.

5.7.9.6.7.3 When a TYPE_UNCOMPRESSED_CLNP packet is received that has a multicast destination NSAP Address, the procedures of 5.7.9.5.2 shall be applied except that the local decompression directory for multicast index numbers shall be used.

5.7.9.6.7.4 If a directory entry for the index number is found, but the Source and Destination NSAP Address of the incoming packet do not match the existing directory entry then the directory entry shall be marked as unsafe and all subsequent compressed packets for this index number discarded until the index number becomes unassigned.

5.7.9.6.7.5 Additionally, a timer (CT2) shall be (re)started for each such TYPE_UNCOMPRESSED_ CLNP received.

5.7.9.6.7.6 When CT2 expires the associated index number shall become unassigned.

5.7.9.7 Timers

Table 5.7-17 Timers used by the CLNP Header Compression Algorithm

Symbol	Parameter Name	Minimum	Maximum	Default	Increment
CT1	Multicast Packet Period	1	255	5	1 packet
CT2	Multicast Refresh Timer	1	32	180	1 second
CT3	Index Idle Timer	1	32	20	1 minute

Note.— The default values shown are appropriate for VDL Mode 3. Other data links may specify different default values.

5.7.9.7.1 CT1 (Multicast Packet Period) Parameter

5.7.9.7.1.1 The Multicast Packet Period shall define the period whereby an uncompressed packet is sent to refresh the compressor state for the receiving unit.

5.7.9.7.1.2 ***Recommendation.—****When the underlying data link uses XID messages to configure the data link and set parameter values, the XID format for CT1 should be:*

Parameter ID	*0 1 0 1*	*0 0 1 0*	*Multicast Packet Period*
Parameter Length	*0 0 0 0*	*0 0 0 1*	
Parameter Value	$v_8\ v_7\ v_6\ v_5$	$v_4\ v_3\ v_2\ v_1$	

5.7.9.7.2 CT2 (Multicast Refresh) Timer

5.7.9.7.2.1 The Multicast Refresh Timer shall define an upper bound on the time between transmission of uncompressed headers in case message traffic is light.

Note.—This ensures that the receiver can correlate the header with the compression index in a timely fashion.

5.7.9.7.2.2 ***Recommendation.—****When the underlying data link uses XID messages to configure the data link and set parameter values, the XID format for CT2 should be:*

Parameter ID	*0 1 0 1*	*0 0 1 1*	*Multicast Refresh Timer*
Parameter Length	*0 0 0 0*	*0 0 1 0*	
Parameter Value	$v_{16}\ v_{15}\ v_{14}\ v_{13}$ $v_8\ v_7\ v_6\ v_5$	$v_{12}\ v_{11}\ v_{10}\ v_9$ $v_4\ v_3\ v_2\ v_1$	

5.7.9.7.3 CT3 (Index Idle) Timer

5.7.9.7.3.1 The Index Idle Timer shall define an upper bound on how long the compressor shall wait before recovering an idle index.

Note.—An index is assumed idle if no message traffic has passed using it before the CT3 timer expires.

5.7.9.7.3.2 ***Recommendation.—****When the underlying data link uses XID messages to configure the data link and set parameter values, the XID format for CT3 should be:*

Parameter ID	*0 1 0 1*	*0 1 0 0*	*Index Idle Timer*
Parameter Length	*0 0 0 0*	*0 0 1 0*	

Parameter Value $v_{16}\ v_{15}\ v_{14}\ v_{13}\quad v_{12}\ v_{11}\ v_{10}\ v_{9}$
$v_{8}\ \ v_{7}\ \ v_{6}\ \ v_{5}\quad v_{4}\ \ v_{3}\ \ v_{2}\ \ v_{1}$

5.8 ROUTING INFORMATION EXCHANGE SPECIFICATION

5.8.1 Introduction

5.8.1.1 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 5.3.

5.8.1.2 Applicability of Requirements

5.8.1.2.1 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 5.8.2, 5.8.3, 5.8.3.2.2 to 5.8.3.2.5 inclusive, 5.8.3.2.8 to 5.8.3.2.9 inclusive, 5.8.3.2.11, 5.8.3.3.2.1, 5.8.3.3.3 and the APRLs specified for an Airborne Router in 5.8.3.5.

5.8.1.2.2 ATN Airborne Routers implementing the procedures for the optional non-use of IDRP shall be compliant with 5.8.2.

5.8.1.2.3 All ATN Air/Ground Routers shall comply with the provisions contained in 5.8.2, 5.8.3, 5.8.3.2.2 to 5.8.3.2.9 inclusive, 5.8.3.2.11, 5.8.3.3.2.2, 5.8.3.3.3 and the APRLs specified for an Air/Ground Router in 5.8.3.5.

5.8.1.2.4 All Ground/Ground Inter-Domain Routers shall comply with the provisions contained in 5.8.2, 5.8.3.2.2 to 5.8.3.2.9 inclusive, 5.8.3.2.11, 5.8.3.3.2.2, 5.8.3.3.3 and the APRLs specified for an Ground/Ground Router in 5.8.3.5.

5.8.1.2.5 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 5.8.3.2.10.1.

5.8.1.2.6 All ATN Routers which support ATN security services shall comply with the provisions contained in 5.8.3.2.10.2.

5.8.2 End System to Intermediate System Routing Information Exchange Protocol (ES-IS) over Mobile Subnetworks

5.8.2.1 General

5.8.2.1.1 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.

5.8.2.1.2 Configuration Information shall be exchanged by both ATN Air/Ground and Airborne Routers over each Mobile Subnetwork connection supporting an adjacency between them.

Note 1.— The use of ISO/IEC 9542 Configuration Information over Mobile Subnetworks in support of air/ground route initiation is specified in 5.3.5.2.6.

Note 2.— The use of ISO/IEC 9542 Configuration Information over Mobile Subnetworks in support of IDRP Authentication Type 2 is specified in 5.3.5.2.16.

5.8.2.1.3 ATN Data Link Capabilities Parameter

5.8.2.1.3.1 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 and to signal authentication related information. 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 and provide its public key certificate, if requested. 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 (e.g. security) 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.

5.8.2.1.3.2 The ATN Data Link Capabilities Parameter shall not occur more than once in the options part of an ISO/IEC 9542 ISH PDU.

5.8.2.1.3.3 The ATN Data Link Capabilities Parameter shall consist of three fields, as illustrated in Figure 5.8-1.

ATN Data Link Capabilities Parameter Code	ATN Data Link Capabilities Parameter Length	ATN Data Link Capabilities Parameter Value
Octet 1	2	3 ..... end

Figure 5.8-1: The ATN Data Link Capabilities Parameter

5.8.2.1.3.4 Encoding of the ATN Data Link Capabilities Parameter

5.8.2.1.3.4.1 The ATN Data Link Capabilities Parameter code field shall be one octet in length.

5.8.2.1.3.4.2 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.

5.8.2.1.3.4.3 The ATN Data Link Capabilities Parameter length field shall be one octet long.

5.8.2.1.3.4.4 The ATN Data Link Capabilities Parameter length field shall define the length in octets of the ATN Data Link Capabilities Parameter value field.

5.8.2.1.3.4.5 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 and signals whether the public key certificate of the peer ATN Router is required or not.

5.8.2.1.3.4.5.1 The ATN Data Link Capabilities Parameter value field shall comprise a bit map, where bit 0 is the low order bit.

5.8.2.1.3.4.5.2 The assignment of bits in the ATN Data Link Capability Parameter value field and the semantic of each bit shall be according to Table 5.8-1

Table 5.8-1 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	1 0	IDRP Type 2 Authentication Requested IDRP Type 2 Authentication Not Requested
2	1 0	Public-Key Certificate Required Public-Key Certificate Not Required

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 5.3.5.2.6.7) 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.

5.8.2.1.3.4.5.3 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.

5.8.2.1.3.5 When an ATN Air/Ground or Airborne Router recognises 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.

5.8.2.1.3.6 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.

5.8.2.1.4 Mobile Subnetwork Capabilities Parameter

5.8.2.1.4.1 ATN Air/Ground and Airborne Routers shall support the Mobile Subnetwork Capabilities Parameter in the options part of an ISO/IEC 9542 ISH PDU.

5.8.2.1.4.2 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.

5.8.2.1.4.3 The Mobile Subnetwork Capabilities Parameter shall consist of three fields, as illustrated in Figure 5.8-2, 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 5.8-2: The Mobile Subnetwork Capabilities Parameter

5.8.2.1.4.4 Encoding of the Mobile Subnetwork Capabilities Parameter

5.8.2.1.4.4.1 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.

5.8.2.1.4.4.2 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.

5.8.2.1.4.4.3 Mobile Subnetwork Capabilities Parameter Value Field

5.8.2.1.4.4.3.1 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.

5.8.2.1.4.4.3.2 This octet shall comprise a bit map, where each bit corresponds to a different traffic type.

5.8.2.1.4.4.3.3 The assignment of bits to traffic types shall be according to Table 5.8-5, where bit 0 is the low order bit.

5.8.2.1.4.4.3.4 Setting a bit to one shall indicate that the corresponding traffic type is allowed to pass over the air/ground subnetwork.

5.8.2.1.4.4.3.5 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 5.8.3.2.3.2.4 through 5.8.3.2.3.2.6.

5.8.2.1.4.4.3.6 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.

5.8.2.1.4.4.3.7 If present, the second octet of the Mobile Subnetwork Capabilities Parameter Value field shall be encoded according to Table 5.8-2.

Table 5.8-2: 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 and Class "A" is the highest class.

5.8.2.1.4.4.3.8 Those ATSC Class values which are not defined in Table 5.8-2 shall be reserved for future use by this specification.

5.8.2.1.5 Route Redirection information shall not be exchanged between an ATN Air/Ground and Airborne Router.

5.8.2.2 ATN Protocol Requirements List - ISO/IEC 9542

5.8.2.2.1 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 5.8-3.

Table 5.8-3 ISO/IEC 9542 - Intermediate System

Item	**Protocol Function**	**Clauses**	**ISO Status**	**ATN Support**
CI	Is configuration information supported over the associated subnetwork?	ATN SARPs Ref.: 5.8.2	O	M
RI	Is redirection information supported over the associated subnetwork?	ATN SARPs Ref.: 5.8.2	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	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

Item	Protocol Function	Clauses	ISO Status	ATN Support
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
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 SARPs Ref: 5.8.2.1.3	--	ISH-s:M
DLC-r	<r> Data Link Capabilities	ATN SARPs Ref: 5.8.2.1.3	--	ISH-r:M
MSNC-s	<s> Mobile Subnetwork Capabilities	ATN SARPs Ref: 5.8.2.1.4, 5.3.5.2.6.5	- -	ISH-s and AGR:M
MSNC-r	<r> Mobile Subnetwork Capabilities	ATN SARPs Ref: 5.8.2.1.4, 5.3.5.2.6.9	- -	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 SARPs Ref.: 5.3.5.2.9	M	M: from: 0 seconds to: 65535 seconds with a tolerance of: 10%

	Parameter Ranges				
CTv	If configuration information is supported, what range of values can be set for the Configuration Timer ?	ATN SARPs Ref.: 5.3.5.2.5	CI:M	M	from: 0 seconds to: 65535 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 case where IDRP is used over the Air/Ground link, the Holding Time field of transmitted ISH PDUs is preferably set to 65534 seconds as recommended in 5.3.5.2.10.9. The purpose of this recommendation is to effectively suppress the regular generation of ISH PDUs on the Air/Ground link.

Note 2.— In 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.

5.8.3 Intermediate System to Intermediate System Inter-Domain Routing Information Exchange Protocol

5.8.3.1 General

5.8.3.1.1 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 5.8.3.5.

5.8.3.2 ATN Specific Features

5.8.3.2.1 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 conforms 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 .

5.8.3.2.2 Use of the Security Path Attribute

5.8.3.2.2.1 ATN Routers supporting inter-domain routing shall support the IDRP Security Path Attribute with a Security Registration Identifier set to the value defined in 5.6.2.2.6 for the ATN Security Registration Identifier.

5.8.3.2.2.2 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 5.6.2.2.6.

5.8.3.2.2.3 The following Security Tag Sets shall be supported:

a) The Air/Ground Subnetwork type, as defined in 5.8.3.2.3.2, and

b) The ATSC Class, as defined in 5.8.3.2.3.3.

5.8.3.2.2.4 **Recommendation.** — *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 5.6.2.2.6.*

5.8.3.2.2.5 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.

5.8.3.2.2.6 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.

5.8.3.2.2.7 At most one ATSC Class Security Tag Set shall be present in a route's Security Path Attribute.

5.8.3.2.2.8 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.

5.8.3.2.3 Encoding of the Security Path Attribute Security Information Field

5.8.3.2.3.1 General

5.8.3.2.3.1.1 The Security Path Attribute Security Information Field shall comprise zero, one or more Security Tag Sets as defined in 5.6.2.2.6.

Note.— The Security Tag Set format defined for use with CLNP in 5.6, has been adopted here as a convenient method for the extensible encoding of security related information.

5.8.3.2.3.2 Encoding of the Air/Ground Subnetwork Type Security Tag Set

5.8.3.2.3.2.1 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.

5.8.3.2.3.2.2 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 5.8-4.

Table 5.8-4 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

5.8.3.2.3.2.3 Those air/ground subnetwork type security tag values which are not defined in Table 5.8-4 shall be reserved for future use by this specification.

5.8.3.2.3.2.4 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.

5.8.3.2.3.2.5 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.

5.8.3.2.3.2.6 The assignment of bits to Traffic Type shall be according to Table 5.8-5, where bit 0 is the low order bit:

Table 5.8-5 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

5.8.3.2.3.2.7 The semantics of bits 5 to 7 shall be reserved for future use and shall always be set to one.

5.8.3.2.3.3 Encoding of the ATSC Class Security Tag Set

5.8.3.2.3.3.1 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.

5.8.3.2.3.3.2 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.

5.8.3.2.3.3.3 The Security Tag shall always be one octet in length.

5.8.3.2.3.3.4 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.

5.8.3.2.3.3.5 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.

5.8.3.2.3.3.6 The ATSC Class(es) supported shall be identified according to Table 5.8-6, where bit 0 is the low order bit, and setting a bit to one shall indicate that the corresponding ATSC Class is supported.

5.8.3.2.3.3.7 A bit set to zero shall indicate that the corresponding ATSC Class is not supported.

Table 5.8-6 Identification of Supported ATSC Classes

Bit Number	ATSC Class
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H

5.8.3.2.4 Update of Security Information

5.8.3.2.4.1 The Air/Ground Subnetwork Type

5.8.3.2.4.1.1 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 5.8.2.1.3) 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 5.3.5.2.12 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.

5.8.3.2.4.1.2 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.

5.8.3.2.4.1.3 Any Air/Ground Subnetwork Security Tags with a second octet that is all zeroes shall be removed from the route.

5.8.3.2.4.1.4 If all Air/Ground Subnetwork Security Tags present have a zero second octet then the route shall not be advertised over this adjacency.

5.8.3.2.4.2 The ATSC Class

5.8.3.2.4.2.1 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 5.8.2.1.3) 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 5.3.5.2.12), 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 5.8.3.2.4.2.5, 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 5.3.7.1.2.1 e), 5.3.7.1.5.1 c), 5.3.7.3.2.1 d), and 5.3.7.1.3.1 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.

5.8.3.2.4.2.2 When an ATSC Class Security tag is added to a route, then the value of the Tag Set Name shall be set according to 5.8.3.2.3.3 and depending upon whether the adjacency has been specified to support ATSC traffic only or both ATSC and non-ATSC traffic.

5.8.3.2.4.2.3 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.

5.8.3.2.4.2.4 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.

5.8.3.2.4.2.5 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.

5.8.3.2.4.2.6 Paragraph has been deleted..

5.8.3.2.4.2.7 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.

5.8.3.2.4.2.8 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 5.8.2.1.3), 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.

5.8.3.2.4.3 The Security Classification

5.8.3.2.4.3.1 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.

5.8.3.2.5 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.

5.8.3.2.5.1 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.

5.8.3.2.5.2 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.

5.8.3.2.6 Route Aggregation and Route Information Reduction

5.8.3.2.6.1 General

5.8.3.2.6.1.1 ATN Routers shall implement the procedures for Route Aggregation and Route Information Reduction when required to do so according to 5.8.3.2.6.2 through 5.8.3.2.6.5.

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.

5.8.3.2.6.2 Policy Based Route Aggregation

5.8.3.2.6.2.1 **Recommendation.—** *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.*

5.8.3.2.6.2.2 **Recommendation.**— *An Air/Ground Router should aggregate all routes to destinations in ATN Islands, other than those to destinations in its own ATN Island.*

5.8.3.2.6.2.3 **Recommendation**.— *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 scaleable internet.

5.8.3.2.6.2.4 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.

5.8.3.2.6.3 Aggregation of Routes in the Same Loc-RIB with Identical NLRI

5.8.3.2.6.3.1 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.

5.8.3.2.6.3.2 Such routes shall be consequently copied to the associated Adj-RIB-Out.

5.8.3.2.6.3.3 For each adjacent BIS, the resulting aggregated route shall be inserted into the associated Adj-RIB-Out.

5.8.3.2.6.3.4 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 5.8.3.2.6.4 below.

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 later revision of these SARPs.

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 recognised 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.

5.8.3.2.6.4 Aggregation of the Security Path Attribute Information Field

5.8.3.2.6.4.1 General

5.8.3.2.6.4.1.1 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.

5.8.3.2.6.4.1.2 Similarly, routes available to ATSC traffic only and routes available to both ATSC and non-ATSC traffic with dissimilar NLRI shall not be aggregated.

5.8.3.2.6.4.1.3 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.

5.8.3.2.6.4.2 Air/Ground Subnetwork Security Tag

5.8.3.2.6.4.2.1 The aggregated security path attribute shall comprise each air/ground subnetwork security tag contained in the security path attribute of the component routes.

5.8.3.2.6.4.2.2 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.

5.8.3.2.6.4.2.3 Only a single air/ground subnetwork type security tag for each distinct air/ground subnetwork type shall be present in the aggregated route.

5.8.3.2.6.4.3 ATSC Class Security Tag

5.8.3.2.6.4.3.1 General

5.8.3.2.6.4.3.1.1 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.

5.8.3.2.6.4.3.2 Non-Identical NLRI in Component Routes

5.8.3.2.6.4.3.2.1 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.

5.8.3.2.6.4.3.2.2 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.

5.8.3.2.6.4.3.2.3 All the other bits in this tag shall be set to zero.

5.8.3.2.6.4.3.3 Identical NLRI in Component Routes

5.8.3.2.6.4.3.3.1 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.

5.8.3.2.6.4.3.3.2 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.

5.8.3.2.6.4.3.3.3 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 5.8.3.2.3.3.1 to take the value [0000 0110].

5.8.3.2.6.4.3.3.4 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.

5.8.3.2.6.4.3.3.5 If none of the component routes contains an ATSC Class security tag, then the aggregated route shall not contain an ATSC Class security tag.

5.8.3.2.6.4.3.4 Security Classification Security Tag

5.8.3.2.6.4.3.4.1 When a Security Classification security tag occurs in all component routes, then the aggregated route shall contain a Security Classification security tag.

5.8.3.2.6.4.3.4.2 This tag shall be set to the lowest classification from the classifications given to the aggregated route's component routes.

5.8.3.2.6.4.3.4.3 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.

5.8.3.2.6.5 Route Information Reduction

5.8.3.2.6.5.1 **Recommendation**.— *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).

5.8.3.2.6.5.2 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.

5.8.3.2.7 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.*

5.8.3.2.7.1 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.

5.8.3.2.7.2 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.

5.8.3.2.8 Interpretation of Route Capacity

5.8.3.2.8.1 For the ATN environment, the CAPACITY path attribute shall contain one of the values listed in Table 5.8-7, and shall be assumed to have the semantics given there:

Table 5.8-7 Interpretation of Capacity Route Metric

Value	Meaning
1 ... 9	Unassigned
13	0 - 19.2 Kbits/sec
12	19.2 - 56 Kbits/sec
11	56 - 1500 Kbits/sec
10	> 1500 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.

5.8.3.2.8.2 Those capacity route metric values which are not assigned in Table 5.8-7 shall be reserved for future use by this specification.

5.8.3.2.9 Network Layer Reachability Information

5.8.3.2.9.1 General

5.8.3.2.9.1.1 In support of ATN communications, ATN Routers shall encode the NLRI Addr_info field of each route as a list of NSAP Address Prefixes.

5.8.3.2.9.1.2 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.

5.8.3.2.9.2 NSAP Address Prefix Alignment

5.8.3.2.9.2.1 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.— 5.8.3.2.12 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.

5.8.3.2.10 BISPDU Authentication

5.8.3.2.10.1 Authentication Type 1

Note.— Authentication type 1 is performed by an ATN Router which does not support authentication type 2 or if local policy permits authentication type 1 in the event that the peer router does not support authentication type 2.

5.8.3.2.10.1.1 ATN Routers shall support the validation of BISPDUs using Authentication Type 1.

5.8.3.2.10.1.2 When an ATN Router, which does not support ATN security services or for which local policy does not permit authentication type 2, establishes 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.

5.8.3.2.10.1.3 When an Airborne or Air/Ground Router, which has signalled type 2 authentication during the ISO/IEC 9542 ISH exchange, receives an OPEN PDU with the Authentication Code field set to 1, it shall process the OPEN PDU only if permitted to do so by local policy.

5.8.3.2.10.1.4 When an Airborne or Air/Ground Router, which has signalled type 2 authentication during the ISO/IEC 9542 ISH exchange, receives an OPEN PDU with the Authentication Code field set to 1, and local policy does not permit it to process the OPEN PDU, then the OPEN PDU shall be discarded without any further action.

5.8.3.2.10.1.5 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.

5.8.3.2.10.1.6 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.

5.8.3.2.10.2 Authentication Type 2

5.8.3.2.10.2.1 Common IDRP Connection Establishment Provisions for Authentication Type 2

Note.— The following requirements apply to the establishment of type 2 IDRP connections over both mobile and ground subnetworks, i.e. they apply to all ATN routers supporting ATN security services.

5.8.3.2.10.2.1.1 An ATN Router which supports ATN security services shall establish a BIS-BIS connection with authentication type 2 only if type 2 authentication is permitted by local policy.

5.8.3.2.10.2.1.2 When an ATN Router establishes a BIS-BIS connection with authentication type 2, then it shall set the value of the Authentication Code to 2 in the OPEN PDU.

5.8.3.2.10.2.1.3 When an ATN Router establishes a BIS-BIS connection with authentication type 2, then it shall place a random variable (see 5.8.3.2.10.3.1.6) in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.1.4 When an ATN Router establishes a BIS-BIS connection with authentication type 2, then it shall place a type 1 authenticator, generated according to clause 7.7.1 of ISO/IEC 10747, in the Validation Pattern field of the OPEN PDU.

Note.— Storing a type 1 authenticator in the Validation Pattern field while authentication type 2 is indicated in the Authentication Code field (only for the OPEN PDU) is an ATN specific convention in support of type 2 authentication.

5.8.3.2.10.2.2 IDRP Connection Establishment with Authentication Type 2 over Mobile Subnetworks

5.8.3.2.10.2.2.1 An Airborne or Air/Ground Router shall establish a BIS-BIS connection with authentication type 2 over a Mobile Subnetwork only if type 2 authentication was signalled by the peer router in the ISO/IEC 9542 ISH PDU.

Note.— Otherwise authentication type 1 will be established if permitted as indicated in section 5.8.3.2.10.1.

5.8.3.2.10.2.3 IDRP Connection Establishment with Authentication Type 2 for Air/Ground Routers

Note.— The following requirements apply to the establishment of type 2 IDRP connections by Air/Ground Routers. They are concerned with whether to perform mutual authentication (and send a public key certificate in the Authentication Data field) or single entity authentication (and send a public key in the Authentication Data field). In the event that the Air/Ground Router attempts to retrieve the Airborne router's certificate subsequent to sending the ISH PDU and the certificate could not be retrieved, then the Airborne Router will indicate public key certificate required in the OPEN PDU.

5.8.3.2.10.2.3.1 When an Air/Ground Router establishes a BIS-BIS connection with authentication type 2 over a Mobile Subnetwork for which 'public-key certificate required' was signalled in the ISO/IEC 9542 ISH PDU received from the Airborne Router, then it shall place its certificate path (see 5.8.3.2.10.3.1.8) in the Authentication Data field of the OPEN PDU to be sent to the Airborne Router.

5.8.3.2.10.2.3.2 When an Air/Ground Router establishes a BIS-BIS connection with authentication type 2 over a Mobile Subnetwork and local policy requires mutual authentication, then it shall place its certificate path (see 5.8.3.2.10.3.1.8) in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.3.3 When an Air/Ground Router establishes a BIS-BIS connection with authentication type 2 over a Mobile Subnetwork for which 'public-key certificate not required' was signalled in the ISH PDU received from the Airborne Router and local policy does not require mutual authentication, then it shall place its public-key information (see 5.8.3.2.10.3.1.7) in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.3.4 When an Air/Ground Router establishes a BIS-BIS connection with authentication type 2 and the public key certificate of the Airborne Router could not be retrieved from a supporting certificate delivery service, then the Air/Ground Router shall signal 'public-key certificate required' (see 5.8.3.2.10.3.1.4) in in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.4 IDRP Connection Establishment with Authentication Type 2 for Airborne Routers

5.8.3.2.10.2.4.1 When an Airborne Router establishes a BIS-BIS connection with authentication type 2 over a Mobile Subnetwork for which 'public-key certificate required' was signalled in the ISO/IEC 9542 ISH PDU received from the Air/Ground Router, then it shall place its certificate path (see 5.8.3.2.10.3.1.8) in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.4.2 When an Airborne Router, which has sent an OPEN PDU without its public-key certificate, receives an OPEN PDU with 'public-key certificate required' signalled in the Authentication Data field, then it shall re-send its OPEN PDU with its certificate path (see 5.8.3.2.10.3.1.8) in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.5 IDRP Connection Establishment with Authentication Type 2 over Ground Subnetworks

5.8.3.2.10.2.5.1 When a Ground or Air/Ground Router establishes a BIS-BIS connection with authentication type 2 over a ground subnetwork, then it shall place its certificate path (see 5.8.3.2.10.3.1.8) in the Authentication Data field of the OPEN PDU.

5.8.3.2.10.2.6 Common Type 2 IDRP Authentication Provisions

Note.— The following authentication requirements apply to all ATN routers supporting ATN security services.

5.8.3.2.10.2.6.1 When an ATN Router receives an OPEN PDU with the Authentication Code field set to 2, then it shall validate the Validation Pattern field according to clause 7.7.1 of ISO/IEC 10747.

5.8.3.2.10.2.6.2 When an ATN Router receives an OPEN PDU with the Authentication Code field set to 2 and the Authentication Data field contains the peer router's public key certificate, then it shall validate the certificate path according to the procedure specified in 8.4.5.

5.8.3.2.10.2.6.3 When an ATN Router receives an OPEN PDU with the Authentication Code field set to 2, then it shall derive a shared session key using the ATN Key Agreement Scheme as specified in 8.5.4.

5.8.3.2.10.2.6.4 If the Public Key Certificate received from a peer ATN router fails verification or if a valid shared session key cannot be derived, then the OPEN PDU shall be discarded without any further action.

5.8.3.2.10.2.6.5 Once an ATN Router has derived a shared session key for a BIS-BIS connection, it shall place a message authenticator over the BISPDU, generated using the ATN Keyed Message Authentication Code Generation Primitive (AMACGP) according to the procedure specified in 8.5.6.2.1, in the Validation Pattern field of all BISPDUs it sends subsequent to the OPEN PDU exchange.

5.8.3.2.10.2.6.6 When an ATN Router, which has derived a shared session key, receives a BISPDU with a type 2 message authenticator in the Validation Pattern field, then it shall verify the authenticator using the ATN Keyed Message Authentication Code Verification Primitive (AMACVP) according to the procedure specified in 8.5.6.2.2.

Note.— Clause 7.20.1 of ISO/IEC 10747 requires BISPDUs which fail verification to be discarded without any further action.

5.8.3.2.10.3 Format and Encoding of IDRP BISPDU Fields to Support Authentication Type 2

5.8.3.2.10.3.1 IDRP Authentication Data Field

Note.— The Authentication Data field contains two fixed form identifiers (the Version Identification and the Authentication Options Identification) followed by two parameters of the form type-length-value. One type-length-value parameter is the Random Value parameter which provides protection against replay and intercept attacks against IDRP authentication. The Random Value parameter is defined as type-length-value to facilitate use of alternative random challenges, e.g., other standardized pseudo-random values or other time variant parameters, in future versions of IDRP security. The other type-length-value parameter in the Authentication Data field is either the Public Key Information Parameter or the Certificate Path parameter. The former is sent by the Air/Ground Router to the Airborne Router when single entity authentication is provided while the latter is sent when mutual authentication is performed over the Air/Ground subnetwork or if IDRP security is performed over ground subnetworks. These parameters are type-length-value to facilitate use of alternate algorithms and/or domain parameters in future versions.

5.8.3.2.10.3.1.1 For Authentication Type 2, the IDRP Authentication Data field shall contain the items illustrated in Figure 5.8-3.

Version Identification	Authentication Options Identification	Variable Length Parameters
Octet 1	2	3 ... end

Figure 5.8-3: Format of IDRP Authentication Data Field

5.8.3.2.10.3.1.2 ATN Routers which support Authentication Type 2 shall ignore unrecognized type-length-value parameters.

Note.— This requirement will enable backwards compatibility of future versions of IDRP security.

5.8.3.2.10.3.1.3 The Version Identification shall be encoded as binary [0000 0001] to indicate the first version of type 2 authentication in support of ATN security services.

5.8.3.2.10.3.1.4 The assignment of bits in and the semantic of each bit for the Authentication Options Identification shall be according to Table 5.8-8, with bit 0 being the low order bit.

Table 5.8-8 Semantics and Value Assignment for Authentication Options Identification Sub-Field

Bit Position	Value	Semantic
0	1 0	Public-Key Certificate Required Public-Key Certificate Not Required
1 - 7	Unassigned	Reserved

5.8.3.2.10.3.1.5 Those bits which are not assigned in Table 5.8-8 shall be reserved for future use by this specification.

5.8.3.2.10.3.1.6 Random Variable Parameter

5.8.3.2.10.3.1.6.1 The Random Variable Parameter shall consist of three fields as illustrated in Figure 5.8-4.

Random Variable Parameter Code	Random Variable Parameter Length	Random Variable Parameter Value
Octet 1	2 and 3	4 ... end

Figure 5.8-4: Format of Random Variable Parameter

5.8.3.2.10.3.1.6.2 The Random Variable Parameter Code field shall be encoded as binary [0000 0001].

5.8.3.2.10.3.1.6.3 The Random Variable Parameter Length field shall define the length in octets of the Random Variable Parameter Value field.

5.8.3.2.10.3.1.6.4 The Random Variable Parameter Value field shall contain a 32-bit unsigned integer value that is encoded most significant byte first.

5.8.3.2.10.3.1.7 Public Key Information Parameter

5.8.3.2.10.3.1.7.1 The Public Key Information Parameter shall consist of three fields as illustrated in Figure 5.8-5.

Public Key Information Parameter Code	Public Key Information Parameter Length	Public Key Information Parameter Value

Octet 1	2 and 3	4 ... end

Figure 5.8-5: Format of Public Key Information Parameter

5.8.3.2.10.3.1.7.2 The Public Key Information Parameter Code field shall be encoded as binary [0000 0010].

5.8.3.2.10.3.1.7.3 The Public Key Information Parameter Length field shall define the length in octets of the Public Key Information Parameter Value field.

5.8.3.2.10.3.1.7.4 The Public Key Information Parameter Value field shall consist of two sub-fields as illustrated in Figure 5.8-6.

Algorithm	Public Key
Octet 1 and 2	3 ... 24

Figure 5.8-6: Format of Public Key Information Parameter Value Field

5.8.3.2.10.3.1.7.5 The Algorithm sub-field shall be encoded as hexadecimal [02 0F].

Note.— The sub-field value is based on the id-PublicKeyType Object Identifier (OID) and the sect163r2 OID (see 8.4.3.2.11). If a new algorithm or a new set of domain parameters is supported in future versions, then the Algorithm sub-field can be modified with an encoding for the new OIDs or to select either the new OIDs or the current OIDs.

5.8.3.2.10.3.1.7.6 The Public Key sub-field shall contain a 22-octet public key.

Note.— The public key is in compressed form 02||x or 03||x where x is the first coordinate of an elliptic curve point as defined in 8.5.1.

5.8.3.2.10.3.1.8 Certificate Path Parameter

5.8.3.2.10.3.1.8.1 The Certificate Path Parameter shall consist of three fields as illustrated in Figure 5.8-7.

Certificate Path Parameter Code	Certificate Path Parameter Length	Certificate Path Parameter Value
Octet 1	2 and 3	4 ... end

Figure 5.8-7: Format of Certificate Path Parameter

5.8.3.2.10.3.1.8.2 The Certificate Path Parameter Code field shall be encoded as binary [0000 0011].

5.8.3.2.10.3.1.8.3 The Certificate Path Parameter Length field shall define the length in octets of the Certificate Path Parameter Value field.

5.8.3.2.10.3.1.8.4 The Certificate Path Parameter Value field shall consist of 2 fixed and 1 repeating sub-field as illustrated in Figure 5.8-8.

ATN Router Certificate	Number of CA Certificates	CA Certificate 1	CA Certificate 2	.....	CA Certificate n
Octet 1 ... 124	125	126 ... 244			.... end

Figure 5.8-8: Format of Certificate Path Parameter Value Field

Note.— Each CA certificate in Figure 5.8-8 above is 119 octets long.

5.8.3.2.10.3.1.8.5 The ATN Router Certificate sub-field shall contain a compressed ATN Router Certificate as defined in 8.4.3.2.

5.8.3.2.10.3.1.8.6 The Number of CA Certificates sub-field shall contain the number of Certificate Authorities (CAs) along the path to the state CA of the peer ATN router.

5.8.3.2.10.3.1.8.7 Each CA Certificate sub-field shall contain a compressed CA Certificate as defined in 8.4.3.2.

5.8.3.2.10.3.2 IDRP Validation Pattern Field

5.8.3.2.10.3.2.1 For Authentication Type 2, the low order portion of the IDRP Validation Pattern field shall contain the Tag resulting from application of the ATN Keyed Message Authentication Code Generation Primitive as specified in 8.5.6.2.1 to the entire BISPDU with all bits of the Validation Pattern field initially set to 0.

Note.— For IDRP an 80-bit Tag will be generated.

5.8.3.2.11 Restrictions on Route Advertisement

5.8.3.2.11.1 A route shall not be advertised to a BIS in another RD when:

a) The route contains the receiving RD's 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).

5.8.3.2.12 RIB_Att Support

Table 5.8-9 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.*
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.*

5.8.3.2.12.1 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.

5.8.3.2.12.2 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.

5.8.3.2.13 Additional Update PDU Error Handling

5.8.3.2.13.1 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.

5.8.3.2.14 CLNP Data PDU Parameters

5.8.3.2.14.1 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.

5.8.3.3 Compliance with ISO/IEC 10747

5.8.3.3.1 General

5.8.3.3.1.1 The IDRP protocol exchange shall use the connectionless network service provided by ISO/IEC 8473, as specified in ISO/IEC 10747.

5.8.3.3.2 ISO/IEC 10747 Mandatory Requirements

5.8.3.3.2.1 Airborne Router

5.8.3.3.2.1.1 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 5.8-9, 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.

5.8.3.3.2.2 Ground Router

Note.— This section refers to both Air/Ground and Ground/Ground Routers generically as Ground Routers.

5.8.3.3.2.2.1 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.

5.8.3.3.2.2.2 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.

5.8.3.3.3 ISO/IEC 10747 Optional Requirements

5.8.3.3.3.1 An ATN Router shall support the Security Path Attribute as specified in 5.8.3.2.2 and 5.8.3.2.3.

5.8.3.3.3.2 **Recommendation.**— *An ATN Air/Ground Router should implement Route Aggregation and Route Information Reduction Procedures.*

5.8.3.3.3.3 **Recommendation**.— *An ATN Ground/Ground Router should implement Route Aggregation and Route Information Reduction Procedures.*

5.8.3.4 KeepAlive Timer

5.8.3.4.1 **Recommendation**.— 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 follows:

Table 5.8-10 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.

5.8.3.4.2 **Recommendation**.— 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.

5.8.3.4.3 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.

5.8.3.5 **APRLs**

5.8.3.5.1 General

5.8.3.5.1.1 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 check list 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.

5.8.3.5.2 ATN Specific Protocol Requirements

Item	**Description**	**ATN SARPs Ref**	**G-G Router**	**A/G Router**	**Airborne Router**
ATNIDRP1	Does this BIS encode and use the Security Path Attribute?	5.8.3.2.2, 5.8.3.2.3	M	M	M
ATNIDRP2	Does this BIS immediately re-advertise routes if the security information contained in the route's security path attribute changes?	5.8.3.2.7	M	M	-
ATNIDRP3	Does this BIS support 'policy based route aggregation'?	5.8.3.2.6.2	O	O	-
ATNIDRP4	Does this BIS support 'policy based route information reduction'?	5.8.3.2.6.5	O	O	-
ATNIDRP5	Does this BIS support aggregation of routes with identical NLRI using 'true route aggregation'?	5.8.3.2.6.3	O.1	O.1	-
ATNIDRP6	Does this BIS support aggregation of routes with identical NLRI using 'route merging'?	5.8.3.2.6.3	O.1	O.1	-
ATNIDRP7	Does this BIS support aggregation of security path attribute information field?	5.8.3.2.6.4	M	M	-

5.8.3.5.3 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 required for this edition of the SARPs and hence it is not reasonable to require mandatory support for this requirement.

5.8.3.5.4 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

5.8.3.5.5 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

5.8.3.5.6 IDRP Decision Process

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

5.8.3.5.7 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

5.8.3.5.8 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.

5.8.3.5.9 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

5.8.3.5.10 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

5.8.3.5.11 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 ^IDRPA G:O	O
NHSN	Does the BIS support generation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	O	IDRPAG: OX ^IDRPA G:O	O
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 ^IDRPA G:O	O
TDLY	Does the BIS support generation of the TRANSIT DELAY attribute?	7.12.8	O	O	IDRPAG: OX ^IDRPA G:O	O
RERR	Does the BIS support generation of the RESIDUAL ERROR attribute?	7.12.9	O	O	IDRPAG: OX ^IDRPA G:O	O
EXP	Does the BIS support generation of the EXPENSE attribute?	7.12.10	O	O	IDRPAG: OX ^IDRPA G:O	O
LQOS G	Does the BIS support generation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	OX	OX	OX

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
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

5.8.3.5.12 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	-
DLEP	Does the BIS support propagation of the DIST_LIST_EXCL attribute?	7.12.6	O	M	IDRPAG: OX ^IDRPAG:M	-

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
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	-

5.8.3.5.13 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 recognise upon receipt the EXT_INFO attribute?	7.12.2	M	M	M	M
NHRSR	Does the BIS recognise upon receipt the NEXT_HOP attribute ?	7.12.4	M	M	M	O

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
DLIR	Does the BIS recognise upon receipt the DIST_LIST_INCL attribute?	7.12.5	M	M	M	M
DLER	Does the BIS recognise upon receipt the DIST_LIST_EXCL attribute?	7.12.6	M	M	M	O
TDLYR	Does the BIS recognise upon receipt the TRANSIT DELAY attribute?	7.12.8	M	M	M	O
RERRR	Does the BIS recognise upon receipt the RESIDUAL ERROR attribute?	7.12.9	M	M	M	O
EXPR	Does the BIS recognise upon receipt the EXPENSE attribute?	7.12.10	M	M	M	O
LQOSR	Does the BIS recognise upon receipt the LOCALLY DEFINED QOS attribute?	7.12.11	M	O	O	O
HRECR	Does the BIS recognise upon receipt the HIERARCHICAL RECORDING attribute?	7.12.12	M	M	M	O
SECR	Does the BIS recognise upon receipt the SECURITY attribute?	7.12.14	M	M	M	M
PRTYR	Does the BIS recognise upon receipt the PRIORITY attribute?	7.12.16	M	M	M	O

5.8.3.5.14 IDRP Timer

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
Ta	KeepAlive timer	11.4, ATN SARPs Ref: 5.8.3.4	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

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
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

5.9 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 the general systems management capabilities specified in 6.3 as the minimum functionality available to a suitably authorised 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.

Note 4.— The details of the mechanisms used to satisfy the requirements for the exchange of management information across management domain boundaries are specified in Section 6 of the ATN SARPs.

— END —