

# **ATN SARPs**

## **Sub-Volume 5 - Internet Communications Service**

*Version 5.1*

**7th June 1996**



## Foreword

In January 1989, the Air Navigation Commission (ANC) expanded the terms of reference of the Secondary Surveillance Radar Improvements and Collision Avoidance Systems Panel (SICASP) to include the development of ICAO material as necessary to permit, to the maximum extent practicable, systems commonality and interoperability between ATS data links, including satellite data links.

The task emerged from the work of the Special Committee on Future Air Navigation Systems (FANS) which emphasized the need for the interchange of digital data over dissimilar aeronautical data links. The committee also recommended that the principles of the International Organization for Standardization (ISO) open systems interconnection (OSI) architecture be applied in developing aeronautical data links in order to provide for their interoperability.

Subsequent studies undertaken by the SICAS Panel resulted in the concept of the aeronautical telecommunication network (ATN) which is intended to support computer-to-computer communications operated by civil aviation authorities and aeronautical operating agencies. At its fourth meeting (March 1989), the SICAS Panel developed a description of the ATN and recommended it be published as an ICAO manual. The first edition of the manual was published in 1991, and the second edition was subsequently developed by the SICAS Panel and recommended for publication at the fifth meeting of the panel, (November 1993), and is expected to be published by ICAO during 1996. The development of the ATN continues with the objective of recommending Standards and Recommended Practices (SARPs) and Guidance Material for the ATN during 1996, for inclusion in Annex 10 at that time.

Following the completion of the work on the ATN Manual (Second Edition) by the SICAS Panel, the Air Navigation Commission transferred the work of developing SARPs and Guidance Material for the ATN to the ATN Panel (ATNP). At its first meeting, (ATNP/1, June 1994), it was agreed that the ATNP develop draft SARPs & guidance material for the "CNS/ATM-1 Package" which was to include the technical provisions for the Internet, the Upper Layers and a limited set of initial Air/Ground and Ground/Ground applications in order to define the initial operational implementation of the ATN. This document, "Sub-Volume 5V" of the ATN SARPs CNS/ATM-1 Package, contains the draft SARPs and Guidance Material for the Internet (i.e. Network & Transport Layers) component of the ATN, as derived from the material in the ATN Manual (second edition) by the ATN Panel Working Group 2 (WG2). Sub-Volume 1 contains introductory material to the ATN SARPs CNS/ATM-1 Package, and additionally "system level" provisions applicable to the Package as a whole. Sub-Volume 2H contains provisions for the initial set of Air/Ground applications i.e. Automatic Dependent Surveillance (ADS), Controller Pilot Data Link Communications (CPDLC), Flight Information Services (FIS) & Context Management (CM). Sub-Volume 3H contains provisions for the initial set of Ground/Ground applications i.e. Inter-Centre Communications (ICC) and Aeronautical Message Handling Service (AHMS). Sub-Volume 4IV contains provisions for the Upper Layer Architecture (ULA) to be supported by ATN SARPs CNS/ATM-1 compliant End Systems.

This document will be maintained and updated by the ATNP WG2 during the development and validation of these draft SARPs and Guidance Material, resulting in validated material expected for recommendation to the ANC at ATNP/2 in November 1996. During this period, this document and its change history will be available to all interested parties.

Please note that the material in this document contains references to the documents of the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU). In using these documents, due attention should be given to their publication dates as shown on the list of references.



## List of Contents

<b>5.1 Introduction</b>	<b>1-1</b>
<b>5.2 Definitions and Concepts</b>	<b>2-1</b>
<b>5.2.1 Objectives and Goals</b>	<b>2-1</b>
<b>5.2.2 Definitions</b>	<b>2-1</b>
5.2.2.1 The ATN Internet	2-1
5.2.2.2 ATN RDs	2-1
5.2.2.2.1 General	2-1
5.2.2.2.2 Fixed RDs	2-1
5.2.2.2.3	2-2
5.2.2.2.3 Mobile RDs	2-2
5.2.2.3 The Ground ATN Internet	2-2
5.2.2.3.1 General	2-2
5.2.2.3.2 ATN Island RDC	2-2
5.2.2.3.3 The Fixed ATN RDC	2-2
5.2.2.4 The Global ATN Backbone	2-2
5.2.2.4.1 General	2-2
5.2.2.4.2 ATN Island Backbone RDCs	2-2
5.2.2.5 The "Home" Domain	2-3
5.2.2.6 Administrative Domains and the ATN	2-3
5.2.2.7 Default Routes	2-3
<b>5.2.3 ATN End Systems</b>	<b>2-4</b>
5.2.3.1 Physical and Data Link Layer	2-4
5.2.3.2 Network Layer	2-4
5.2.3.3 Transport Layer	2-4
5.2.3.4 Upper Layers	2-4
5.2.3.5 Applications	2-4
<b>5.2.4 ATN Routers</b>	<b>2-4</b>
5.2.4.1 ATN Router Classes	2-4
5.2.4.2 Physical and Data Link Layers	2-5
5.2.4.3 Network Layer	2-5
<b>5.2.5 ATN Subnetworks</b>	<b>2-6</b>
5.2.5.1 Requirements for All ATN Subnetworks	2-6
5.2.5.1.2 Byte and Code Independence	2-6
5.2.5.1.3 Subnetwork QoS	2-6
5.2.5.1.4 Subnetwork Addressing	2-6
5.2.5.1.5 Internal Subnetwork Routing	2-6
5.2.5.1.6 Minimum SNSDU Size	2-6
5.2.5.2 Requirements for ATN Mobile Subnetworks	2-6
5.2.5.2.1 General	2-6
5.2.5.2.2 Invocation of Subnetwork Priority	2-6
5.2.5.2.3 Invocation of Subnetwork Quality of Service for Mobile Subnetworks	2-7
5.2.5.2.4 Connection-Mode Subnetwork Service	2-7
5.2.5.2.5 Connectivity Status Changes	2-7
5.2.5.2.6 Segmentation/Reassembly Mechanism	2-7
<b>5.2.6 Quality of Service Concept</b>	<b>2-7</b>
<b>5.2.7 ATN Security Concept</b>	<b>2-7</b>
5.2.7.1 The ATN Security Label	2-8
5.2.7.1.1 General	2-8
5.2.7.1.2 Traffic Types	2-8

5.2.7.1.3 ATSC Class	2-8
5.2.7.1.4 Security Classification	2-8
5.2.7.2 Applications Use of ATN Security Labels	2-8
5.2.7.3 Transport Layer Security	2-9
5.2.7.3.1 In the Connection Mode	2-9
5.2.7.3.2 In the Connectionless Mode	2-9
5.2.7.4 Network Layer Security	2-9
5.2.7.4.1 Service Provider to the Transport Layer	2-9
5.2.7.4.2 Routing Control	2-9
5.2.7.4.3 Protection of the Routing Information Base	2-10
5.2.7.5 Subnetwork Provisions	2-10
<b>5.2.8 ATN Use of Priority</b>	<b>2-10</b>
5.2.8.1 Application Priority	2-11
5.2.8.2 Transport Connection Priority	2-11
5.2.8.3 Connectionless Transport Service Priority	2-11
5.2.8.4 ATN Internet Priority	2-11
5.2.8.5 ATN Subnetwork Priority	2-12
5.2.8.5.1 Connection-Mode Subnetworks	2-12
5.2.8.5.2 Connectionless-Mode Subnetworks	2-12
<b>5.3 ATN Routing</b>	<b>3-1</b>
<b>5.3.1 Introduction</b>	<b>3-1</b>
5.3.1.1 Scope	3-1
5.3.1.2	3-1
5.3.1.2 Applicability of Requirements	3-1
<b>5.3.2 Service Provided by an ATN Router</b>	<b>3-1</b>
5.3.2.1 General	3-1
5.3.2.2 Forwarding CLNP NPDUs	3-2
5.3.2.2.1 General	3-2
5.3.2.2.2 Forwarding a CLNP NPDU when no Security Parameter is present in the PDU Header	3-2
5.3.2.2.3 Forwarding a CLNP NPDU when a Security Parameter is present in the PDU Header	3-2
5.3.2.2.3.1 General	3-2
5.3.2.2.3.2 ATN Operational Communications Traffic Type - ATSC Traffic Category	3-2
5.3.2.2.3.2.1 No Traffic Type Policy Preference	3-2
5.3.2.2.3.2.2 ATSC Class Specified	3-3
5.3.2.2.3.3 ATN Operational Communications Traffic Type - AOC Traffic Category	3-3
5.3.2.2.3.3.1 No Traffic Type Policy Preference	3-3
5.3.2.2.3.3.2 Air/Ground Subnetwork Type Specified	3-4
5.3.2.2.3.3.3 Air/Ground Subnetwork Order of Preference Specified	3-4
5.3.2.2.3.4 ATN Administrative Communications Traffic Type	3-5
5.3.2.2.3.5 ATN Systems Management Communications Traffic Type	3-5
<b>5.3.3 The Deployment of ATN Components</b>	<b>3-5</b>
5.3.3.1 Interconnection of ATN RDs	3-5
5.3.3.1.1 General	3-5
5.3.3.1.2 Interconnection between Members of an ATN Island Backbone RDC	3-6
5.3.3.1.3 Interconnection between Members of an ATN Island Backbone RDC and other ATN RDs within the ATN Island	3-6
5.3.3.1.4 Interconnection of ATN Islands	3-6
5.3.3.1.5 Interconnection of Mobile and Fixed RDs	3-6
5.3.3.1.6 Interconnection of ATN RDs and non-ATN RDs	3-6
<b>5.3.4 Ground/Ground Interconnection</b>	<b>3-7</b>
5.3.4.1 Interconnection Scenarios	3-7
5.3.4.2 Ground/Ground Route Initiation	3-7
5.3.4.3 Ground/Ground Routing Information Exchange	3-7
5.3.4.4 Ground/Ground Route Termination	3-8

<b>5.3.5 Air/Ground Interconnection</b>	<b>3-8</b>
5.3.5.1 Interconnection Scenarios	3-8
5.3.5.2 Air/Ground Route Initiation	3-8
5.3.5.2.1 General	3-8
5.3.5.2.2 Route Initiation Procedures for a Responding ATN Router	3-9
5.3.5.2.2.1 General	3-10
5.3.5.2.2.2 Emergency Use of a Mobile Subnetwork	3-10
5.3.5.2.3 Air-Initiated Route Initiation	3-10
5.3.5.2.3.1 Airborne Router Procedures for use of an ISO/IEC 8208 Mobile Subnetwork that does not Provide Information on Subnetwork Connectivity	3-10
5.3.5.2.3.1.1 General	3-10
5.3.5.2.3.1.2 Call Request Failure	3-11
5.3.5.2.3.2 Airborne Router Procedures for use of an ISO/IEC 8208 Mobile Subnetwork that does Provide Connectivity Information	3-11
5.3.5.2.4 Ground-Initiated Route Initiation	3-11
5.3.5.2.5 Air or Ground-Initiated Route Initiation	3-12
5.3.5.2.6 Exchange of Configuration Information using the ISO/IEC 9542 ISH PDU	3-12
5.3.5.2.7 Validation of the Received NET	3-13
5.3.5.2.8 Determination of the Routing Information Exchange Procedure by an Air/Ground Router	3-13
5.3.5.2.9 Determination of the Routing Information Exchange Procedure by an Airborne Router	3-13
5.3.5.2.10 Establishment of a BIS-BIS Connection	3-13
5.3.5.2.11 Exchange of Routing Information using IDRPs	3-14
5.3.5.2.12 Procedures for the Optional Non-Use of IDRPs over an Air/Ground Data Link	3-14
5.3.5.2.12.1 Air/Ground Router	3-14
5.3.5.2.12.2 Airborne Router	3-15
5.3.5.2.13 Air/Ground Route Termination	3-15
5.3.5.2.14 APRL for Air/Ground Route Initiation	3-17
5.3.5.2.14.1 General	3-17
5.3.5.2.14.2 Airborne Router - Subnetwork Connection Responder	3-17
5.3.5.2.14.3 Airborne Router - Subnetwork Connection Initiator	3-18
5.3.5.2.14.4 Air/Ground Router - Subnetwork Connection Responder	3-18
5.3.5.2.14.5 Air/Ground Router - Subnetwork Connection Initiator	3-19
5.3.5.2.14.6 Termination Procedures	3-20
<b>5.3.6 Handling Routing Information</b>	<b>3-21</b>
<b>5.3.7 Policy Based Selection of Routes for Advertisement to Adjacent RDs</b>	<b>3-21</b>
5.3.7.1 Routing Policy Requirements for Members of an ATN Island Backbone RDC	3-21
5.3.7.1.1 General	3-21
5.3.7.1.2 Adjacent ATN RDs within the Backbone RDC	3-21
5.3.7.1.3 All other ATN RDs within the ATN Island	3-22
5.3.7.1.4 Mobile RDs	3-22
5.3.7.1.5 ATN RDs in other ATN Islands	3-23
5.3.7.2 Routing Policy Requirements for a Mobile RD	3-23
5.3.7.3 Routing Policy Requirements for an ATN TRD that is not a Member of the ATN Island Backbone RDC	3-23
5.3.7.3.1 General	3-23
5.3.7.3.2 Adjacent ATN RDs that are Members of the ATN Island's Backbone RDC	3-24
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	3-24
5.3.7.3.4 Mobile RDs	3-25
5.3.7.4 The Routing Policy for a Fixed ATN ERD	3-25
<b>5.3.8</b>	<b>3-25</b>
<b>5.4 Network and Transport Addressing Specification</b>	<b>4-1</b>
<b>5.4.1 Introduction</b>	<b>4-1</b>
5.4.1.1 Addressing Plan Scope	4-1

5.4.1.2 Addressing Plan Applicability	4-1
<b>5.4.2 Network Layer Addressing</b>	<b>4-1</b>
5.4.2.1 General	4-1
5.4.2.1.1	4-1
5.4.2.1.2 Conformance to ISO Standards	4-2
5.4.2.1.3 ISO Address Format Definition	4-2
5.4.2.1.4 Subnetwork Independence	4-2
5.4.2.1.5 Address Mapping	4-2
5.4.2.1.6	4-2
5.4.2.1.6 Definition of a Network Entity Title	4-2
5.4.2.1.7 Network Addressing Domains	4-2
5.4.2.2	4-3
5.4.2.1.8	4-3
5.4.2.1.8	4-3
5.4.2.1.8	4-3
5.4.2.2 Abstract Syntax Provisions	4-3
5.4.2.2.1 General	4-3
5.4.2.2.2 Format Definition	4-4
5.4.2.2.3 Field Abstract Syntax	4-4
5.4.2.2.4 Field Syntax Construction	4-4
5.4.2.2.5 Reserved Values in Address Fields	4-4
5.4.2.2.6	4-4
5.4.2.3 Encoding Provisions	4-4
5.4.2.3.1 Field Encoding Definition	4-4
5.4.2.3.2 Fill Bits	4-4
5.4.2.3.3 Field Size	4-5
5.4.2.3.4 Encoding of Decimal Syntax	4-5
5.4.2.3.5 Encoding of Hexadecimal Syntax	4-5
5.4.2.3.6 Encoding of Alphanumeric Syntax	4-5
5.4.2.3.7 Encoding of Identifier Syntax	4-5
5.4.2.4 Address Field Provisions	4-5
5.4.2.4.1 Authority/Format Identifier	4-5
5.4.2.4.1.1 Format	4-6
5.4.2.4.1.2 Administration	4-6
5.4.2.4.1.3 Range	4-6
5.4.2.4.1.4 Encoding	4-6
5.4.2.4.2 Initial Domain Identifier	4-6
5.4.2.4.2.1 Format	4-6
5.4.2.4.2.2 Administration	4-6
5.4.2.4.2.3 Range	4-6
5.4.2.4.2.4 Encoding	4-6
5.4.2.4.3 Version Identifier	4-6
5.4.2.4.3.1 Format	4-6
5.4.2.4.3.2 Administration	4-6
5.4.2.4.3.3 Range	4-6
5.4.2.4.3.4 Encoding	4-7
5.4.2.4.4 Administration Identifier	4-7
5.4.2.4.4.1 Format	4-7
5.4.2.4.4.1.1 General	4-7
5.4.2.4.4.1.2 ATSC Format	4-7
5.4.2.4.4.1.3 AINSC Format	4-7
5.4.2.4.4.2 Administration	4-7
5.4.2.4.4.2.1 General	4-7
5.4.2.4.4.2.2 ATSC Administration	4-7
5.4.2.4.4.2.3 AINSC Administration	4-7
5.4.2.4.4.3 Range	4-7
5.4.2.4.4.3.1 General	4-7



5.4.2.4.4.3.2 ATSC Range	4-7
5.4.2.4.4.3.3 AINSC Range	4-8
5.4.2.4.4.4 Encoding	4-8
5.4.2.4.5 Routing Domain Format	4-8
5.4.2.4.6 Administrative Region Selector	4-8
5.4.2.4.6.1 Format	4-8
5.4.2.4.6.1.1 General	4-8
5.4.2.4.6.1.2 ATSC-Fixed Format	4-8
5.4.2.4.6.1.3 AINSC-Fixed Format	4-8
5.4.2.4.6.1.4 Mobile Format	4-8
5.4.2.4.6.2 Administration	4-8
5.4.2.4.6.2.1 General	4-8
5.4.2.4.6.2.2 ATSC-Fixed Administration	4-8
5.4.2.4.6.2.3 AINSC-Fixed Administration	4-8
5.4.2.4.6.2.4 Mobile Administration	4-8
5.4.2.4.6.3 Range	4-9
5.4.2.4.6.4 Encoding	4-9
5.4.2.4.6.5 Default Value	4-9
5.4.2.4.7 Location Identifier	4-9
5.4.2.4.7.1 Format	4-9
5.4.2.4.7.1.1 General	4-9
5.4.2.4.7.1.2 ATSC Format	4-9
5.4.2.4.7.1.3 AINSC Format	4-9
5.4.2.4.7.1.4 Mobile Format	4-9
5.4.2.4.7.2 Administration	4-9
5.4.2.4.7.3 Range	4-9
5.4.2.4.7.4 Encoding	4-9
5.4.2.4.7.5 Default Value	4-9
5.4.2.4.8 System Identifier	4-9
5.4.2.4.8.1 Format	4-9
5.4.2.4.8.2 Administration	4-10
5.4.2.4.8.3 Range	4-10
5.4.2.4.8.4 Encoding	4-10
5.4.2.4.9 NSAP Selector	4-10
5.4.2.4.9.1 Format	4-10
5.4.2.4.9.2 Administration	4-10
5.4.2.4.9.2.1 SEL field values in the range [01-fd] shall be assigned and administered by the authority designated in the ADM field.	4-10
5.4.2.4.9.3 Range	4-10
5.4.2.4.9.4 Encoding	4-10
<b>5.4.3 Transport Layer Addressing</b>	<b>4-10</b>
5.4.3.1 General	4-10
5.4.3.2 ATN TSAP Selector	4-10
5.4.3.3 Format	4-10
5.4.3.4 Administration	4-10
5.4.3.5 Range	4-10
5.4.3.6 Encoding	4-10
<b>5.5 Transport Service and Protocol Specification</b>	<b>5-1</b>
<b>5.5.1 General</b>	<b>5-1</b>
5.5.1.1 Overview	5-1
5.5.1.2	5-1
5.5.1.2 Transport Service Description	5-1
5.5.1.3 Transport Service Access Point Addresses	5-2
5.5.1.4	5-2
5.5.1.4 Exchange of Transport-Selector parameters	5-2

<b>5.5.2 Connection Mode Transport Layer Operation</b>	<b>5-2</b>
5.5.2.1 Connection Mode Transport Service Primitives	5-2
5.5.2.2 ATN Specific Requirements	5-2
5.5.2.3 Connection Mode Transport Quality of Service	5-3
5.5.2.3.1 Connection Mode Transport Priority	5-3
5.5.2.3.2 Connection Mode Transport Security	5-3
5.5.2.4 Encoding of Transport Protocol Data Units	5-3
5.5.2.4.1 General	5-4
5.5.2.4.2 Encoding of the Acknowledgment Time Parameter	5-4
5.5.2.5 Transport Layer Congestion Avoidance	5-4
5.5.2.5.1 General	5-4
5.5.2.5.2 Advertised Window	5-4
5.5.2.5.2.1 General	5-4
5.5.2.5.2.2 Initialisation of the Advertised Window	5-4
5.5.2.5.3 Receiving Transport Entity Congestion Avoidance	5-4
5.5.2.5.3.1 General	5-4
5.5.2.5.3.2 Start of Update Phase	5-4
5.5.2.5.3.3 Ignoring Congestion Information	5-5
5.5.2.5.3.4 Sampling Congestion Information	5-5
5.5.2.5.3.5 Action Upon the End of the Update Phase	5-5
5.5.2.5.4 Recommended Algorithm Values	5-5
5.5.2.6 Use of the ATN Network Service	5-5
5.5.2.6.1 Use of the N-UNITDATA Request	5-5
5.5.2.6.1.1 General	5-5
5.5.2.6.1.2 NS-user-data	5-5
5.5.2.6.1.3 Network Service Access Point Addresses	5-6
5.5.2.6.1.4 Network Quality of Service	5-6
5.5.2.6.1.4.1 General	5-6
5.5.2.6.1.4.2 Network Layer Priority	5-6
5.5.2.6.1.4.3 Network Layer Security	5-6
5.5.2.6.2 Use of the N-UNITDATA Indication	5-6
5.5.2.6.2.1 General	5-6
5.5.2.6.2.2 NS-user-data	5-6
5.5.2.6.2.3	5-6
5.5.2.6.2.3	5-6
5.5.2.6.2.2.1	5-6
5.5.2.7 Connection Mode Transport APRL	5-6
5.5.2.7.1 Mandatory and Optional Functions	5-6
5.5.2.7.1.1 General	5-6
5.5.2.7.1.2 Protocol Implementation	5-7
5.5.2.7.1.2.1 Classes Implemented	5-7
5.5.2.7.1.3 Initiator/Responder Capability for Protocol Classes 0-4	5-9
5.5.2.7.1.4.1 Supported Functions for Class 4 (C4 or C4L::)	5-11
5.5.2.7.1.6 Supported Parameters of Issued TPDU	5-14
5.5.2.7.1.6.1 Parameter Values for CR TPDU (C4L::)	5-14
5.5.2.7.1.6.2 Supported parameters for Class 4 TPDU (C4L::)	5-14
5.5.2.7.1.7.1 TPDU in Class 4 (C4L::)	5-19
5.5.2.7.1.8 User Data in Issued TPDU	5-19
5.5.2.7.1.8.1 Class 4 (C4 or C4L::)	5-19
5.5.2.7.1.10 Negotiation	5-20
5.5.2.7.1.10.1 Class Negotiation - Initiator	5-20
5.5.2.7.1.10.2 Class negotiation - responder side	5-20
5.5.2.7.1.10.5 Expedited data Transport service	5-23
5.5.2.7.1.10.6 Non-use of Checksum (C4L and T4F29::)	5-23
5.5.2.7.1.10.8 Use of Request Acknowledgement	5-24
5.5.2.7.1.11 Error Handling	5-24
5.5.2.7.1.11.1 Action on Detection of a Protocol Error	5-24
5.5.2.7.1.12 Class 4 Timers and Protocol Parameters	5-26

<b>5.5.3 Connectionless Mode Transport Protocol Operation</b>	<b>5-28</b>
5.5.3.1 Connectionless Mode Transport Protocol Overview	5-28
5.5.3.2 Connectionless Mode Transport Service Primitives	5-28
5.5.3.2.1 T-UNITDATA Request	5-28
5.5.3.2.2 T-UNITDATA Indication	5-28
5.5.3.3 ATN Connectionless Mode Transport Quality of Service Parameters	5-28
5.5.3.3.1 General	5-28
5.5.3.3.2 Priority	5-28
5.5.3.3.3 Security	5-28
5.5.3.3.4	5-28
5.5.3.4 Encoding of Transport Protocol Data Units	5-28
5.5.3.5 Use of the ATN Network Service	5-28
5.5.3.5.1	5-28
5.5.3.5.1 Use of the N-UNITDATA Request	5-28
5.5.3.5.1.1 General	5-28
5.5.3.5.1.2 NS-user-data	5-28
5.5.3.5.1.3 Network Service Access Point Addresses	5-29
5.5.3.5.1.4 Network Quality of Service	5-29
5.5.3.5.1.4.1 General	5-29
5.5.3.5.1.4.2 Network Layer Priority	5-29
5.5.3.5.1.4.3 Network Layer Security	5-29
5.5.3.5.2 Use of the N-UNITDATA Indication	5-29
5.5.3.5.2.1	5-29
5.5.3.5.2.1 Network Quality of Service	5-29
5.5.3.6 ATN Connectionless Mode Transport APRL	5-29
<b>5.6 Internetwork Service and Protocol Specification</b>	<b>6-1</b>
<b>5.6.1 Introduction</b>	<b>6-1</b>
5.6.1.1 Scope	6-1
5.6.1.2 Applicability of Requirements	6-1
<b>5.6.2 ATN Specific Features</b>	<b>6-1</b>
5.6.2.1 Purpose of ATN Specific Features	6-1
5.6.2.2 The Security Function	6-2
5.6.2.2.1 General	6-2
5.6.2.2.2 Encoding of the Security Parameter	6-2
5.6.2.2.3 Security Registration ID Length	6-2
5.6.2.2.4 Security Registration ID	6-2
5.6.2.2.5 Security Information Length	6-2
5.6.2.2.6 Security Information	6-2
5.6.2.2.6.1 General	6-2
5.6.2.2.6.2 Encoding of the Security Information Field	6-3
5.6.2.2.6.3 Security Tag Set Name Length	6-3
5.6.2.2.6.4 Security Tag Set Name	6-3
5.6.2.2.6.5 Tag Set Length	6-3
5.6.2.2.6.6 Security Tag	6-3
5.6.2.2.6.7 Encoding of the Tag Set for Traffic Type and Associated Routing Policies	6-3
5.6.2.2.6.8	6-4
5.6.2.2.6.8 Encoding of the Tag Set for Security Classification	6-5
5.6.2.3 Management of Network Priority	6-5
5.6.2.4 Congestion Management	6-5
5.6.2.4.1 Setting of the congestion experienced flag	6-5
5.6.2.4.2 Forwarding congestion information to the receiving NS-User	6-5
5.6.2.4.3 Required algorithm values	6-5
<b>5.6.3 ATN Specific Requirements for ISO/IEC 8473</b>	<b>6-6</b>
5.6.3.1	6-6
5.6.3.1.1	6-6

5.6.3.1.1	6-6
5.6.3.1.1	6-6
5.6.3.1.1	6-6
5.6.3.1.1	6-6
5.6.3.1 Segmentation Function	6-6
5.6.3.1.5	6-6
5.6.3.1.5	6-6
5.6.3.1.5	6-6
5.6.3.1.5	6-6
5.6.3.2	6-6
5.6.3.1.5	6-6
5.6.3.2 Security Function	6-6
5.6.3.2.1	6-7
5.6.3.2.1	6-7
5.6.3.2.1	6-7
5.6.3.2.1	6-7
5.6.3.2.1	6-7
5.6.3.3 Echo Request Function	6-7
5.6.3.4 Network Priority	6-7
5.6.3.4.1	6-7
5.6.3.4.1	6-7
<b>5.6.4 APRLs</b>	<b>6-8</b>
5.6.4.1 General	6-8
5.6.4.2 Support of ATN-Specific Network Layer features	6-8
5.6.4.3 Major Capabilities	6-8
5.6.4.4 End Systems - Supported Functions	6-9
5.6.4.5 End Systems - Supported NPDUs	6-11
5.6.4.12.2 Quality of Service Maintenance Function	6-25
5.6.4.19 Subnetwork Dependent Convergence Functions SNDCF for use with ISO/IEC 8802-2 Subnetworks - Functions	6-36
5.6.4.20 Subnetwork Dependent Convergence Functions SNDCF for use with ISO/IEC 8802-2 Subnetworks - Multi Layer Dependencies	6-36
5.6.4.23 Subnetwork Dependent Convergence Functions SNDCF for use with ISO/IEC 8208 Subnetworks - ISO/IEC 8208 SNDCF Timers	6-38

## 5.7 Specification of Subnetwork Dependant Convergence

<b>Functions</b>	<b>7-1</b>
<b>5.7.1 Scope and Applicability</b>	<b>7-1</b>
<b>5.7.2</b>	<b>7-1</b>
<b>5.7.2 Service Provided by the SNDCF</b>	<b>7-1</b>
5.7.2.1 Subnetwork Service Primitive Parameters	7-2
5.7.2.1.1 Subnetwork Point of Attachment (SNPA) Addresses	7-2
5.7.2.1.2 Subnetwork Priority	7-2
5.7.2.1.3 Subnetwork Quality of Service (SNQoS)	7-2
5.7.2.1.4 Subnetwork Service Userdata	7-3
5.7.2.2	7-3
<b>5.7.3</b>	<b>7-3</b>
<b>5.7.3 Convergence Provisions for ISO/IEC 8208 Subnetworks</b>	<b>7-3</b>
5.7.3.1 General	7-3
5.7.3.2 Service Coordination between the SNDCF and SN-Service-Users	7-3
5.7.3.3 Service Coordination between the SNDCF and ISO/IEC 8208 Subnetwork Providers	7-3
5.7.3.3.1 General	7-3
5.7.3.3.2 Transit Delay	7-4
5.7.3.3.2.1 General	7-4

5.7.3.3.2.2 Transit Delay Selection and Indication Facility	7-4
5.7.3.3.3 Residual Error Probability	7-4
5.7.3.3.4 Economic cost	7-4
5.7.3.3.5 Protection against Unauthorized Access	7-4
5.7.3.3.6 Throughput	7-5
5.7.3.3.6.1 General	7-5
5.7.3.3.6.2 Throughput Class Negotiation Facility	7-5
5.7.3.3.7 Priority	7-5
5.7.3.3.7.1 General	7-5
5.7.3.3.7.2 Use of the Priority Facility	7-5
5.7.3.4 Convergence Provisions for ISO/IEC 8208 General Topology Subnetworks	7-5
5.7.3.5 Convergence Provisions for ISO/IEC 8208 Mobile Subnetworks	7-6
5.7.3.5.1 General	7-6
5.7.3.5.2	7-6
5.7.3.5.2 Conformance	7-6
5.7.3.5.3 Call Setup	7-6
5.7.3.5.3.1 General	7-6
5.7.3.5.3.2 Call Setup Mechanism and Timing	7-6
5.7.3.5.3.3 Call Setup Functions	7-6
5.7.3.5.3.4 Format of Call Request and Call Accept User Data	7-7
5.7.3.5.3.4.1 Call Request User Data	7-7
5.7.3.5.3.4.2 Call Accept User Data	7-8
5.7.3.5.3.5 Application of Compression Procedures	7-8
5.7.3.5.3.6 Call acceptance and compression negotiation	7-9
5.7.3.5.3.7 Call rejection	7-9
5.7.3.5.4 Local Directory Initialization	7-9
5.7.3.5.5 Action following an SN-UNITDATA Request	7-10
5.7.3.5.5.1 General	7-10
5.7.3.5.5.2 Identification of Network Layer Protocol	7-10
5.7.3.5.5.3 Identification of Option Parameter and Local Directory Look-up	7-10
5.7.3.5.5.4 Establishing a New Local Reference	7-11
5.7.3.5.5.5 Reference Cancellation Option	7-12
5.7.3.5.5.6 Transfer of the Modified ISO/IEC 8473 PDU	7-12
5.7.3.5.6 Compression of SN-Userdata	7-12
5.7.3.5.6.1 General	7-12
5.7.3.5.6.2 Initial DT PDU Compression	7-12
5.7.3.5.6.2.1 General	7-12
5.7.3.5.6.2.2 Type Field	7-12
5.7.3.5.6.2.3 PDU Priority Field	7-12
5.7.3.5.6.2.4 PDU Lifetime Field	7-12
5.7.3.5.6.2.5 P bit Field	7-12
5.7.3.5.6.2.6 Q bit Field	7-13
5.7.3.5.6.2.7 R bit Field	7-13
5.7.3.5.6.2.8 S/T, CE, T/C, E/T, and E/C Fields	7-13
5.7.3.5.6.2.9 EXP, Local-REF/A and Local-REF/B Fields	7-13
5.7.3.5.6.2.10 PDU Identifier	7-13
5.7.3.5.6.2.11 PDU Segment Offset	7-14
5.7.3.5.6.2.12 PDU Total Length	7-14
5.7.3.5.6.2.13 Network Service Data Unit Field	7-14
5.7.3.5.6.3 Derived DT PDU Compression	7-14
5.7.3.5.6.3.1 General	7-14
5.7.3.5.6.3.2 Type Field	7-14
5.7.3.5.6.3.3 PDU Priority Field	7-15
5.7.3.5.6.3.4 PDU Lifetime Field	7-15
5.7.3.5.6.3.5 P bit Field	7-15
5.7.3.5.6.3.6 Q bit Field	7-15
5.7.3.5.6.3.7 S/T, CE, T/C, E/T, and E/C Fields	7-15
5.7.3.5.6.3.8 EXP, Local-REF/A and Local-REF/B Fields	7-15

5.7.3.5.6.3.9 PDU Identifier Field	7-15
5.7.3.5.6.3.10 PDU Segment Offset Field	7-15
5.7.3.5.6.3.11 PDU Total Length Field	7-15
5.7.3.5.6.4 Error Report PDU Compression	7-15
5.7.3.5.6.4.1 General	7-15
5.7.3.5.6.4.2 PDU Type Field	7-15
5.7.3.5.6.4.3 PDU Priority Field	7-15
5.7.3.5.6.4.4 PDU Lifetime Field	7-15
5.7.3.5.6.4.5 P bit Field	7-15
5.7.3.5.6.4.6 Q bit Field	7-15
5.7.3.5.6.4.7 S/T, CE , T/C, E/T and E/C Fields	7-15
5.7.3.5.6.4.8 EXP, Local-REF/A, Local-REF/B Fields	7-16
5.7.3.5.6.4.9 Discard Reason Field	7-16
5.7.3.5.6.4.10 Header of Discarded NPDU Field	7-16
5.7.3.5.6.4.11 Transfer of Compressed ISO/IEC 8473 PDUs	7-16
5.7.3.5.7 Processing of Packets Received from the Subnetwork Service Provider	7-16
5.7.3.5.7.1 Initial Processing of NPDU	7-16
5.7.3.5.7.2 Incoming ISO/IEC 8473 PDU with Uncompressed Header	7-17
5.7.3.5.7.2.1 General	7-17
5.7.3.5.7.2.2 Processing of Unmodified ISO/IEC 8473 PDUs	7-17
5.7.3.5.7.2.3 Processing of Modified ISO/IEC 8473 PDUs	7-17
5.7.3.5.7.3 Incoming Compressed Data PDU	7-17
5.7.3.5.7.3.1 General	7-17
5.7.3.5.7.3.2 Fixed Part	7-18
5.7.3.5.7.3.3 Address Part	7-19
5.7.3.5.7.3.4 Segmentation Part	7-19
5.7.3.5.7.3.5 Options Part	7-19
5.7.3.5.7.3.6 Data Part	7-20
5.7.3.5.7.4 Incoming Compressed Error Report PDU	7-20
5.7.3.5.7.4.1 General	7-20
5.7.3.5.7.4.2 Fixed Part	7-20
5.7.3.5.7.4.3 Address Part	7-20
5.7.3.5.7.4.4 Options Part	7-20
5.7.3.5.7.4.5 Reason for Discard	7-20
5.7.3.5.7.4.6 Error Report Data Part	7-20
5.7.3.5.7.5 Incoming SNDCF Error Report	7-20
5.7.3.5.8 SNDCF Error Report	7-20
5.7.3.5.9 Local Reference Cancellation Option	7-21
5.7.3.5.9.1 General	7-21
5.7.3.5.9.2 The Cancellation Request PDU	7-21
5.7.3.5.9.3 The Cancellation Accept PDU	7-22
5.7.3.5.10 Call Clearing Provisions	7-22
5.7.3.5.11 Call Reset Provisions	7-23
<b>5.7.4 Convergence Provisions for ISO/IEC 8802-2 Broadcast Subnetworks</b>	<b>7-24</b>
<b>5.7.5 Convergence Provisions for Common ICAO Data Interchange Network (CIDIN)</b>	<b>7-24</b>
5.7.5.1 General Considerations	7-24
5.7.5.2	7-24
5.7.5.2 SN-UNITDATA Request and Indication Primitives	7-24
5.7.5.3 SN Source Address	7-24
5.7.5.4 SN Destination Address	7-24
5.7.5.5 SN Quality of Service	7-24
5.7.5.6 SN Priority	7-24
5.7.5.7 SNS-Userdata	7-24
<b>5.7.6 ATN NSAP Compression Algorithm (ACA)</b>	<b>7-24</b>
5.7.6.1 General Overview	7-24
5.7.6.2 Address Length Determination	7-24

5.7.6.3 Compressed Address Structure	7-25
5.7.6.3.1 General	7-25
5.7.6.3.2 Address Header Octets	7-25
5.7.6.3.2.1 General	7-25
5.7.6.3.2.2 First Header Octet	7-25
5.7.6.3.2.2.1 General	7-25
5.7.6.3.2.2.2 IDRP Subfield	7-25
5.7.6.3.2.2.3 FP Subfield	7-26
5.7.6.3.2.2.4 LEN/SEL Subfield	7-26
5.7.6.3.2.2.5 CVER Subfield	7-26
5.7.6.3.2.3 Second Header Octet	7-26
5.7.6.3.2.3.1 General	7-26
5.7.6.3.2.3.2 ADMF Subfield	7-26
5.7.6.3.2.3.3 T/I Subfield	7-27
5.7.6.3.2.3.4 F/M Subfield	7-27
5.7.6.3.2.3.5 ARSD Subfield	7-27
5.7.6.3.2.3.6 LOCD Subfield	7-27
5.7.6.3.2.3.7 SYS6 Subfield	7-27
5.7.6.3.2.3.8 SYS5 Subfield	7-27
5.7.6.3.2.3.9 SYS4 Subfield	7-27
5.7.6.3.3 Compressed ADM Field	7-27
5.7.6.3.4 Variable Fields	7-28
5.7.6.4 Compressed Address Marker	7-28
5.7.6.4.1 General	7-28
5.7.6.4.2 Normal Address Case	7-28
5.7.6.4.3 Embedded Address Marker Case	7-28
5.7.6.5 Compression Algorithm	7-28
5.7.6.5.1 General	7-28
5.7.6.5.2 Address Encoding Process	7-28
5.7.6.5.2.1 General	7-28
5.7.6.5.2.2 Encoding Address Length	7-29
5.7.6.5.2.3 Encoding the AFI and IDI Fields	7-29
5.7.6.5.2.4 Encoding the VER Field	7-29
5.7.6.5.2.5 Encoding the ADM Field	7-29
5.7.6.5.2.6 Encoding the RDF Field	7-30
5.7.6.5.2.7 Encoding the ARS Field	7-30
5.7.6.5.2.8 Encoding the LOC Field	7-30
5.7.6.5.2.9 Encoding the SYS Field	7-30
5.7.6.5.2.10 Encoding the SEL Field	7-30
5.7.6.5.3 Compression Logic Flow	7-30
5.7.6.6 Decompression Algorithm	7-31
5.7.6.6.1 General	7-31
5.7.6.6.2 Address Decoding Process	7-31
5.7.6.6.2.1 General	7-31
5.7.6.6.2.2 Decoding Address Length	7-31
5.7.6.6.2.3 Decoding the AFI and IDI Fields	7-31
5.7.6.6.2.4 Decoding the VER Fields	7-31
5.7.6.6.2.5 Decoding the ADM Fields	7-32
5.7.6.6.2.6 Decoding the RDF Fields	7-32
5.7.6.6.2.7 Decoding the ARS Fields	7-32
5.7.6.6.2.8 Decoding the LOC Fields	7-32
5.7.6.6.2.9 Decoding the SYS Fields	7-32
5.7.6.6.2.10 Decoding the SEL Fields	7-32
5.7.6.6.3 Decompression Logic Flow	7-33
<b>5.7.7 ATN SNDCF Protocol Requirements List</b>	<b>7-34</b>
<b>5.7.8 ATN Requirements for Mobile SINDCFs</b>	<b>7-34</b>
5.7.8.1 Major Capabilities	7-34

5.7.8.2 Call Setup and Clearing Procedures	7-34
5.7.8.3 Negotiation of Compression Algorithm	7-36
5.7.8.4 Local Reference Header Compression	7-36
5.7.8.5 Local Reference Cancellation	7-38
5.7.8.6 ICAO Address Compression Algorithm	7-38
5.7.8.7.1 Call Request User Data	7-40
5.7.8.7.2 Call Accept User Data	7-40
5.7.8.7.3 Modified ISO/IEC 8473 NPDU	7-40
5.7.8.7.5 Compressed Derived PDU	7-41
5.7.8.7.7 SNDCEF Error Report PDU	7-42
5.7.8.7.8 Cancellation Request	7-42
5.7.8.7.9 Cancellation Accept	7-43

## **5.8 Routing Information Exchange Specification** **8-1**

### **5.8.1 Introduction** **8-1**

5.8.1.1 Scope	8-1
5.8.1.2 Applicability of Requirements	8-1

### **5.8.2 End System to Intermediate System Routing Information Exchange Protocol (ES-IS) over Mobile Subnetworks** **8-1**

5.8.2.1 General	8-1
5.8.2.2	8-1
5.8.2.2 ATN Protocol Requirements List - ISO/IEC 9542	8-1

### **5.8.3 Intermediate System to Intermediate System Inter-Domain Routing Information Exchange Protocol** **8-6**

5.8.3.1 General	8-6
5.8.3.2 ATN Specific Features	8-6
5.8.3.2.1 Purpose of ATN Specific Features	8-6
5.8.3.2.2 Use of the Security Path Attribute	8-6
5.8.3.2.3 Encoding of the Security Path Attribute Security Information Field	8-6
5.8.3.2.3.1 General	8-6
5.8.3.2.3.2 Encoding of the Air/Ground Subnetwork Type Security Tag Set	8-6
5.8.3.2.3.3 Encoding of the ATSC Class Security Tag Set	8-7
5.8.3.2.4 Update of Security Information	8-7
5.8.3.2.4.1 The Air/Ground Subnetwork Type	8-7
5.8.3.2.4.2 The ATSC Class	8-8
5.8.3.2.4.3 The Security Classification	8-9
5.8.3.2.5 Route Selection	8-9
5.8.3.2.6 Route Aggregation and Route Information Reduction	8-10
5.8.3.2.6.1 General	8-10
5.8.3.2.6.2 Policy Based Route Aggregation	8-10
5.8.3.2.6.3 Aggregation of Routes in the Same Loc-RIB with Identical NLRI	8-11
5.8.3.2.6.4 Aggregation of the Security Path Attribute Information Field	8-11
5.8.3.2.6.5 Route Information Reduction	8-12
5.8.3.2.7 Frequency of Route Advertisement	8-12
5.8.3.2.8 Interpretation of Route Capacity	8-12
5.8.3.2.9 Network Layer Reachability Information	8-12
5.8.3.2.9.1 General	8-13
5.8.3.2.9.2 NSAP Address Prefix Alignment	8-13
5.8.3.2.10 BISPDU Authentication	8-13
5.8.3.2.11 Restrictions on Route Advertisement	8-13
5.8.3.2.12 RIB_Att Support	8-13
5.8.3.2.13 Additional Update PDU Error Handling	8-14
5.8.3.2.14 CLNP Data PDU Parameters	8-14
5.8.3.3 Compliance with ISO/IEC 10747	8-15
5.8.3.3.1 General	8-15

5.8.3.3.2 ISO/IEC 10747 Mandatory Requirements	8-15
--	------



5.8.3.3.2.1 Airborne Router	8-15
5.8.3.3.2.2 Ground Router	8-15
5.8.3.3.3 ISO/IEC 10747 Optional Requirements	8-15
5.8.3.4 APRLs	8-15
5.8.3.4.1 General	8-15
5.8.3.4.2 ATN Specific Protocol Requirements	8-16
5.8.3.4.3 IDRP General	8-16
5.8.3.4.4 IDRP Update Send Process	8-17
5.8.3.4.5 IDRP Update Receive Process	8-17
5.8.3.4.6 IDRP Decision Process	8-18
5.8.3.4.7 IDRP Receive	8-18
5.8.3.4.8 Peer Entity Authentication	8-18
5.8.3.4.9 IDRP CLNS Forwarding	8-19
5.8.3.4.10 IDRP Receive Process	8-19
5.8.3.4.11 IDRP Optional Transitive Attributes	8-19
5.8.3.4.12 Generating Well-Known Discretionary Attributes	8-20
5.8.3.4.15 IDRP Timer	8-23
<b>5.9 Systems Management Provisions</b>	<b>9-1</b>
<b>5.9.1 Introduction</b>	<b>9-1</b>

## 5.1. INTRODUCTION

*Note 1-*

5.1.1—The ATN SARPs ~~SARPs (Standards and Recommended Practices)~~ for the CNS/ATM-1 Package are documented in five "Sub-Volumes" as follows:

- Sub-Volume 1 - Introduction & System Level Requirements
- Sub-Volume 2 - Air/Ground Applications
- Sub-Volume 3 - Ground/Ground Applications
- Sub-Volume 4 - Upper Layer Architecture
- Sub-Volume 5 - Internet Communications Service

5.1.2—This document comprises Sub-Volume 5.

5.1.3—Sub-Volume 5 defines the provisions that ATN~~Aeronautical Telecommunication Network~~ compliant End Systems (ESs) and Intermediate Systems (ISs) must implement in order to provide thea ATN SARPs~~CNS/ATM-1 Package~~ compliant "Internet Communications Service" to the "User" i.e. the Upper Layer Architecture as defined in Sub-Volume 4 of the ATN~~CNS/ATM-1 Package~~ SARPs. For the protocols, the majority of such provisions are specified in a tabular fashion under the title of "ATN Protocol Requirements Lists" (APRLs).

5.1.4—Sub-Volume 5 comprises nine Chapters as introduced below.

5.1.4.1—Chapter 5.1, i.e. this Chapter, contains introductory material to the remainder of the Sub-Volume.

5.1.4.2—Chapter 5.2 contains pertinent Internet 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 (~~Aeronautical Telecommunication Network~~) End Systems and Intermediate Systems, and SARPs related to security and priority handling within the ATN internet.

5.1.4.3—Chapter 5.3 contains provisions related to the deployment~~definition~~ of the 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.~~Internet Routing Architecture and components thereof e.g. Routing Domains, Administrative Domains, Routing Domain Confederations, ATN Backbone, ATN Islands, Routing Policies etc.~~

5.1.4.4—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.

5.1.4.5—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. The majority of such provisions are defined in a tabular fashion under the title of "ATN Protocol Requirements Lists" (APRLs) as are the provisions for the protocols defined in subsequent chapters of this Sub-Volume.

~~5.1.4.6—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.~~

~~5.1.4.7—Chapter 5.7 contains provisions related to the use of the various candidate Gground/Gground and Aair/Gground 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 and to enable the efficient use of the limited bandwidth available over such the currently standardised Aair/Gground subnetworks, via the definition of appropriate compression techniques.~~

~~5.1.4.8—Chapter 5.8 contains provisions related to the exchange of routing information between ATN Intermediate Systems and End Systems using based on ISO OSI Routing Information Exchange protocols such as the Inter Domain Routing Information Exchange Protocol (IDRP) and specific features of the ES-IS protocol.~~

~~5.1.4.9—Chapter 5.9 contains a recommendaassumptions regarding the implementation of Iinternet Systems Management within the frame of the CNS/ATM-1 Package.~~

## 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 this 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~~ one unique 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 Administration RDs

5.2.2.2.2.1 Each State and Organisation ~~Administration~~ 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 Administrations may alternatively combine their RDs into a single RD.

#### Aeronautical Industry RDs

5.2.2.2.2.2 ~~Each aeronautical industry member participating in the ATN shall operate one or more Routing Domains (RDs), comprising Air/Ground and Ground/Ground Routers as required to interconnect with Mobile RDs and other ground-based ATN RDs, respectively.~~

Note.—Adjacent aeronautical industry domains 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 Mmobile 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 Mmobile platform, and at least one Airborne Router (Router Class 6 or 7 as defined in Table 5.2.-1).

Note 1.—An ATN Mmobile platform may operate multiple ERDs.

Note 2.—When more than one Airborne Router (BIS) is installed on board an aircraft, then each shall ~~must~~ be in a separate Routing Domain.

5.2.2.2.3.3 **Recommendation.**—ATSC and AINSC End-Systems and Intermediate Systems (non-BISs) located within a Mmobile platform should form a single Routing Domain including the airborne router (BIS) referred to in the above note, within the appropriate Administrative Domain.

Note 3.—A single routing domain minimizes the transfer of routing information over low-bandwidth Air/Ground subnetworks.

Note 4.—It is anticipated that other classes of Mmobile 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 (Routing Domain Confederation).

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

Note. — An example ATN Island RDC topology is presented in Figure 5.5.2-1.

#### 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 Mmobile, the destination of which is the entire fixed ATN, without having to enumerate the

*RIDs (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 MmMobile rRouting.*

### **5.2.2.4.2 ATN Island Backbone RDCs**

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 Mmmobile 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.*

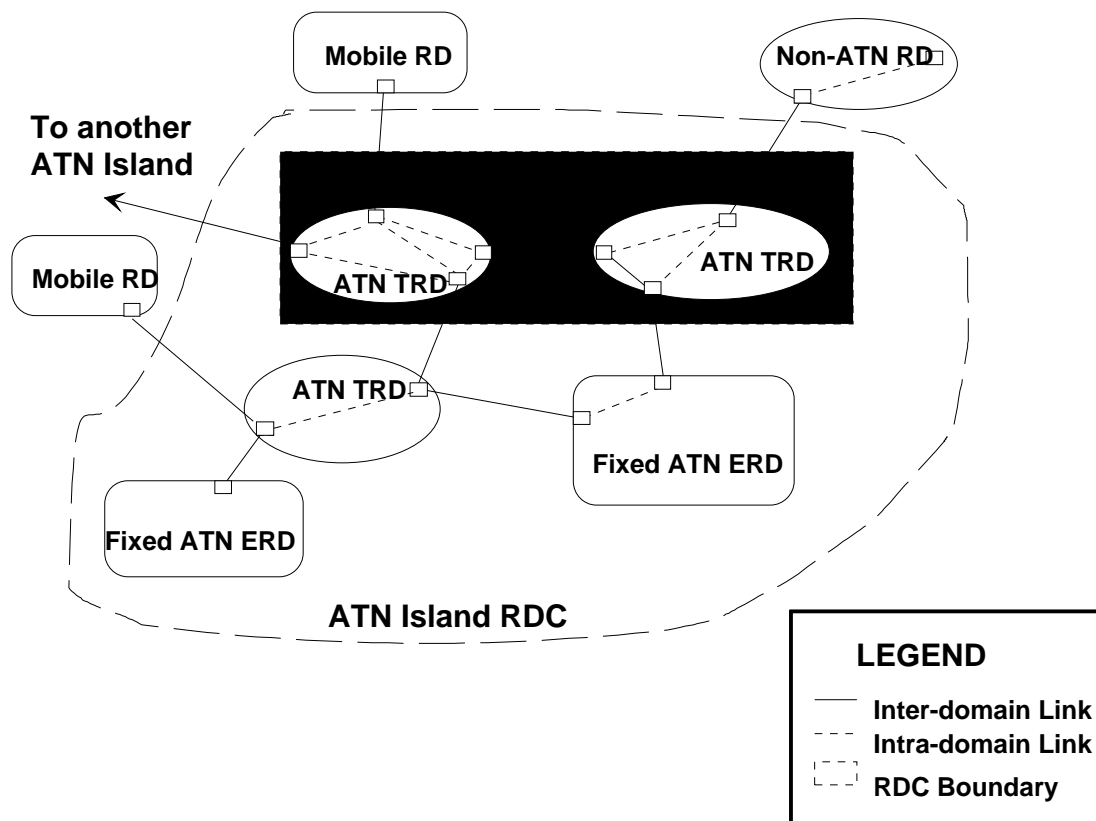


Figure 5.5.2-1 Example ATN Island Routing Domain Confederation Structure

### 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.*—The Routing Policies for communication between ATN and non-ATN RDs within the same 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:

- is available to all traffic types (see 5.2.7.1.2.), and
- has in its destination an NSAP address prefix which is common to all Airborne Systems and only 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:

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

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 both Air/Ground and/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 — Protocol for Providing the Connectionless Mode Network Service~~ as the Subnetwork Independent Convergence Function (SNICF) as specified in Chapter 5.6.
- b) a Subnetwork Access Protocol (SNAcP) suitable for each underlying subnetwork.
- c) a Subnetwork Dependent Convergence Facility (SNDCF) providing byte and code independent service to the SNICF (i.e. ISO/IEC 8473) via the ~~appropriate~~ selected Subnetwork Access Protocol, as specified in Chapter 5.7.

**Recommendation.** — ~~ATN End Systems should implement the End System provisions of ISO/IEC 9542 — End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless mode network service — to facilitate the exchange of routing information between the ES and any locally attached IS(s).~~

÷

- d) ~~The End System provisions of ISO/IEC 9542 — End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for the Provision of providing the Connectionless mode Network Service — 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 — Protocol for providing the Connection mode Oriented Transport Protocol transport service (Class 4)~~ as specified in Chapter 5.5.
- b) ~~ISO/IEC 8602 — Protocol for providing the OSI Connectionless mode Transport service Protocol~~ as specified in Chapter 5.5.

### 5.2.3.4 Upper Layers

~~Note 1. — The requirements for session, presentation and application layer protocols to support end-user applications on ATN End Systems are defined in Sub-volume 4 of the ATN CNS/ATM-1 SARPs.~~

### 5.2.3.5 Applications

~~Note 1. — The requirements for CNS/ATM-1 Air/Ground and Ground/Ground applications are contained in Sub-volumes 2 and 3 of the ATN CNS/ATM-1 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 Inter-Domain Routers (i.e. Router Classes 4 to 7 inclusive) shall support:

- a) the ISO/IEC 8473 Connectionless Network Protocol (CLNP) as specified in Chapter 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 according to 5.3.8.
- b) the ISO/IEC 10747 Inter-Domain Routing Protocol (IDRP) as specified in Chapter 5.8 for the exchange of inter-domain routing information according to 5.3.6 and 5.3.7.

5.2.4.1.3 An Airborne (Router Classes 6 or 7) or Air/Ground Router (Router Class 5) shall support the Mobile SND CF specified in Chapter 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 Chapter 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 — *Protocol for Providing the Connectionless Mode Network Service*— as the Subnetwork Independent Convergence Function (SNICF) as specified in Chapter 5.6.
- b) a Subnetwork Access Protocol (SNACp) suitable for each underlying subnetwork.

- c) a Subnetwork Dependent Convergence Facility (SND CF) providing byte and code independent service to the SNICF (i.e. ISO/IEC 8473) via the selected Subnetwork Access Protocol, as specified in Chapter 5.7.
- d) The routing protocols specified in Table 5.5.2-1 for the Router's Router Class, as specified in Chapter 5.8.
- e) The Route Initiation procedures appropriate to the Router Class, as specified in Chapter 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 End-System to Intermediate System Routing Exchange Protocol for use in conjunction with the Protocol for the Provision of providing the Connectionless mode Network Service for operation over those subnetworks to facilitate the exchange of addressing information (BIS Network Entity Title) information between the Router and its peer as specified in Chapter 5.3 (see 5.3.5.2) and in Chapter 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 Chapter 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 require that aircraft operating in their airspace, after July 1999, and desiring ATSC services via the ATN must support the use of ISO/IEC 10747, as specified in Chapter 5.8.

## 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 Both fixed- and Mobile ATN subnetworks shall conform to the following requirements :

#### 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 SND CF.

#### 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 shall either be constant and known, or must be capable of being determined on a dynamic basis, in order to support the internetwork routing decision process.

*Note.* — The service referred to is the quality of the SN-Service, which may differ from the inherent subnetwork QoS where an SND CF is employed.

#### 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 local subnetwork shall be carried out by mechanisms internal to the subnetwork, based solely on the subnetwork addressing information given to the SN-Service provider when the SN-Service is invoked.

#### 5.2.5.1.6 Minimum SNSDU Size

5.2.5.1.6.1 An ATN subnetwork shall support a minimum Subnetwork Service Data Unit (SNSDU) size of 1100 octets.

*Note 1.* — The 1100 octet number is derived from a 1024 octets user data, 9 octets fixed ISO 8473 header, 42 octets Source and Destination NSAP Addresses, 4 octets for the SND CF local reference option, 3 octets for

the QoS Maintenance parameter, 3 octets for the priority parameter, and 15 octets for the security parameter.

Note 2. — This will permit the use of the non-segmenting ISO/IEC 8473 subset for NSDUs of up to 1024 octets.

## 5.2.5.2 Requirements for ATN Mobile ATN-Subnetworks

### 5.2.5.2.1 General

5.2.5.2.1.1 An ATN Mmobile Ssubnetwork shall conform to the following requirements:

#### 5.2.5.2.2 Invocation of Subnetwork Priority

5.2.5.2.2.1 When priority is implemented within that subnetwork, an ATN Mmobile Ssubnetwork 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 ATN-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 Mmobile Ssubnetworks 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 Mmobile Ssubnetwork 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 Mmobile Ssubnetwork 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 Mmobile SNAcP.

### 5.2.5.2.5 Connectivity Status Changes

Note 1. — ATN Mobile ATN-Ssubnetworks may provide a mechanism for detection of change in media connectivity and for the conveyance of this information to connected ATN routers.

5.2.5.2.5.1 If a Mmobile Ssubnetwork provides subnetwork connectivity information, the subnetwork shall convey this information to connected subnetwork service users (i.e. connected ATN routers), in order to initiate operation of the internetwork routing protocols as specified in Chapter 5.3.

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.

### 5.2.5.2.6 Segmentation/Reassembly Mechanism

5.2.5.2.6.1 **Recommendation.**— An ATN Mmobile Ssubnetwork should provide a mechanism that allows the conveyance of large SNSDUs greater than the subnetwork's internal packet size between SNPAsubnetwork points of attachment.

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 ATN Subnetwork, ISO/IEC 8473 can support segmentation of NPDU's 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 ~~c~~Capacity ~~p~~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 CNS/ATM applications that use it.

Note 2. — Network Administrators may take advantage of the ~~strong~~ QoS requirements signalled by the ATSC Class (see ~~Section~~Chapter 5.2.7 Security Concept), in order to ensure that only those parts of the ATN that support the ~~high~~ QoS requirements of ATSC applications, need be designed to meet those requirements.

## 5.2.7 ATN Security Concept

Note 1. — ATN Security Functions are concerned with:

- a) Protecting ATN Data Link CNS/ATM applications from internal and external threats;
- b) Ensuring that application Quality of Service and Routing Policy Requirements are maintained, including service availability; and,
- c) Ensuring that Air/Ground subnetworks are used in accordance with ITU requirements.

Note 2. — Other than through the provision of physical security mechanisms, no security mechanisms are provided in the ATN Internet for protecting ATN Data Link CNS/ATM applications. ATN Data Link CNS/ATM applications need to develop their own security mechanisms for countering any threats to their proper operation. This may change in future versions of the specification.

Note 3. — There are currently no mechanisms for protecting the Routing Information Base from an attacker. However, the use of ISO/IEC 10747 type 2 authentication is under consideration for specification in future versions of this specification.

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 ~~Data~~ 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 ~~Data~~ 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 restrictions.

### 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 ~~section 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 1.~~ — 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 An CLNP Data NPDU’s Security Label shall identify the “Traffic Type” of its user data, as either:

- a) ATN Operational Communications—  
ATSC
- b) ATN Administrative Communications

- c) ATN Systems Management Communications.

*Note 1. — 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—ATSC traffic type and the ATSC traffic category, routing policy requirements shall be expressed through further information encoded into the Security Label, as either:

- a) An preferred ATSC Class, or
- b) An ordered preference for the class of air-ground subnetwork used to convey the data; the only order that may be expressed is Mode S, VDL, AMSS and finally HF, or
- b) No routing policy preference.

5.2.7.1.2.3 For the ATN Operational Communications—AOC 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 2. — The possible ordering of Air/Ground subnetworks are specified in Sub-Volume 1, Table 1.2-1 (ATSC Traffic Classes) Table 5.6-1.*

### 5.2.7.1.3 ATSC Class

*Note 1. — The Transit Delay semantics of ATSC Class are defined in Sub-Volume 1, Table 1.2-1 (ATSC Traffic Classes).*

*Note 2. — The semantics of the ATSC Classes 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 Applications data.*

## 5.2.7.2 Applications Use of ATN Security Labels

5.2.7.2.1 ATN Data LinkATSC and AINSC 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 5.5.2.7.1.2.1

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 specified for the specified message's 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 1. — 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 2. — The Network Layer functions may then encode this ATN Security Label in the NPDU header.*

5.2.7.3.1.4 TPDU's 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 ~~NPDU~~ header of the NPDU that conveyed it, shall define the ATN Security Label that is associated with the transport connection.

*Note 3. — 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 4. — 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 for determining 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). 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 ~~T~~transport ~~L~~layer to the ~~N~~network ~~L~~layer in an NS-UNITDATA.request, This ATN Security Label shall be encoded into the header of the corresponding CLNP NPDU(s) ~~header(s)~~ according to ~~section 5.6.2.2.21~~.
- b) When passed from the ~~N~~network ~~L~~layer to the ~~T~~transport ~~L~~layer in an NS-UNITDATA.indication. This ATN Security Label shall be that received in the header of the associated CLNP NPDU header(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 ~~User~~ 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.

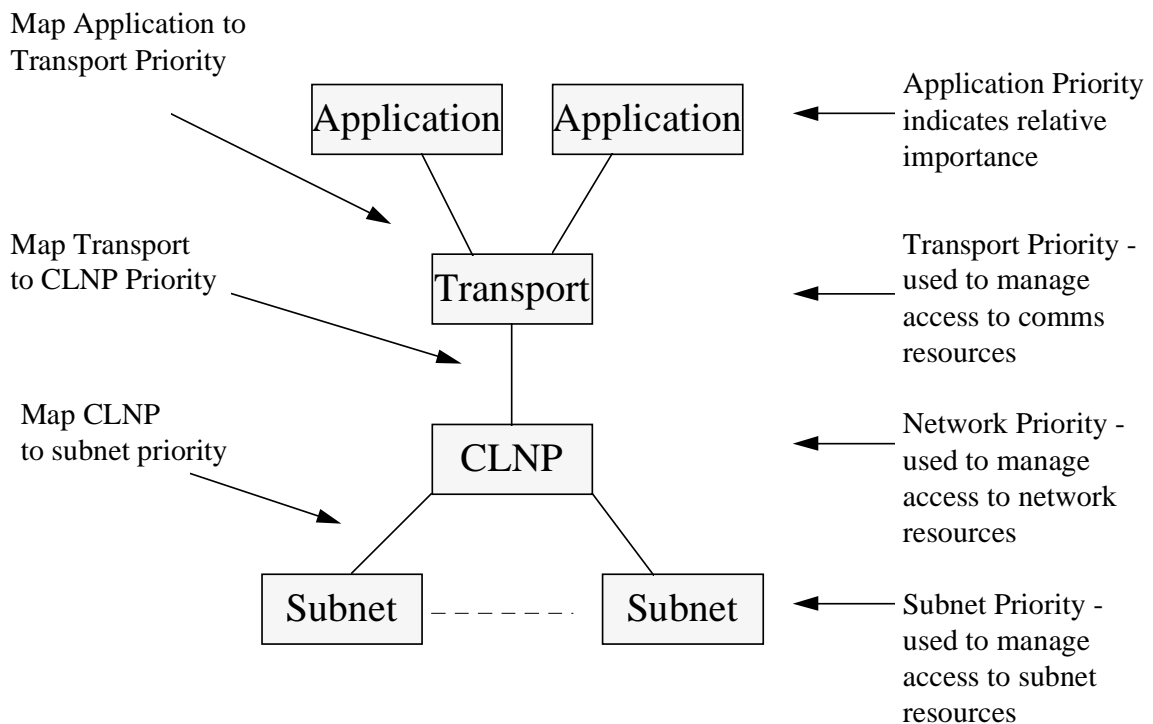
*Note 1. — ~~Section 5.3.2.21~~ specifies the forwarding procedures that ensure the above.*

*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 used as a mechanism for ensuring the integrity of routing information exchange by IDRP.

*Note. — A later extension to support type 2 authentication will enable 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.*



**Figure 5.5.2-2. Use of Priority in the ATN**

### 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 5.5.2-2 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, even and in particular when the network is overloaded with low priority data.

### 5.2.8.1 Application Priority

*Note 1.* — 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 ~~Sub-Volume 1, Table 1.2-2 (Relationship of Communication priorities)~~ Table 5.2-1.

*Note 2. — 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 ~~Sub-Volume 1, Table 1.2-2 (Relationship of Communication priorities)~~ for the message's message category, or
- b) the connectionless transport service, signalling the Connectionless Transport Service Priority listed in ~~Sub-Volume 1, Table 1.2-2 (Relationship of Communication priorities)~~ for the message's message category.

*Note 3. — 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.*

*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 3. — 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 TPDU's, by reducing credit windows, etc.*

5.2.8.2.2 All TPDU's 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 ~~Sub-Volume 1, Table 1.2-2 (Relationship of Communication priorities)~~.

### 5.2.8.3 Connectionless Transport Service Priority

*Note 1. — 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 TPDU's 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 ~~Sub-Volume 1, Table 1.2-2, (Relationship of Communication priorities)~~

### 5.2.8.4 ATN Internet Priority

*Note 1. — 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 NPDU's 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 2. — *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 3. — *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 4. — *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 subnetworks 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.

Note 4. — *The following does not apply to AMSS and Mode S Subnetworks, which have specified their own priority mapping schemes.*

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) For the “High” priority connection type, the priority to gain a connection, keep a connection and for data on the connection shall be appropriate for urgent and network management data in the context of the subnetwork. In the absence of guidance from the subnetwork provider, the value decimal 8 shall be used for each of the three priorities.
- d) “High” priority connections shall be used to convey NPDUs of priority six and above. “Low” priority connections shall be used to convey all other NPDUs.

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 ~~priority 14~~ NPDUs of priority 14 (i.e. Network/Systems Management).

*Note 5. — 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

##### 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 ATNAeronautical Telecommunications Network; and the Route Initiation procedures for initiating the exchange of routing information using the ISO/IEC 10747 protocol. In the case of Air/G-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 Chapter 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/G-Ground Routers shall comply with the provisions of 5.5.3.4 and 5.5.3.6.

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/G-Ground Router shall also comply with the provisions of 5.5.3.7.1.

5.3.1.2.3 When used in any other ATN Transit Routing Domain, an ATN Ground/G-Ground Router shall also comply with the provisions of 5.5.3.7.3.

5.3.1.2.4 Otherwise, an ATN Ground/G-Ground Router shall comply with the provisions of 5.5.3.7.4.

5.3.1.2.5 ATN Air/Ground Routers shall comply with the provisions of 5.5.3.4. for Ground/G-Ground interconnection, 5.5.3.5 for Air/G-ground interconnection and 5.5.3.6.

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 5.5.3.7.1.

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 5.5.3.7.3.

5.3.1.2.8 ATN Airborne Routers shall comply with the provisions of 5.5.3.5, 5.5.3.6, and 5.5.3.7.2.

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 RouterRouting Domain

#### 5.3.2.1 General

*Note 1.*— An ATN Routing Domain may operate as an ATN Service Provider, in which case it operates as a Transit Routing Domain and offers routes to other ATN RDs.

*Note 2.—~~An ATN RD may also be considered as providing the facilities of an ATN Service Provider when offering routes to destinations within itself.~~*

5.3.2.1.1 A route shall only be advertised by an ATN ~~Router Service Provider~~ 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 3.— The acceptability of a route may be determined using a priori knowledge derived from interconnection agreements with other RDs.*

~~An ATN RD shall only forward a CLNP NPDU to an ATN Service Provider when that ATN Service Provider is advertising a route to the NPDU's destination, and the route is defined below as being a route over which the ATN Service Provider is required to forward the NPDU.~~

## 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 NPDU 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 1.— Forwarding decisions that also take into account the CLNP QoS Maintenance Parameter are a local matter and an ATN ~~Router Service Provider~~ 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 ~~section 5.2.7.1~~).*

5.3.2.2.2.1 When a CLNP NPDU is received by an ATN ~~Router Service Provider~~ and that NPDU does not contain a Security Parameter in the PDU Header then that NPDU shall be forwarded over

the route, if present, that either:

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-General Communications" in its set of permissible Traffic Types, or
  - b) no Air/Ground Subnetwork Security Tag,

~~or~~

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 Service Provider~~ and that NPDU contains a Security Parameter in the Globally Unique Format, and encodes security related information according to ~~5.6.2.2~~ Chapter 6 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 CategoryType

*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 Routing Policy PreferenceSpecified

*Note 1.— 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~~Chapter 5.6~~ 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~~Routing Policy Preference~~Specified,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that 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
  - I. no ATSC Class \_Security Tag, or,
  - II. if no such route is present, then an ATSC Class Security Tag indicating support of the lowest class out of all such routes available.

*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 1.— 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~~Chapter 5.6~~ 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 a selected route to the NPDU's destination that 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,

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 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 shall be selected.

#### **5.3.2.2.3.3 ATN Operational Communications Traffic Type - AOC Traffic Category**~~Type~~

*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**~~Routing Policy Preference~~Specified

*Note 1.— 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~~Chapter 5-6~~ 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~~Routing Policy Preference~~ Specified,

then the NPDU shall be forwarded over a selected route to the NPDU’s destination that 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.

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 ~~so~~ 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~~Chapter 6~~ 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 a selected route to the NPDU’s destination that 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.

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 ~~so~~ 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~~Chapter 5-6~~ 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 a selected route to the NPDU’s destination that 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.

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 3.— 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 1.— 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~~Chapter 5-6~~ under the ATN Security Registration Identifier, and

- b) a traffic type of ATN Administrative Communications,

then the NPDU shall be forwarded over a selected route to the NPDU’s destination that 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.

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 1.— 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~~Chapter 5-6~~ under the ATN Security Registration Identifier, and
- b) a traffic type of ATN Systems Management Communications,

then the NPDU shall be forwarded over a selected route to the NPDU’s destination that:

- 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 and can be used to convey the ISO 8473 protocol and provides the required quality of service.

*Note 3.— 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 4.— The dynamic procedures for the interconnection of two ground-based ATN Routers are specified in 5.5.3.4, and for interconnection of an Air/Ground and an Airborne Router in 5.5.3.5. 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 a suitable and mutually agreeable real subnetwork(s), or

- b) interconnected directly as in a) above, 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 1.— 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 CNS/ATM*



applications and other aeronautical or airline industry applications.

5.3.3.1.5.1 In order to meet the availability requirements of ATN Data LinkCNS/ATM applications, Airborne and Air/Ground Routers shall be capable of supporting multiple concurrent adjacencies with other Routers.;

*Note 2.— These adjacencies are supported by multiple subnetwork connections at the same or different priorities, using the same or different Air/Ground subnetworks.*

*Note 32. — 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 43. — 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 1.— 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 nNetwork aAdministrators agree to the gGround/-gGround 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 2.— 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 when this step may be omitted.

*Note 3.— 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 4.— 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 Chapter 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 5.— This step is necessary to ensure that the connectionless network service can be used to exchange the BISPDU's of IDRPs.*

5.3.4.2.2 Using global or local Systems Management mechanisms:

- a) append the NET of the remote ATN Router to the **externalBISNeighbor\_**-attribute of the BIS's **idrpConfig MO**,
- b) create an **AdjacentBIS** Managed Object (MO) in each ATN Router to represent the other ATN Router, and
- c) invoke the start event action on each such MO, in order to initiate a BIS-BIS connection between the two ATN Routers.

*Note 6.— As a matter for the bilateral agreement of the nNetwork aAdministrators, either (a) both ATN Routers will attempt to open the BIS-BIS connection using the active-open procedures, that is with the ListenForOpen MO attribute set to false, or (b) one and only one acts as the BIS-BIS connection initiator sets this attribute to true.*

### 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 Chapter 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 5.5.3.7.1, 5.5.3.7.3, or 5.5.3.7.4, 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 nNetwork aAdministrators 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 5.5.3.4.2 may be re-invoked, as appropriate to re-establish communication, and to exchange routing information.*

5.3.4.4.1 When a nNetwork aAdministrator 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.

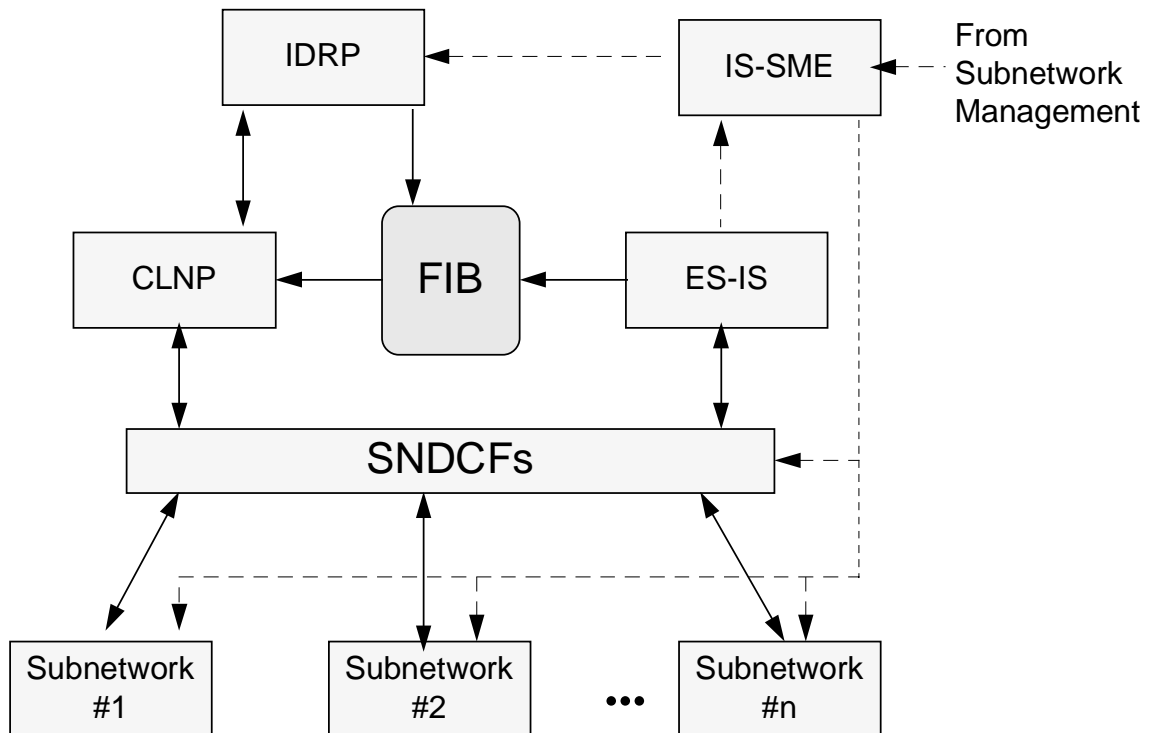
5.3.4.4.3 For either temporary or permanent termination, and if required, by using global or local Systems Management mechanisms, the nNetwork aAdministrator(s) shall also terminate the underlying subnetwork connections.

## 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 Mmobile Ssubnetworks.*

*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*



**Figure 5.5.3-1 Assumed ATN Router Architecture for Air/Ground Route Initiation**

communications and local policy, while, in the latter case, interconnection is a deliberate and planned action with the direct involvement of nNetwork aAdministrators.

*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 5.5.3.5.2.12.

*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) ~~For the~~, the data flow between them as thick 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.

## 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.— Two types of Mmobile Subnetworks are also recognised by this specification. These are:  
 (a) those which provide information on the availability of specific Mmobile Systems on the subnetwork through the Join Event defined in this section, and (b) those which do not. The latter type are only appropriate to Route Initiation Procedures which are Air-Initiated.

Note 3.— For a given Mmobile 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 4.— The interfaces to all Mmobile 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 Mmobile Subnetwork.

5.3.5.2.1.2 For Air-Initiated Subnetworks that do not provide information on the availability of specific Mmobile Systems, Airborne Routers shall comply with the procedures specified in 5.5.3.5.2.3.1, and Air/Ground Routers shall comply with the procedures specified in 5.5.3.5.2.2.

5.3.5.2.1.3 For Air-Initiated Subnetworks that do provide information on the availability of specific Mmobile Systems, Airborne Routers shall comply with the procedures specified in 5.5.3.5.2.3.2, and Air/Ground Routers shall comply with the procedures specified in 5.5.3.5.2.2.

5.3.5.2.1.4 For Ground-Initiated Subnetworks, Air/Ground Routers shall comply with the procedures specified in 5.5.3.5.2.4, and Airborne Routers shall comply with the procedures specified in 5.5.3.5.2.2.

5.3.5.2.1.5 For Air or Ground-Initiated Subnetworks, Air/Ground and Airborne Routers shall comply with the procedures specified in 5.5.3.5.2.2 and 5.5.3.5.2.5.

### 5.3.5.2.2 Route Initiation Procedures for a Responding ATN Router

#### 5.3.5.2.2.1 General

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 3.— ~~The procedures used to~~ Whenever such a Call Indication is received the ATN Router validates the calling DTE address and to determine the acceptability of the call, ~~are using procedures outside the scope of this specification.~~

Note 4.— 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 5.5.3.5.2.6 shall be applied to that subnetwork connection.

#### 5.3.5.2.2.2 Emergency Use of a Mobile Subnetwork

5.3.5.2.2.2.1 In the case of Air-Initiated Mobile Subnetworks, an Air/Ground Router shall not refuse a Call Indication or refuse to establish a BIS-BIS connection with an ATN Airborne Router, when a Call Indication from the ATN Airborne Router is received less than 5 minutes after a Call Indication was rejected, or a call was terminated by Systems Management.

5.3.5.2.2.2.2 The Air/Ground Router shall permit, through the implementation of an

appropriate routing policy, the use of a so established connection for emergency and distress data.

*Note 5. — This situation arises when the Airborne Router has no other Air/Ground connectivity, and refusal to accept a connection may cause a safety hazard. An Air/Ground Router may limit the use of such connections through routing policy, or permit full access, as a local matter.*

### 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 Airborne Router Procedures for use of an ISO/IEC 8208 Mobile Subnetwork that does not Provide Information on Subnetwork Connectivity

##### 5.3.5.2.3.1.1 General

5.3.5.2.3.1.1.1 An Airborne Router's IS-SME shall be configured with a list of subnetwork addresses for each supported Mobile Subnetwork that does not provide information on subnetwork connectivity of this type that it supports.

5.3.5.2.3.1.1.2 This list ~~shall~~ should include the addresses which are necessary to meet the communication needs of the aircraft.

*Note.— In the case of the AMSS, the Airborne Router's IS-SME will be configured with a list for each GES that the aircraft may will use to communicate. —Each such list will include the subnetwork addresses (e.g. DTE addresses) of the Air/Ground routers attached to the GES in question through which communications services may be required.*

5.3.5.2.3.1.1.3 An Airborne Router's IS-SME shall continually issue a Call Request to each subnetwork address on each appropriate list with which it does not currently have a subnetwork connection and which is not subject to a back-off period (see 5.3.5.2.3.1.2), in turn.

5.3.5.2.3.1.1.4 The period between each successive Call Request shall be configurable to ensure that the Mobile Subnetwork is not rendered unavailable.

5.3.5.2.3.1.1.5 When a subnetwork connection is successfully established, then the procedures of 5.3.5.2.6 shall be applied to that subnetwork connection. The polling procedure shall continue for the remaining subnetwork addresses on the list, if any.

##### 5.3.5.2.3.1.2 Call Request Failure

5.3.5.2.3.1.2.1 Whenever a Clear Indication is received in response to a Call Request that indicates rejection by the called DTE and includes a call clearing diagnostic code of 0, 133, 160..163, or 240, 241, 242, 244, 246, 248, then the Airborne Router shall implement a "back off" procedure.

5.3.5.2.3.1.2.2 The back off procedure shall comprise the effective quarantining of the called subnetwork address for a period configurable on a per subnetwork basis from 5 minutes to 20 minutes. During this period, a Call Request shall not be issued to the subnetwork address.

*Note 1.— The purpose of the back off procedure is to avoid unnecessarily overloading of the Air/Ground subnetwork with Call Requests.*

5.3.5.2.3.1.2.3 The "back off" procedure shall not be started on receipt of a Clear Indication which includes any other call clearing diagnostic code.

5.3.5.2.3.1.2.4 If a Clear Indication is received ~~the call is cleared~~ with a diagnostic code reporting an error that the SNDCF is unable to correct, then the called DTE shall be removed from the polled DTEs list.

5.3.5.2.3.1.2.5 Otherwise, if required, the SNDCF shall retry the call after having resolved the cause of the call rejection.

*Note 2.— Certain call clearing diagnostic codes in the range 128..143 are used by the Mobile SNDCF specified in chapter 5.7. The semantics of these codes ~~are~~ described in Table 5.7-86.*

5.3.5.2.3.1.2.6 However, during any period when an Airborne Router does not have any subnetwork connections over Mobile Subnetworks, then all back off procedures shall be suspended until connectivity is established with at least one Air/Ground Router.

*Note 2.— The purpose of the backoff procedure is to avoid unnecessarily overloading the network with Call Requests.*

### 5.3.5.2.3.2 Airborne Router Procedures for use of an ISO/IEC 8208 Mobile Subnetwork that does Provide Connectivity Information

*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 DTE Address of the newly available system.*

*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.*

5.3.5.2.3.2.1 On receipt of a Join Event, the Airborne Router shall either:

- a) Issue an ISO/IEC 8208 Call Request with the DTE Address reported by the Join Event as the Called Address, or
- b) Validate 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 shall be issued with the DTE Address reported by the Join Event as the Called Address. Otherwise, the Join Event shall be ignored.

*Note 4.— 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 When a subnetwork connection is successfully established, then the procedures of 5.5.3.5.2.6 shall be applied to that subnetwork connection.

### 5.3.5.2.4 Ground-Initiated Route Initiation

*Note 1.— Ground-Initiated Route Initiation is only appropriate for Mobile Subnetworks that originate a Join Event from their ground*

*component.*

*Note 2.— For ground-initiated subnetworks, the Join Event is received by the IS-SME in the Air/Ground Router. The mechanism by which it is received is both subnetwork and implementation dependent and is outside of the scope of this specification.*

5.3.5.2.4.1 On receipt of a Join Event, the Air/Ground Router shall either:

- a) Issue an ISO/IEC 8208 Call Request with the DTE Address reported by the Join Event as the Called Address, or
- b) Validate 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 shall be issued with the DTE Address reported by the Join Event as the Called Address. Otherwise, the Join Event shall be ignored.

*Note 3.— 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.*

5.3.5.2.4.2 When a subnetwork connection is successfully established, then the procedures of 5.5.3.5.2.6 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~~ both Airborne or and Air/Ground Routers, 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.*

5.3.5.2.5.1 On receipt of a Join Event, the ATN Router shall either:

- a) Issue an ISO/IEC 8208 Call Request with the DTE Address reported by the Join Event as the Called Address, or
- b) Validate 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 shall be issued with the DTE Address reported by the Join Event as the Called Address. Otherwise, the Join Event shall be ignored.

*Note 3.— 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.*

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

*Note 4.— 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.

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 Recommendation.**— *When in the initiator role, 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.*

**5.3.5.2.6.6 Recommendation.**— *When in the responder role 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.*

*Note 1.— The purpose of encoding an ISH PDU in call request/ or call accept 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.*

5.3.5.2.6.7 Whenever an ISO/IEC 9542 ISH PDU is received, either as Call Request/ or Call Accept 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 NPDU's to be sent over the subnetwork connection to the indicated NET shall be written into the Forwarding Information Base for use by ISO/IEC 8473.

5.3.5.2.6.8 A Systems Management notification shall also 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 2.— Except for the case of the situation described in 5.5.3.5.2.2.2, 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 5.5.3.5.2.8, and an Airborne Router shall apply the procedures of 5.5.3.5.2.9.

#### **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 5.5.3.5.2.10 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 5.5.3.5.2.12 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 5.5.3.5.2.10 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 5.5.3.5.2.12 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 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 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 1.— 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 Router, then 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.

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

5.3.5.2.10.6 The IS-SME shall also ~~check to~~ 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.

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



**5.3.5.2.10.8 Recommendation.**—When IDRPs are 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, except when a watchdog timer is applied to the subnetwork connection (see 5.5.3.5.2.13).

*Note 2.*—The purpose of the above is to effectively suppress the further generation of ISH PDUs.

*Note 3.*—Normally, the IDRPs 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 IDRPs

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 5.5.3.7.2.
- b) An Air/Ground Router shall advertise routes to the Airborne Router in accordance with the Routing Policy specified in 5.5.3.7.1.4 or 5.5.3.7.3.4 as appropriate for the role of the Air/Ground Router’s RD.

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

*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 IDRPs, this re-transmission is necessary to maintain the “liveness” of the connection.

#### 5.3.5.2.12.1 Air/Ground Router

5.3.5.2.12.1.1 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 IDRPs 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 and an Adj-RIB-Out shall hence be created for this remote ATN Router and for the Security RIB-Att.

*Note 1.*—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. There is also no need to ever place routes in the Adj-RIB-Out. Implementations may choose to optimise the operation of these procedures with a special interface to IDRPs.

- 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 is 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 2.*—According to the rules for the update of path information specified in Chapter 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 IDRPs over a Mobile Subnetwork.

- c) The well-known mandatory path attribute RD\_HOP\_COUNT shall be set to 1 in the for routes to be inserted into the Adj-RIB-In of an A/G-BIS for the remote Router adjacent Airborne BISs not implementing the procedures for the optional non-use of IDRPs. In addition, for routes to be inserted into the Adj-RIB-In for an adjacent Airborne RouterBISs not implementing the procedures for the optional non-use of IDRPs, the well-known mandatory path attribute CAPACITY shall be set according to the capacity of the Mobile Subnetwork(s) over which the Airborne RouterBIS is reachable.

*Note 3.*—If the CAPACITY attribute is set to the value of the RD in which the Air/Ground BIS is

*located, the route pretends to provide the capacity of a ground subnetwork that is probably much higher than the capacity of the mobile subnetwork. This could result in inefficient forwarding decisions for NPDU's towards Airborne ESs. The CAPACITY attribute is correlated with the ATSC Class Security information.*

5.3.5.2.12.1.2 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.

5.3.5.2.12.1.3 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.

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

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

5.3.5.2.12.1.6 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.

#### **5.3.5.2.12.2 Airborne Router**

5.3.5.2.12.2.1 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.

5.3.5.2.12.2.2 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 locally known

information.

*Note 1.— 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 and 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 locally known information.

*Note 2.— 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**

*Note 1.— The "Leave Event" is defined to signal when subnetwork connectivity 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 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.

5.3.5.2.13.2 When a Mobile Subnetwork does not provide a network generated Clear Indication (e.g. to indicate that an aircraft has left the range of the Mobile Subnetwork, or when some other communication failure occurs, etc.), an ATN Router shall maintain a "watchdog" timer for each affected subnetwork connection and clear each

such subnetwork connection once activity has ceased for a configurable period.

5.3.5.2.13.3 When such a “watchdog” timer expires, this shall be reported as a “Leave Event” for that subnetwork connection.

5.3.5.2.13.4 **Recommendation.**— *The timer should be configurable according to the characteristics of the subnetwork.*

*Note 3.*—*An ATN Router maintains a “watchdog” timer for each applicable subnetwork connection to detect the event of an aircraft leaving coverage (or other communication failure), if such an event detection is not provided by the subnetwork.*

5.3.5.2.13.5 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.

5.3.5.2.13.6 If, as a result of this procedure, there are no other subnetwork connections with the ATN Router that was the ultimate subject of the Leave Event then,

1. ~~\_\_\_~~ In the case of an ATN Router having established a BIS-BIS connection with that ATN Router, an IDRPs deactivate action shall be invoked to terminate that BIS-BIS connection.

~~\_\_\_~~ *Note 4.*—*As a consequence of the deactivate action and following normal IDRPs operation, the IDRPs 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.*

2. ~~\_\_\_~~ 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 IDRPs, all routes shall be removed from the Loc-RIB that had been inserted into it according to the procedures of ~~section 5.5.3.5.2.12.1~~ as a result of an ISH PDU having been received from the Airborne Router for which the Leave Event reports a loss of connectivity.

3. ~~\_\_\_~~ In the case of an Airborne Router implementing the procedures for the optional

non-use of IDRPs, all routes shall be removed from the loc-RIB that had been inserted into it according to the procedures of ~~section~~

5.5.3.5.2.12.2 as a result of an ISH PDU having been received from the Air/Ground Router for which the Leave Event reports a loss of connectivity.

- 5.3.5.2.13.7 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 adjacent BIS Managed Object associated with the initiating BIS shall be deleted, and the initiating BIS’s NET removed from the external BISNeighbor attribute of the BIS’s idrpConfig Managed Object.

**5.3.5.2.14 APRL for Air/Ground Route Initiation**

**5.3.5.2.14.1 General**

<b>Item</b>	<b>Description</b>	<b>ATN SARPs Reference</b>	<b>ATNCNS /ATM Package-1 Support</b>
njSubnet	Support of Subnetworks that do not provide a Join Event	5.5.3.5.2	O.1
jSubnet	Support of Subnetworks that do provide a Join Event	5.5.3.5.2	O.1
giSubnet	Support of Ground-Initiated Subnetworks	5.5.3.5.2	O.2
aiSubnet	Support of Air-Initiated Subnetworks	5.5.3.5.2	O.2
agSubnet	Support of Air or Ground-Initiated Subnetworks	5.5.3.5.2	O.2
fsSubnet	Support of Subnetworks that support Fast Select	-	O
noIDRP-a	Support of optional non-use of IDRP by (Airborne BIS)	5.5.3.5.2.12 .2	O
noIDRP-ag	Support of optional non-use of IDRP by (Air/Ground BIS)	5.5.3.5.2.12 .1	M
lvSubnet	Support of Subnetworks that provide a Leave Event	5.5.3.5.2.13	M

**5.3.5.2.14.2 Airborne Router - Subnetwork Connection Responder**

<b>Item</b>	<b>Description</b>	<b>ATN SARPs Reference</b>	<b>ATNCNS/ATM Package-1 Support</b>
respAR-ar	Response to incoming Call Requests	5.5.3.5.2.2	giOragSubnet: M
valCR-ar	Validation of incoming Call Request	5.5.3.5.2.2	giOragSubnet:O
RespISH-ar	Generation of ISH PDU	5.5.3.5.2.6	giOragSubnet: M
ISHinCC-ar	Encoding ISH PDU in <del>Connect Confirm</del> Call Accept User Data	5.5.3.5.2.6	RespISH-ar & fsSubnet: O
negNoIDRP-ar	Transmission of ISH PDU with SEL field of NET set to 0FEh	5.5.3.5.2.6	noIDRP-a:M
negIDRP-ar	Transmission of ISH PDU with SEL field of NET set to zero	5.5.3.5.2.6	^noIDRP-a:M

Item	Description	ATN SARP Reference	ATNCNS/ATM Package-1 Support
autoRoute-ar	Inference of available routes from <u>received NET</u> of A/G Router- <del>NET</del>	5.5.3.5.2.12.2	noIDRP-a:M
initIDRP-ar	IDRP startup procedures - Invoke activate action	5.5.3.5.2.10	^noIDRP-a:M
supISH-ar	Suppression of <u>_</u> multiple ISH PDUs	5.5.3.5.2.10	^noIDRP-a: O
valNET-ar	Validation of received NET	5.5.3.5.2.7	^noIDRP-a: O

giOragSubnet: giSubnet ^ agSubnet

#### 5.3.5.2.14.3 Airborne Router - Subnetwork Connection Initiator

Item	Description	ATN SARP Reference	ATNCNS/ATM Package-1 Support
polling-ai	Procedures for polling a list of subnet addresses	5.5.3.5.2.3.1	pollReq: M
backoff-ai	Backoff Procedure	5.5.3.5.2.3.1.2	pollReq: M
connect-ai	Connect on receipt of Join Event	5.5.3.5.2.3.2	EventDrvn: M
ValJoin-ai	Validation of Join Event	5.5.3.5.2.3.2	EventDrvn: O
SendISH-ai	Generation of ISH PDU	5.5.3.5.2.6	EventDrvn ^ pollReq:M
ISHinCR-ai	Encoding of ISH PDU in <u>CallConnect</u> Request	5.5.3.5.2.6	SendISH-ar & fsSubnet: O
negNoIDRP-ai	Transmission of ISH <u>PDU</u> with SEL field of <u>NET</u> set to 0FEh	5.5.3.5.2.8	noIDRP-a:M
negIDRP-ai	Transmission of ISH <u>PDU</u> with SEL field of <u>NET</u> set to zero	5.5.3.5.2.8	^noIDRP-a:M
autoRoute-ai	Inference of available routes from <u>received NET</u> of A/G Router- <del>NET</del>	5.5.3.5.2.12.2	noIDRP-a:M
initIDRP-ai	IDRP startup procedures - listenForOpen set to true	5.5.3.5.2.10	^noIDRP-a:M
supISH-ai	Suppression of <u>_</u> multiple ISH PDUs	5.5.3.5.2.10	^noIDRP-a: O
valNET-ai	Validation of received NET	5.5.3.5.2.7	^noIDRP-a: O

pollReq: aiSubnet & njSubnet

EventDrvn: jSubnet & (aiSubnet ^ agSubnet)

**5.3.5.2.14.4 Air/Ground Router - Subnetwork Connection Responder**

<b>Item</b>	<b>Description</b>	<b>ATN SARPs Reference</b>	<b>ATN CNS/ATM Package-1 Support</b>
respAR-agr	Response to incoming Call Requests	5.5.3.5.2.2	aiOragSubnet: M
valCR-agr	Validation of incoming Call Request	5.5.3.5.2.2	aiOragSubnet:O
emgncy-agr	Emergency Procedures	5.5.3.5.2.2. 2	M
RespISH-agr	Generation of ISH PDU	5.5.3.5.2.6	aiOragSubnet: M
ISHinCC-agr	Encoding ISH PDU in <del>Connect Confirm</del> Call Accepted User Data	5.5.3.5.2.6	RespISH-agr & fsSubnet: O
negNoIDRP-agr	Receipt of ISH PDU with SEL field of NET set to 0FEh	5.5.3.5.2.8	M
negIDRP-agr	Receipt of ISH PDU with SEL field of NET set to zero	5.5.3.5.2.8	M
autoRoute-agr	Inference of available routes from <u>received NET</u> of Airborne Router <del>NET</del>	5.5.3.5.2.12 .1	M
initIDRP-agr	IDRP startup procedures - Invoke activate action	5.5.3.5.2.10	M
supISH-agr	Suppression of <del>_</del> multiple ISH PDUs	5.5.3.5.2.10	O
valNET-agr	Validation of received NET	5.5.3.5.2.7	O

aiOragSubnet: aiSubnet ^ agSubnet

**5.3.5.2.14.5 Air/Ground Router - Subnetwork Connection Initiator**

<b>Item</b>	<b>Description</b>	<b>ATN SARPs Reference</b>	<b>ATN CNS/ATM Package-1 Support</b>
connect-agi	Connect on receipt of Join Event	5.5.3.5.2.4	goOragSubnet: M
ValJoin-agi	Validation of Join Event	5.5.3.5.2.4	connect-agi: O
SendISH-agi	Generation of ISH PDU	5.5.3.5.2.6	connect-agi: M

Item	Description	ATN SARPs Reference	ATN CNS/ATM Package-1 Support
ISHinCR-agi	Encoding of ISH PDU in <del>Connect</del> Call Request	5.5.3.5.2.6	Send-ISH-agi & fsSubnet: O
negNoIDRP-agi	Receipt of ISH PDU with SEL field of NET set to 0FEh	5.5.3.5.2.8	M
negIDRP-agi	Receipt of ISH PDU with SEL field of NET set to zero	5.5.3.5.2.8	M
autoRoute-agi	Inference of available routes from received NET of Airborne Router <del>NET</del>	5.5.3.5.2.12.1	M
initIDRP-agi	IDRP startup procedures - listenForOpen set to true	5.5.3.5.2.10	M
supISH-agi	Suppression of multiple ISH PDUs	5.5.3.5.2.10	O
valNET-agi	Validation of received NET	5.5.3.5.2.7	O

goOragSubnet: giSubnet ^ agSubnet

#### 5.3.5.2.14.6 Termination Procedures

Item	Description	ATN SARPs Reference	ATN CNS/ATM Package-1 Support
lvEvent	Processing of Leave Event	5.5.3.5.2.13	M
Watchdog	Watchdog Timer	5.5.3.5.2.13	M
ConfigWD	Configurability of Watchdog for Subnetwork Characteristics	5.5.3.5.2.13	O
conLeave	Processing of a per connection Leave Event	5.5.3.5.2.13	M
subnetLeave	Processing of a per-subnetwork Leave Event	5.5.3.5.2.13	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 Chapter 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. This section specifies the baseline Routing Policy for each class of RD identified in 5.2.5.2.2.2 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/G-ground routing only. Routing Policy rules for support of G-ground/-G-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.

*Note.— The routing policies expressed in this section do not constrain RD policies as much as define whether an RD's policies define it as being in the backbone or not.*

### 5.3.7.1.2 Adjacent ATN RDs within the Backbone RDC

*Note 1.— 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 Default and Security RIB-Atts :

- 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 2.— 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 3.— 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 4.—The objective of this rule is to ensure that a member of an ATN Island Backbone RDC will inform all other B-backbone RDC members within the island about all routes to 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 5.—The objective of this rule is to ensure that a member of an ATN Island Backbone RDC will tell other members of the same B-backbone RDC about all fixed RDs that it knows about.*

- d) Each selected route to a Mobile RD's "home".

*Note 6.—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 fixed RDs about all the "homes" that it knows about.*

*Note 7.—Such a route can be characterised by an NSAP Address Prefix which ends at the ADMVER field and the VER field takes either the value 041h or the value 0e1h.*

### 5.3.7.1.3 All other ATN RDs within the ATN Island

*Note 1.—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's 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~~ are not a members of the ATN Island's Backbone RDC, and for the Default and Security RIB-Atts :

- 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 2.—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 3.—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 4.—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 Mmobiles 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 all ATSC Classes supported for Air/Ground data interchange, if any.

*Note 5.—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 6.—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 7.—This route is formally the result of aggregating all the routes to Mmobile Ssystems 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 8.—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 Mmobile RDs which have “home” routes advertised.*

#### **5.3.7.1.4 Mobile RDs**

*Note 1.—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 IDRIP is being used to exchange routing information with an Aairborne 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 Default and Security RIB-Atts; the route’s destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the local RD.

*Note 2.—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 Mmobiles 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 3.—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 Mmobile 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 4.—The objective of this rule is to ensure that an RD that is a member of an ATN Island Backbone RDC will be willing to provide to each connected Mmobile RD routing information to the backbone of other*

*ATN islands.*

#### **5.3.7.1.5 ATN RDs in other ATN Islands**

*Note 1.—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 for the Default and Security RIB-Atts :

- a) An aggregated route to NSAPs and NETs contained within the ATN Island RDC.

*Note 2.—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 an ATN Island Backbone RDCs in different ATN Islands about the local ATN Island.*

- b) A route to the common NSAP Address Prefix for each group of Mobile RDs for which the "home" exists on the RD's ATN Island.

*Note 3.—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 Mmobiles whose “home” is in the local island.*

*Note 4.—The "home" identified above needs not correspond to a geographical notion of a home.*

*Note 5.—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.*

- c) A route to each Mobile RD for which the adjacent RD is advertising a route to the Mobile RD's "home".

*Note 6.—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.*

- d) A route to each Mobile RD for which there is no known home.

*Note 7.—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 an ATN Island Backbone RDCs in different ATN Islands about all of the Mobile RDs that ~~it~~<sup>they</sup> knows about.*

### **5.3.7.2 Routing Policy Requirements for a Mobile RD**

5.3.7.2.1 When IDRPs are 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 Default and Security RIB-Atts.

*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 1.—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 Default and Security RIB-Atts :

- 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 2.—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 3.—The objective of this rule is to ensure that an ATN TRD that is not itself a member of ~~the~~ an ATN Island Backbone RDC, will tell all adjacent ATN RDs which are members of ~~the~~ 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 4.—The objective of this rule is to ensure that a ATN TRD that is not itself a member of ~~the~~ an ATN Island Backbone RDC, will tell all adjacent ATN RDs which are members of ~~the~~ 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 5.—The objective of this rule is to ensure that a ATN TRD that is not itself a member of ~~the~~ an ATN Island Backbone RDC,*

will tell all adjacent ATN RDs which are members of ~~the~~ 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~~ 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 all ATSC Classes supported for Air/Ground data interchange, if any.

*Note 6.*—*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 1.*—*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 other ATN RDs which are members of the ATN Island Backbone RDC, and for the Default and Security RIB-Atts:

- a) A route to NSAPs and NETs contained within the RD for the Default and Security RIB-Atts; the route’s destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD.

*Note 2.*—*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 3.*—*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 34.*—*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 54.*—*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 Mmobiles, except when the RD is the source of this route.

*Note 65.*—*The objective of this rule is to ensure propagation of the default route to all Mmobiles 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 76.*—*The objective of this rule is to ensure routes to Mmobile RDs are propagated to off Bbackbone 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 all ATSC Classes supported for Air/Ground data interchange, if any.

*Note 87.*—*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 1.*—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 IDRPs 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 Default and Security RIB-Att-5; the route’s destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD.

*Note 2.*—The objective of this rule is to ensure that an ATN TRD will tell adjacent Mmobile RDs about itself.

5.3.7.3.4.2 **Recommendation.**—An ATN TRD should also provide to each adjacent Mobile RD, and for the Default and Security RIB-Att-5—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 3.*—The objective of this rule is to encourage an RD to provide to each adjacent Mmobile RD routing information ~~to~~ *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 Default and Security RIB-Att-5.

*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~~ *ese* policy statements *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.

### 5.3.8 Use of the Forwarding Information Base

The forwarding processes for a CLNP NDPUs 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. The next hop information found in this FIB entry is shall then be used to forward the NPDUs.

## 5.4. NETWORK AND TRANSPORT ADDRESSING SPECIFICATION

### 5.4.1 Introduction ~~General~~ Provisions

*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.— In general, where reference is made in this chapter to delegation of administrative responsibility by ICAO to States or organisations, it is expected that the practical effect of this delegation is that the respective States or organisations assume full administrative duties related to the delegated responsibilities. This means, for example, that if ICAO delegates to one or more States or organisations the responsibility for allocation, assignment and general administration of particular segments of the ATN address space, then those States or organisations must place into operation the necessary administrative structure to carry out the delegated allocation, assignment and administration activities. After having carried out the delegated administration of these field values, the State or organisation is then obliged to inform ICAO on a mutually agreed basis of administrative actions taken, so that ICAO may fulfill its responsibility as the ATN addressing authority in terms of publication and communication of this information for use by the civil aviation community. It is also important to note that a State or organisation may request delegation by ICAO of direct responsibility for its own administrative address space, if and when that State or organisation wishes to commence its own administrative activities. Finally, it is important to note that the role of ICAO in this area is one of international coordination,*

*advice and consultation in order to ensure orderly and efficient operation of the global aspects of the ATN. Thus, ICAO may be expected to provide counsel to States and organisations having assumed such delegated responsibilities, in order to ensure that address administration is carried out in a manner that supports the orderly and efficient global operation of the ATN ~~Internet~~*

#### 5.4.1.1 Addressing Plan Scope

5.4.1.1.1 The Aeronautical Telecommunication Network (ATN) OSI Network Service Access Point (NSAP) Internet Addressing Plan shall be used by ATN End Systems and Intermediate Systems participating in the aeronautical OSI.

*Note.— The ATN NSAP ~~Internet~~ Addressing Plan serves the needs of a variety of aeronautical data communication user groups, including Air Traffic Service Communications (ATSC) and Aeronautical Industry Services Communications (AINSC) users.*

#### 5.4.1.2 Addressing Plan Applicability

The ATN NSAP Addressing Plan shall be applicable to the identification of both fixed and mobile end systems and intermediate systems.

*Note.— The ATN Internet NSAP Addressing Plan defines the Network Layer and Transport Layer addressing information to be utilized by ATN End Systems, and by ATN Intermediate Systems.*

## 5.4.2 Network Layer Addressing

### 5.4.2.1 General Addressing Goal

#### 5.4.2.1.1

5.4.2.1.1.1 ATN NSAP addresses shall provide unambiguous identification of NSAPs and network entities located in ATN OSI End Systems and Intermediate Systems operating within the ATN OSI environment.

*Note.* — *When allocating NSAP addresses meeting this goal, it is important to consider the impact of address assignment strategies on the quantity and frequency of exchange of routing information. In other words, while it is given that the unambiguous identification of Network entities is the primary goal of the assignment of Network addresses, it is also true that without due caution, both routing information exchange efficiency and the resulting effectiveness of routing aggregation may be adversely affected. These effects must be considered when performing the administrative functions of address assignment and field value allocation.*

#### 5.4.2.1.2 Conformance to ISO Standards

5.4.2.1.2.1 ATN NSAP addresses shall conform to ISO/IEC 8348.

#### 5.4.2.1.3 ISO Address Format Definition

5.4.2.1.3.1 All ATN NSAP addresses shall use employ an ISO 6523-ICD IDI format and a binary abstract syntax DSP. an International Code Designator (ICD) format Domain Specific Part (DSP) using binary DSP syntax.

*Note.* — *This requires an AFI value of [47].*

#### 5.4.2.1.4 Subnetwork Independence

*Note.* — *The ATN NSAP Addressing Plan does shall not depend upon particular subnetwork address syntax, semantics or encoding techniques.*

*Note.* — *This facilitates the internetworking of End Systems and Intermediate Systems operated by various end-users and service providers within the aeronautical domain, while allowing these end-users and service*

*providers to retain local control of local End System and subnetwork operations.*

#### 5.4.2.1.5 Address Mapping

5.4.2.1.5.1 Routing and forwarding functions within ATN End Systems and Intermediate Systems shall perform any required mapping of ATN NSAP addresses formats to the SNPA addresses formats required for onward forwarding of CLNP packets. on interconnecting data subnetworks.

*Note.* — *For this reason, only ATN Host Computers (i.e. End Systems) and Routers (i.e. Intermediate Systems) need evaluate the contents of an ATN NSAP address.*

#### Address Transfer

ATN NSAP address information shall be transferred transparently between adjoining ATN Network Layer entities, by means of interconnecting data subnetworks. Valid ATN NSAP address syntaxes must transit unchanged via data encoding or data compression techniques employed in association with these interconnecting data subnetworks.

*Note.* — *ATN NSAP address formats may be carried over any aeronautical subnetwork which provides bit-oriented (i.e. transparent) transfer of subnetwork user data fields, including those fields carrying Network Layer protocol headers.*

#### 5.4.2.1.6 Definition of a Network Entity Title

*Note 1.* — *A Network Entity Title (NET) is the unique name of a Network Entity (NE) contained in an End System (ES) or in an Intermediate System (IS). It is used to unambiguously identify a given NE. An End or Intermediate System may comprise multiple NETs, in which case each will be identified by a unique NET.*

*Note 2.* — *NETs are assigned from the same addressing space as Network Service Access Point (NSAP) addresses. The authority which is responsible for allocating addresses from a given address space to NSAPs, may choose also to allocate NETs following the same procedures and rules it observes in the allocation of NSAPs.*

*Note 3.— NET's and NSAP addresses are syntactically indistinguishable; any value that the responsible authority is permitted to allocate as an NSAP address may be allocated as a NET.*

*Note 4.— The ATN NSAP Addressing Plan mandates specific values for the Selector (SEL) field for two types of NE's contained in ATN Intermediate Systems, as given in section 5.5.4.2.4.9.3*

#### **5.4.2.1.7 Network Addressing Administrative Domains**

*Note . — A Network Addressing Domain is a subset of a Global Network Addressing Domain consisting of all of the NSAP addresses that are assigned by one or more addressing authorities, as defined in ISO/IEC 8348.*

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

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

5.4.2.1.7.3 ATN Eend S-systems or Iintermediate S-systems located on-board general aviation aircraft shall belong to an ATSC Network Addressing administrative Ddomain, whereas ATN systems installed llocated on-board commercial aircraft shall belong to an AINSC Network Addressing administrative Ddomain.

#### **Administrative Provisions**

*Note.— This clause specifies general provisions applicable to the administration of the ATN internetwork addressing plan.*

##### **Syntax Administration**

The ATN NSAP address syntax (i.e. field boundaries, sizes and formats) shall be defined and administered by ICAO as the international aeronautical authority.

##### **Semantic Administration**

The ATN NSAP address semantics (i.e. field content and interpretation) shall be defined

and administered by ICAO as the international aeronautical authority.

*Note.— Authority for the semantic content of particular fields may be delegated by ICAO to other State, aeronautical and telecommunication standards authorities.*

##### **Encoding Administration**

The ATN NSAP address encoding procedures (i.e. the representation of abstract syntax and semantics in machine-readable form) shall be administered by ICAO as the international aeronautical authority.

*Note.— Authority for the encoding of particular fields may be delegated by ICAO to other State, aeronautical and telecommunication standards authorities.*

#### **5.4.2.2 Abstract Syntax Provisions**

##### **5.4.2.2.1 General**

5.4.2.2.1.1 The Domain Specific Part (DSP) of the ATN NSAP Addresses shall be represented in the binary abstract syntax.

*Note 1.— The Initial Domain Part (IDP) is specified in ISO/IEC 8348 to have a decimal abstract syntax.*

*Note 2.— For the purpose of administration and assignment of ATN NSAP Addresses, the NSAP address format includes nine fields, two of which comprise the IDP (AFI and IDI) and the remaining seven of which comprise the DSP. The AFI and IDI follow the ISO standard and thus have a decimal abstract syntax.*

*Note 3 . — However, e Certain DSP fields of ATN NSAP addresses are derived from existing ICAO and IATA registration schemes which do not specify them in a binary abstract syntax and are not specified in a native binary form.— Rules for the translation of their native abstract syntaxes to the required binary abstract syntax are provided in this specification.*



**5.4.2.2.2 Format Definition**

5.4.2.2.2.1 The ATN NSAP address format shall comprise nine (9) fields, as specified in Figure 5.4-1.

**5.4.2.2.3 Field Abstract Syntax**

5.4.2.2.3.1 The address field abstract syntax shall be as specified in Table 5.5.4-1.

**5.4.2.2.4 Field Syntax Construction**

5.4.2.2.4.1 All fields shall be right-justified,

*Note.—These field values are currently unassigned, and are retained by ICAO for future assignment.*

**Unassigned Values in Address Fields**

Address field values specified as "spare" shall be available for local use until assigned by ICAO.

*Note.—These field values are currently unassigned, and are retained by ICAO for future assignment.*

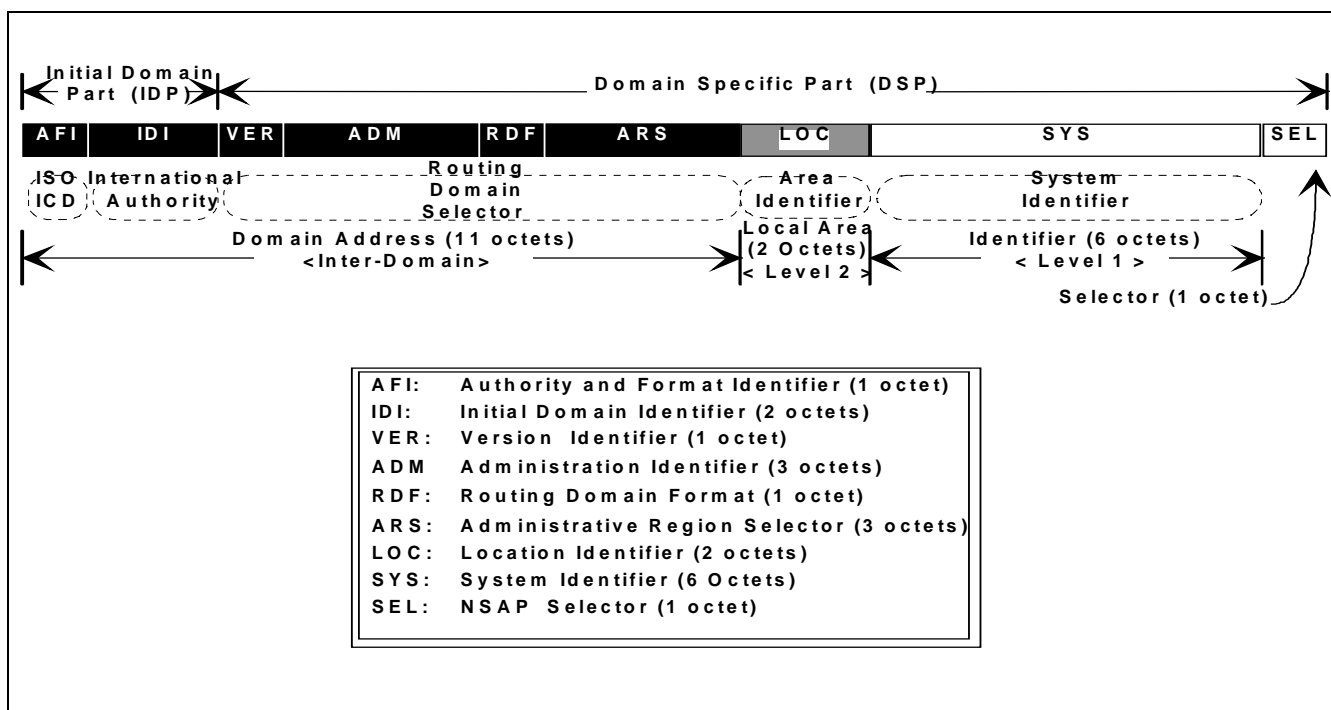


Figure 5.5.4-1 ATN NSAP Address Format

and shall be filled with leading "zero" digits (for decimal or hexadecimal syntax fields) or leading "\_" characters (for

alphanumeric syntax fields) as required to produce fields of specified fixed lengths.

**5.4.2.2.5 Reserved Values in Address Fields**

5.4.2.2.5.1 Address field values specified as "reserved" shall not be used until assigned by future versions of the specification.

**5.4.2.3 Encoding Provisions**

*Note.— This clause specifies general provisions applicable to the encoding rules of the ATN NSAP internet network Addressing Plan.*

**5.4.2.3.1 Field Encoding Definition**

5.4.2.3.1.1 The address field encoding shall be as specified in Table 5.5.4-1.

**5.4.2.3.2 Fill Bits**

Table 5.5.4-1 ATN NSAP Address Field Characteristics

<u>Address Field Name</u>	<u>Address Field Size</u>	<u>Field Abstract Syntax</u>	<u>Digit/Character Count</u>	<u>Field Encoding</u>
<u>AFI</u>	<u>1 Octet</u>	<u>Decimal</u>	<u>2 Digits</u>	<u>BCD</u>
<u>IDI</u>	<u>2 Octets</u>	<u>Decimal</u>	<u>4 Digits</u>	<u>BCD</u>
<u>VER</u>	<u>1 Octet</u>	<u>Hexadecimal</u>	<u>2 Digits</u>	<u>Binary</u>
<u>ADM</u>	<u>3 Octets</u>	<u>Hexadecimal</u>	<u>6 Digits</u>	<u>Binary</u>
<u>RDF</u>	<u>1 Octet</u>	<u>Hexadecimal</u>	<u>2 Digits</u>	<u>Binary</u>

5.4.2.3.2.1 Unspecified leading bits in all encoded fields shall be filled with the binary value zero<sup>“0”</sup>.

#### 5.4.2.3.3 Field Size

5.4.2.3.3.1 All encoded fields shall be fixed in size, as specified in Table 5.5.4-1.

#### 5.4.2.3.4 Encoding of Decimal Syntax

5.4.2.3.4.1 The BCD numeric digit set shall comprise the ten digits “0” through “9”. BCD field digits shall be represented with 4-bit binary numbers ranging in encoded decimal values from [0] through [9].

#### 5.4.2.3.5 Encoding of Hexadecimal Syntax

5.4.2.3.5.1 The hexadecimal digit set shall comprise the sixteen digits “0” through “9”, and “a” through “f”. Hexadecimal field digits shall be represented with 4-bit binary numbers ranging in encoded decimal values from [0] through [15].

#### 5.4.2.3.6 Encoding of Alphanumeric Syntax

5.4.2.3.6.1 The alphanumeric character set shall comprise the International Alphabet No. 5 (IA-5) character set, and shall be encoded according to IA-5 encoding rules.

#### 5.4.2.3.7 Encoding of Identifier Syntax

5.4.2.3.7.1 The identifier meta-character set shall comprise the list of all three-character identifiers composed from the character set including only:

- the decimal numerals “0” through “9”, with decimal ordinal values [0] through [9];
- the symbol “@”, with decimal ordinal value [10]; and,
- the upper-case alphabet “A” through “Z”, with decimal ordinal values [11] through [37].

5.4.2.3.7.2 The resulting list of identifier metacharacters shall comprise a range in abstract syntax from “000” through “ZZZ”, with an ordinal range in encoded decimal values from [0] through [50652].

*Note 1.*—This construct may be viewed as a three-digit radix-37 number.

*Note 2.*—This encoding mechanism is provided to support the optional mapping of certain IATA-defined character-based identifiers into binary address fields.

#### 5.4.2.4 Address Field Provisions

*Note 1.*—This clause specifies the detailed requirements for each of the nine fields which form the ATN NSAP address.

*Note 2.*—Field value specifications are enclosed in square brackets (i.e. [ ]), with syntax as noted (i.e. hexadecimal, decimal, alphanumeric or identifier).

#### 5.4.2.4.1 Authority/Format Identifier

*Note.*—The Authority/Format Identifier (AFI) field specifies the authority responsible for allocating values for the IDI field, the format of the IDI field, and the abstract syntax representation used for the Domain Specific Part (DSP) of the NSAP address.

##### 5.4.2.4.1.1 Format

5.4.2.4.1.1.1 The AFI field shall contain the two-digit decimal representation of the ATN NSAP Authority and Format Identifier.

##### 5.4.2.4.1.2 Administration

*Note.*—The AFI field value for an ATN NSAP address has been selected by ICAO from the set of values specified by ISO.

##### 5.4.2.4.1.3 Range

5.4.2.4.1.3.1 The AFI field value for an ATN NSAP address shall be [47], expressed as a decimal number.

##### 5.4.2.4.1.4 Encoding

5.4.2.4.1.4.1 The AFI field shall be encoded using BCD rules, as defined in 5.5.4.2.3.4.

#### 5.4.2.4.2 Initial Domain Identifier

*Note.*—The Initial Domain Identifier (IDI) field introduces shall specify the abstract syntax and semantics of the DSP portion of the ATN NSAP address.

##### 5.4.2.4.2.1 Format

5.4.2.4.2.1.1 The IDI field shall contain the four-digit decimal representation of the International Code Designator which defines an ICAO standardized-administered ATN NSAP DSP format.

##### 5.4.2.4.2.2 Administration

*Note.*—The IDI value of an ATN NSAP Addresses is registered with ISO as defined in ISO-6523.

#### 5.4.2.4.2.3 Range

5.4.2.4.2.3.1 The IDI field value for an ATN NSAP address shall be [0027], expressed as a decimal number.

##### 5.4.2.4.2.4 Encoding

5.4.2.4.2.4.1 The IDI field shall be encoded using BCD rules, as defined in 5.5.4.2.3.4.

#### 5.4.2.4.3 Version Identifier

*Note.*—Beside the version number of the ATN NSAP Addressing Plan which is applicable to the ATN NSAP address, the Version Identifier (VER) field identifies the type of the addressed object in terms of whether it belongs to a fixed or Mobile system, and whether it belongs to an ATSC or AINSC addressing domain. The Version Identifier (VER) field shall specify the version number applicable to the ATN NSAP address syntax, semantics and encoding.

##### 5.4.2.4.3.1 Format

5.4.2.4.3.1.1 The VER field shall contain the two-digit hexadecimal representation of the version number of for the ATN NSAP Addressing Plan applicable to the ATN NSAP address which represents

- a) the network addressing domain type (ATSC or AINSC), and
- b) whether the addressed object is contained in a mobile or fixed ATN system.

##### 5.4.2.4.3.2 Administration

*Note.*—The VER field value for an ATN NSAP address is defined by this specification and is administered, if required, through future versions of this specification ICAO.

##### 5.4.2.4.3.3 Range

5.4.2.4.3.3.1 The VER field value for Version 1 of an the AINSC ATN NSAP Address in fixed systems, expressed as a two-digit hexadecimal number, shall be [01].

5.4.2.4.3.3.2 The VER field value for Version 1 of the AINSC ATN NSAP Address in Mmobile systems, expressed as a two-digit hexadecimal number, shall be [41].

5.4.2.4.3.3.3 The VER field value for Version 1 of an the ATSC ATN NSAP Address in fixed systems, expressed as a two-digit hexadecimal number, shall be [81].

5.4.2.4.3.3.4 The VER field value for Version 1 of an the ATSC ATN NSAP Address in Mmobile systems, expressed as a two-digit hexadecimal number, shall be [c1].

*Note.— VER field values in the range [02 - 3f] may be allocated to fixed AINSC systems and VER field values in the range [42 - 7f] to Mobile AINSC systems in future versions of this specification. VER field values in the range [82 - bf] may be allocated to fixed ATSC systems and VER field values in the range [c2 - ff] to Mobile ATSC systems in future versions of this specification.*

Future versions of the AINSC ATN NSAP Address shall be allocated VER field values in the range [02]–[3f] for fixed systems and [42]–[7f] for mobile systems; these values shall be reserved until they are assigned.

Future versions of the ATSC ATN NSAP Address shall be allocated VER field values in the range [82]–[bf] for fixed systems and [c2]–[ff] for mobile systems;:

These values shall be reserved until they are assigned.

The VER field values [00], [40], [80] and [e0] shall be reserved.

#### 5.4.2.4.3.4 Encoding

5.4.2.4.3.4.1 The VER field shall be encoded using binary rules, as defined in 5.5.4.2.3.5.

#### 5.4.2.4.4 Administration Identifier

*Note . — The Administration Identifier (ADM) field shall specifies the organization responsible for administration of an ATN Network Addressing Administrative Domain.*

##### 5.4.2.4.4.1 Format

###### 5.4.2.4.4.1.1 General

5.4.2.4.4.1.1.1 The format of the ADM field shall be as given in 5.5.4.2.4.4.1.2 or 5.5.4.2.4.4.1.3, based on whether the organization responsible for administration of the associated ATN Network Addressing

Administrative Domain is an ATSC organization or an AINSC organization.

##### 5.4.2.4.4.1.2 ATSC Format

5.4.2.4.4.1.2.1 The ATSC ADM field shall contain the six-digit hexadecimal code for an ATSC Network Addressing Administrative Domain identifier.

5.4.2.4.4.1.2.2 This field value shall be derived from the set of three-character alphanumeric symbols representing a three-character ISO country designator as defined in ISO-3166.

##### 5.4.2.4.4.1.3 AINSC Format

5.4.2.4.4.1.3.1 The AINSC ADM field shall contain the six-digit hexadecimal code for an AINSC Network Addressing Administrative Domain identifier.

5.4.2.4.4.1.3.2 **Recommendation.**— *This field value should be derived from the set of three-character alphanumeric symbols representing an IATA Airline or Aeronautical Stakeholder Designator.*

##### 5.4.2.4.4.2 Administration

###### 5.4.2.4.4.2.1 General

5.4.2.4.4.2.1.1 ADM field values shall be administered by the authority given in 5.5.4.2.4.4.2.2 or 5.5.4.2.4.4.2.3, based on whether the associated ATN Network Addressing Administrative Domain is an ATSC domain or an AINSC domain.

###### 5.4.2.4.4.2.2 ATSC Administration

*Note. — ATSC ADM values are assigned by this specification, shall be assigned and administered by ICAO.*

*Note.— Authority may be further delegated to State authorities as required.*

###### 5.4.2.4.4.2.3 AINSC Administration

5.4.2.4.4.2.3.1 AINSC ADM values shall be assigned and administered by IATA.

*Note.— Authority may be further delegated to aeronautical industry authorities as required.*

**5.4.2.4.4.3 Range****5.4.2.4.4.3.1 General**

5.4.2.4.4.3.1.1 The range of ADM field values shall be determined as given in 5.5.4.2.4.4.3.2 or 5.5.4.2.4.4.3.3, based on whether the associated ATN Network Addressing Administrative Domain is an ATSC domain or an AINSC domain.

**5.4.2.4.4.3.2 ATSC Range**

5.4.2.4.4.3.2.1 The ATSC ADM field values shall be in the range [000000] - [ffffff], represented as hexadecimal numbers.

5.4.2.4.4.3.2.2 The ATSC ADM field shall contain the IA-5 encoding of valid three-character alphanumeric ISO Country Code values, as specified in ISO\_3166.

5.4.2.4.4.3.2.3 For this purpose, the ATSC ADM field shall be represented using upper-case alphabetic characters and decimal numerals.

**5.4.2.4.4.3.3 AINSC Range**

5.4.2.4.4.3.3.1 The AINSC ADM field values shall be in the range [000000] - [ffffff], represented as hexadecimal numbers.

5.4.2.4.4.3.3.2 **Recommendation.**—*The AINSC ADM field should contain the IA-5 encoding of valid three-character alphanumeric IATA Airline or Aeronautical Stakeholder Designator values, as specified in the IATA Airline Coding Directory.*—*For this purpose, the AINSC ADM field should be represented using upper-case alphabetic characters and decimal numerals.*

**5.4.2.4.4.4 Encoding**

5.4.2.4.4.4.1 The ADM field shall be encoded using alphanumeric rules, as defined in 5.5.4.2.3.6.

**5.4.2.4.5 Routing Domain Format**

The Routing Domain Format (RDF) field shall be reserved.

5.4.2.4.5.1 The RDF field value shall be [00] expressed as a two-digit hexadecimal number. Other RDF field values shall be reserved.

5.4.2.4.5.2 The RDF field shall be encoded using binary rules, as defined in 5.5.4.2.3.5.

**5.4.2.4.6 Administrative Region Selector**

*Note . — The Administrative Region Selector (ARS) field shall identify the routing domain of the addressed network entity or NSAP.*

*Note 1.— In the case of a fixed (i.e. ground-based) network entity, the ARS field will indicate the fixed routing domain within which that network entity is located.*

*Note 2.— In the case of a M#mobile (i.e. aircraft-based) network entity, the ARS field will indicate the identity of the M#mobile (i.e. aircraft) routing domain within which that network entity is located.*

**5.4.2.4.6.1 Format****5.4.2.4.6.1.1 General**

5.4.2.4.6.1.1.1 The format of the ARS field shall be as given in 5.5.4.2.4.6.1.2, 5.5.4.2.4.6.1.3, or 5.5.4.2.4.6.1.4, based on the authority responsible for the associated ATN Administrative Domain, and based on the value of the VER field.

**5.4.2.4.6.1.2 ATSC-Fixed Format**

5.4.2.4.6.1.2.1 The ATSC-Fixed ARS field shall contain the six-digit hexadecimal code for an ATN routing domain, when a “Fixed” VER value of [81] is present.

*Note.— An ATSC administration may opt to derive six-digit hexadecimal ATSC-Fixed ARS field value syntax from the IA-5 encoding of the three least-significant characters of a four-character alphabetic symbol representing an appropriate ICAO Location Indicator.*

**5.4.2.4.6.1.3 AINSC-Fixed Format**

5.4.2.4.6.1.3.1 The AINSC-Fixed ARS field shall contain the six-digit hexadecimal code for an ATN routing domain, when a “Fixed” VER value of [01] is present.

*Note.— An AINSC administration may opt to derive six-digit hexadecimal AINSC-Fixed ARS field value syntax from the IA-5 encoding of a three-character alphabetic symbol*

representing an appropriate IATA Location Identifier.

#### 5.4.2.4.6.1.4 Mobile Format

5.4.2.4.6.1.4.1 The Mobile-ARS field shall contain a six-digit hexadecimal number representing the 24-bit ICAO Aircraft Identifier, when a “Mobile” VER value of [4] or [c] is present.

#### 5.4.2.4.6.2 Administration

##### 5.4.2.4.6.2.1 General

5.4.2.4.6.2.1.1 ARS field values shall be administered by the authority given in 5.5.4.2.4.6.2.2, 5.5.4.2.4.6.2.3, or 5.5.4.2.4.6.2.4, based on the value of the VER field.

##### 5.4.2.4.6.2.2 ATSC-Fixed Administration

5.4.2.4.6.2.2.1 ATSC ARS values shall be assigned and administered by ICAO.

*Note.— Authority may be further delegated to State authorities as required.*

##### 5.4.2.4.6.2.3 AINSC-Fixed Administration

5.4.2.4.6.2.3.1 AINSC ARS values shall be assigned and administered by IATA.

*Note.— Authority may be further delegated to aeronautical industry authorities as required.*

##### 5.4.2.4.6.2.4 Mobile Administration

5.4.2.4.6.2.4.1 Mobile ARS values shall be assigned and administered by ICAO.

*Note.— Authority may be further delegated to State authorities as required.*

##### 5.4.2.4.6.3 Range

5.4.2.4.6.3.1 ARS field values shall be in the range [000000]-[ffffff], expressed as hexadecimal numbers.

##### 5.4.2.4.6.4 Encoding

5.4.2.4.6.4.1 The ARS field shall be encoded using binary rules, as defined in 5.5.4.2.3.5.

##### 5.4.2.4.6.5 Default Value

5.4.2.4.6.5.1 If an ATN administrative domain chooses not to allocate fixed ARS field values (i.e. chooses not to partition the administrative domain into routing domains), then the value of the ARS field for all fixed addresses within that ATN administrative domain shall be [000001].

5.4.2.4.6.5.2 No default ARS field value shall be defined or allowed for Mmobile routing domains.

#### 5.4.2.4.7 Location Identifier

*Note .— The Location Identifier (LOC) field may shall be used for partitioning the address space administered by a single ATN routing domain authority into more than one routing area.*

##### 5.4.2.4.7.1 Format

###### 5.4.2.4.7.1.1 General

5.4.2.4.7.1.1.1 The format of the LOC field shall be as given in 5.5.4.2.4.7.1.2, 5.5.4.2.4.7.1.3 or 5.5.4.2.4.7.1.4, based on the authority responsible for the associated ATN Network Addressing Administrative Domain, and based on the value of the VER field.

###### 5.4.2.4.7.1.2 ATSC Format

5.4.2.4.7.1.2.1 The ATSC-Fixed LOC field shall contain the four-digit hexadecimal code for an ATN routing area identifier, when an “ATSC” ADM value is present in combination with a “Fixed” VER value of [8].

*Note.— An ATSC administration may opt to derive four-digit hexadecimal ATSC LOC field value syntax from the three least-significant characters of a four-character identifier meta-character representing appropriate ICAO Location Indicators, encoded using ordinal rules defined in 5.5.4.2.3.7.*

###### 5.4.2.4.7.1.3 AINSC Format

5.4.2.4.7.1.3.1 The AINSC-Fixed LOC field shall contain the four-digit hexadecimal code for an ATN routing area identifier, when an “AINSC” ADM value is present in combination with a “Fixed” VER value of [0].

*Note.*— An AINSC administration may opt to derive four-digit hexadecimal AINSC LOC field value syntax from a three-character identifier meta-character representing appropriate IATA Location Identifiers, encoded using ordinal rules defined in 5.5.4.2.3.7.

#### 5.4.2.4.7.1.4 Mobile Format

5.4.2.4.7.1.4.1 The Mobile-LOC field shall contain the four-digit hexadecimal code for an ATN routing area identifier, when a “Mobile” VER value of **[41]** or **[c1]** is present.

#### 5.4.2.4.7.2 Administration

5.4.2.4.7.2.1 LOC field values shall be administered by the authority designated in the ADM field.

#### 5.4.2.4.7.3 Range

5.4.2.4.7.3.1 LOC field values shall be in the range **[0000]**-**[ffff]**, expressed as hexadecimal numbers.

#### 5.4.2.4.7.4 Encoding

5.4.2.4.7.4.1 The LOC field shall be encoded using binary rules, as defined in 5.5.4.2.3.5.

#### 5.4.2.4.7.5 Default Value

5.4.2.4.7.5.1 If an ATN routing domain administration chooses not to allocate LOC field values (i.e. chooses not to partition the routing domain into routing areas), then the value of the LOC field for all addresses within that ATN routing domain shall be **[0001]**.

#### 5.4.2.4.8 System Identifier

*Note.* — *The System Identifier (SYS) field shall identify the Eend S-system or Intermediate S-system containing the addressed Network entity or NSAP.*

#### 5.4.2.4.8.1 Format

5.4.2.4.8.1.1 The format of the SYS field shall be determined by the authority designated in the ADM field.

#### 5.4.2.4.8.2 Administration

5.4.2.4.8.2.1 The SYS field shall be administered by the authority designated in the ADM field.

#### 5.4.2.4.8.3 Range

5.4.2.4.8.3.1 SYS field values shall be in the range **[000000000000]**-**[ffffffffffff]**, expressed as hexadecimal numbers.

#### 5.4.2.4.8.4 Encoding

5.4.2.4.8.4.1 The SYS field shall be encoded using binary rules, as defined in 5.5.4.2.3.5.

#### 5.4.2.4.9 NSAP Selector

*Note.* — *The NSAP Selector (SEL) field shall identify the Eend S-system or Intermediate S-system network entity or network service user process responsible for originating or receiving Network Service Data Units (NSDUs).*

#### 5.4.2.4.9.1 Format

5.4.2.4.9.1.1 The SEL field shall contain the two-digit hexadecimal representation of a network entity or network service user protocol selector.

#### 5.4.2.4.9.2 Administration

5.4.2.4.9.2.1 SEL field values in the range **[01]**-**[fd]** shall be assigned and administered by the authority designated in the ADM field.

*Note.* — *Authority may be further delegated by the designated authority as required.*

#### 5.4.2.4.9.3 Range

5.4.2.4.9.3.1 Valid SEL field values shall be in the range **[00-ff]**.

5.4.2.4.9.3.2 The SEL field value for an Intermediate S-system network entity shall be **[00]**, except for the case of an airborne Intermediate S-system implementing the procedures for the optional non-use of not supporting IDRP.

5.4.2.4.9.3.3 In that case, the SEL field value shall be **[fe]**.

5.4.2.4.9.3.4 The SEL field value **[ff]** shall be reserved.

*Note.* — *SEL field values in stand-alone End-Systems (i.e. in End-Systems not co-located with Intermediate-Systems) are not constrained.*

**5.4.3.6.2 Recommendation.** — *TSAP selector values in the range [0] – [255] should be encoded using one octet, higher values should be encoded using two octets.*

#### 5.4.2.4.9.4 Encoding

5.4.2.4.9.4.1 The SEL field shall be encoded using binary rules, as defined in 5.5.4.2.3.5.

### 5.4.3 Transport Layer Addressing

#### 5.4.3.1 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.*

#### 5.4.3.2 ATN TSAP Selector

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

#### 5.4.3.3 Format

5.4.3.3.1 The TSAP Selector field shall be interpreted as an unsigned binary integer.

#### 5.4.3.4 Administration

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

#### 5.4.3.5 Range

5.4.3.5.1 Valid ATN TSAP Selector field values shall be in the range [0] – [65535].

#### 5.4.3.6 Encoding

5.4.3.6.1 The TSAP Selector field shall be encoded using binary rules, as defined in 5.5.4.2.3.5.



## 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 8073:1992 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.*

#### References

ISO/IEC 8073:1992 Information Technology—  
Telecommunications and Information  
Exchange between Systems—Open Systems  
Interconnection—Protocol for providing the  
Connection-mode Transport Service

ISO/IEC 8602 Information Processing Systems—  
Open Systems Interconnection—Protocol for

providing the Connectionless-mode Transport Service.

#### 5.5.1.2 Transport Service Description

*Note 1.*— *When the TS-user USER requires use of the connection mode transport protocol the TS-user USER will provide the following information to the TS-provider 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 or non-use of the transport checksum is allowed;
- d) the Application Service Priority to be mapped into the resulting CLNP NPDU's according to *Sub-Volume 1, Table 1.2-2 (Relationship of communication priorities)*;
- 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 USER will additionally provide the traffic category sub-type, i.e. Air Traffic Services Communications (ATSC) or Aeronautical Operational Control Communications (AOCC).*

*Note 3.*— *In the case of the ATSC traffic category sub-type the TS-user USER will further specify the required ATSC Class of*

*Communications Service from Class as defined in Table 1.2-1, or no traffic type policy preference-A to Class H.*

*Note 4. — In the case of the AOC ~~traffic category~~ sub-type the TS-user ~~USER~~ will further specify the subnetwork preference (including no preference).*

*Note 5. — The ATN Traffic Types and their associated ~~traffic categories~~ sub-types are specified in ~~Chapter 5.6, Table 5.6-1~~. The encoding of the ATN Security Label is specified in ~~Chapter 5.6, Figure 5.6-1 and section 5.6.2.2.2~~ bullet b)2.*

*Note 6. — The TS-user ~~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 Chapter 5.4.

### Network Service Specification

~~1. The COTP shall operate using the CLNS (Connectionless Network Service) as specified in Chapter 5.6.~~

*Note. — TPDU's (Transport Protocol Data Units) are sent via the N-UNITDATA Request primitive.*

### 5.5.1.4 Exchange of Transport-Selector parameters

*Note 1. — 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 Chapter 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 2. — 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 ~~OSI~~ 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~~ specified 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 Connection Mode Transport Protocol Overview

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 network.

*Note.*— The ATN COTS model conforms to the model defined in ISO/IEC 8072.

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

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

5.5.2.2.3 The transport entity shall not concatenate TPDU from TCs with different transport priorities or different security label types.

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 TPDU.

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 1.*— This is to support efficient transmission of anticipated application data exchanges, a TPDU size resulting from TPDU size negotiation (using either the maximum TPDU size or the preferred maximum TPDU size parameters) of at least 1024 octets is recommended.

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

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.

*NEF3:— Note 21.*— Because the increased TPDU size resulting from use of extended data TPDU numbering may be more inefficient, this option ~~is should be~~ 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 **Recommendation.**— The following timers and variables should be configurable on a TC basis:

- the local retransmission timer (TI),
- the acknowledgement timer (AL),
- the window update timer (W),
- the inactivity timer (I),
- the frozen reference time (L),
- the maximum retransmission number (N),
- the persistence timer (R).

### 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) TS-user to specify 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 transport connection priority, the relationship between this TC transport connection priority and the CLNP priority shall be as specified in Sub-Volume 1, Table 1.2-2, (Relationship of communication priorities).

#### 5.5.2.3.2 Connection Mode Transport Security

*Note 1.*— The ATN security mechanism does not make use of the ISO/IEC 8073 Protection parameter. The support of the Protection parameter is therefore optional for CNS/ATM-I Package.

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 encoded according to the provisions of Chapter 5.6, section 5.2.7.15.6.2.2.1. The Ttransport Layer shall not alter the Security Label specified by the TS-user.

*Note 2 . — When no Security Label is present, a « General Communications » traffic type is implied. In this case, CLNP NPDUs are generated without the Security parameter.*

The transport layer shall treat all connections without expressed security as default security.

The default security shall be the zero-length Security Label value indicating « General Communications » traffic.

*Note.—When default security label is specified, NPDUs are generated without CLNP Security parameter.*

### 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 TPDU's shall conform to ISO/IEC 8073 for the COTP.

#### 5.5.2.4.2 Encoding of the Acknowledgment Time Parameter Implementation

5.5.2.4.2.1 For use in the ATN compliant systems, the acknowledgement time parameter of the CR and CC TPDU's (A<sub>L</sub>) shall be encoded as follows modified according to the following:

Parameter Code: 1000 0101

*Note 1. — This is identical to the ISO/IEC 8073 standard parameter*

Parameter Length: 2 or 3 octets (up to 24 bits).

Parameter Value: Acknowledgment Timer (A<sub>L</sub>) value expressed in milliseconds (per ISO/IEC 8073 standard)

*Note 21 . — This ~~enhancement~~change is in response to the unique requirements of the aeronautical environment which may require longer acknowledgment times than foreseen in ISO/IEC 8073.*

*Note 32. — Initial values of these timers ~~may~~will be dependant upon the subnetwork, traffic type and routing policy requirements expressed in the associated ATN Security Label.*

*Note 43. — In cases where the A<sub>L</sub> value is expressed in 2 octets (less than 65,536 milliseconds), the ATN implementation will behave in compliance with the ISO/IEC 8073 standard.*

*Note 54. — Implementors are advised to permit systems administrators to readily specify such initial values.*

### 5.5.2.5 Transport Layer Congestion Avoidance

#### 5.5.2.5.1 General

*Note 1.— The congestion avoidance mechanisms in the Ttransport Layer make use of the notification by the Nnetwork Layer of Congestion Experience flags in received NPDUs. This mechanism allows transport entities to reduce the window, i.e. the number of DT TPDU's 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 oriented transport service only.*

*Note 4.— The algorithm defined in this section is applied for each transport connection individually.*

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 NPDU's that convey DT-TPDUs, and a count  $NC$

equal to the number of such NPDU's 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  $\lambda$  % of the count  $N$ , the receiving transport entity shall increase the size of the advertised window by adding  $\delta$  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  $\beta$ . 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 5.5-1. Congestion Avoidance algorithm values**

Name	Description	Recommended
------	-------------	-------------

		value/range
$\beta$	Window decrease factor	0.75 to 0.95
$\delta$	Window increase amount	1
$W_0$	Initial window	1
$\lambda$	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 Nnetwork Llayer.*

**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 Ttransport Llayer shall use the N-UNITDATA Request primitive, as defined in ISO/IEC 8073, to transmit TPDU(s).

*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 TPDU(s) as NS-user-data of the N-UNITDATA Request primitive.*

**5.5.2.6.1.3 Network Service Access Point Addresses**

*Note.— The Ttransport Llayer 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 Sub-Volume 1, Table 1.2-2 (Relationship of communication priorities).

5.5.2.6.1.4.2.3 If the Ttransport Llayer supports levels of TC priority numerically greater than 14, TPDU(s) associated with the TC shall be transmitted using a network priority level of zero.

*Note.— As specified in ISO/IEC 8073, the Ttransport Llayer priority level zero is highest. ISO/IEC 8473 specifies zero as the lowest network priority and fourteen as the highest. Sub-Volume 1, Table 1.2-2 (Relationship of communication priorities) defines the required provides a suitable 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 Nnetwork Llayer security is specified in 5.2.7.34.1.*

**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 Ttransport Llayer shall be capable of receiving TPDU(s) 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 TPDU(s) as NS-user-data of the N-UNITDATA Indication primitive.*

**Network Service Access Point Addresses**

*Note.— The source and destination address parameters supplied to the COTP by the CLNS via the N-UNITDATA primitive supports the ATN NSAP addressing plan as specified in Chapter 5.4.*

**Network Quality of Service**

**Network Layer Security:**

*Note.—The use of the network layer security is specified in 5.2.7.4.1.*

## **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 ~~file~~ Requirements List (APRL). ~~The APRL has been prepared using the PICS (Protocol Implementation Conformance Statement) —proforma provided with ISO/IEC 8073. The APRL conventions are described in Part 1 of the CNS/ATM-1 Package SARPs.~~*

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**

*The ATN-COTP shall implement the features marked "M" in the table.*

<b>Index</b>	<b>Class</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
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:**

The CNS/ATM-1 ATN COTP shall implement the features marked "M" in the table.

<b>Index</b>	<b>Feature</b>	<b>ATNCNS/ATM-1 Package - Support</b>
—ATN1	Initiating CR TPDU?	M
—ATN2	Responding to CR TPDU?	M
—ATN3	Extended TPDU Numbering?	Ø
—ATN4	Acceptance of Non-use of Checksum?	M
—ATN5	Use of Concatenation?	Ø
—ATN6	Use of Selective Acknowledgement?	Ø
—ATN7	Use of Request of Acknowledgment?	Ø
—ATN8	Reduction of Credit Window?	M
—ATN9	ER TPDU Transmission?	Ø
—ATN10	Use of Called Transport Selector Parameter in CR TPDU?	M
—ATN11	Use of Calling Transport Selector Parameter in CR TPDU?	M
—ATN12	Use of TPDU Size Parameter in CR TPDU?	Ø
—ATN13	Use of the Additional Option Selection Parameter in CR TPDU?	M
—ATN14	Use of the Priority Parameter in CR TPDU?	M
—ATN15	Use of the Acknowledgment Timer Parameter in CR TPDU?	M
—ATN16	Use of Preferred Maximum TPDU Size Parameter in CR TPDU?	Ø
—ATN17	Use of Inactivity Time Parameter in CR TPDU?	M
—ATN18	Use of Called Transport Selector Parameter in CC TPDU?	M
—ATN19	Use of Calling Transport Selector Parameter in CC TPDU?	M
—ATN20	Support of TPDU Size Parameter in CC TPDU?	Ø

Index	Feature	SARPs Reference	ATNCNS/ATM-1 Package Support
ATN21	Use of the Additional Option Selection Parameter in CC TPDU?		M
ATN22	Use of the Priority Parameter in CC TPDU?		M
ATN23	Use of the Acknowledgment Timer Parameter in CC TPDU?		M
ATN24	Use of Preferred Maximum TPDU Size Parameter in CC TPDU?		Ø
ATN25	Use of Inactivity Time Parameter in CC TPDU?		M
ATN26	1024 octets as the minimum preferred maximum TPDU size in a CR TPDU?		Ø
ATN27	1024 octets as the minimum preferred maximum TPDU size in a CC TPDU?		Ø
ATN28	1024 octets as the largest value of the maximum TPDU size parameter in a CR TPDU with preferred class 4?		Ø
ATN29	1024 octets as the largest value of the maximum TPDU size parameter which may be sent in a CC TPDU when class 4 is selected?		Ø
ATN130	Support of Congestion Avoidance Procedures/Measures?	5.5.5.2.5	M
ATN231	Quality of Service Transport to Network Priority Mapping?	5.5.5.2.6.1.4.2	M
ATN3	Support of ATN Security Label	5.5.5.2.6.1.4.3	M
ATN432	Timer Settings on a per Transport Connection basis?	5.5.5.2.2.12	O
ATN5	Enhanced encoding of Acknowledgment Time Parameter	5.5.5.2.4.2	M

Note.— ATN 31 refers to:

—— a) the passing of the CE bit and the security parameter between the transport and the network entity, and

—— b) the mapping of the priority value between the transport and the network entity

### 5.5.2.7.1.3 Initiator/Responder Capability for Protocol Classes 0-4

The ATN transport protocol shall implement the features marked "M" in the table.

<b>Index</b>		<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
IR1	Initiating CR TPDU	14.5 a)	O.2	M
IR2	Responding to CR TPDU	14.5 a)	O.2	M

*Note.* — ISO 8073 requires that at least one of these options shall be implemented.

**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:**

*The ATN-COTP shall implement the features marked "M" in the table.*

<b>Index</b>	<b>Function</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
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 TPDU's (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.**

*The ATN COTP shall implement the features marked "M" in the table.*

<b>Index</b>	<b>Function</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
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 TPDU's 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.**

*The ATN COTP shall implement the features marked "Predicate:M" in the table if the predicate is true, i.e. the ATN recommendation has been followed.*

<b>Index</b>	<b>Feature</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
T4F28	Data TPDU numbering (extended)	6.10	O	<u>Q</u> ATN3:M
T4F29	Non-use of checksum	6.17	O	ATN4:M
T4F30	Concatenation	6.4	O	<u>Q</u> ATN5:M
T4F31	Retention and acknowledgement of TPDU's  Use of selective acknowledgement	6.13.4.3	O	<u>Q</u> ATN6:MO
T4F32	Retention and acknowledgement of TPDU's  Use of request acknowledgement	6.13.4.2	O	<u>Q</u> ATN7:MO

*Note.~The classification "MO" indicates mandatory to implement, optional to use.*

5.5.2.7.1.5 Supported TPDU's

The ATN-COTP shall implement the features marked "M" in the table.

Index	TPDU's		ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package Support
ST1	CR	supported on transmission	13.1	IR1:M	M
ST2	CR	supported on receipt	13.1	IR2:M	M
ST3	CC	supported on transmission	13.1	IR2:M	M
ST4	CC	supported on receipt	13.1	IR1:M	M
ST5	DR	supported on transmission	13.1	IR2:M	M
ST6	DR	supported on receipt	13.1	IR1:M	M
ST7	DC	supported on transmission	13.1	C4L:M	M
ST8	DC	supported on receipt	13.1	C4L:M	M
ST9	DT	supported on transmission	13.1	M	M
ST10	DT	supported on receipt	13.1	M	M
ST11	ED	supported on transmission	13.1	C4L:M	MO
ST12	ED	supported on receipt	13.1	C4L:M	MO
ST13	AK	supported on transmission	13.1	C4L:M	M
ST14	AK	supported on receipt	13.1	C4L:M	M
ST15	EA	supported on transmission	13.1	C4L:M	MO
ST16	EA	supported on receipt	13.1	C4L:M	MO

ST19	ER	supported on receipt	13.1	M	M
------	----	----------------------	------	---	---

Note.— The following table states for which classes, if any, ER TPDU is supported on transmission:

Index	Class	ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package Support
SER4L	Class 4 over CLNS	6.22.2	O	<u>O</u> ATN9:M

#### 5.5.2.7.1.6 Supported Parameters of Issued TPDUs

##### 5.5.2.7.1.6.1 Parameter Values for CR TPDU (C4L::)

If the additional options selection parameter is issued in a CR TPDU it is mandatory that:

Index	feature	ISO/IEC 8073 Reference	ISO Status	ATN Support
ICR1	Bits 8 to 7 in the <u>additional options selection parameter of a CR TPDU shall be set to zero?</u>	13.3.4 g)	<u>M</u>	<u>M</u>

##### 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	ATNCNS/ATM-1 Package 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:

5.5.2.7.1.6.2.1.1 The ATN COTP shall implement the features marked "M" in the table.

Index	Supported parameters	ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package 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	<u>O</u> ATN12:MO
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	<u>M</u> ATN14:M
I4CR16	Transit delay	13.3.4 p)	O	O
I4CR17	Acknowledgement time	13.3.4 j)	O	<u>M</u> ATN15:M
I4CR18	Preferred maximum TPDU size	13.3.4 c)	O	<u>O</u> ATN16:MØ
I4CR19	Inactivity timer	13.3.4 r)	O	ATN17:M



**5.5.2.7.1.6.2.2 Optional Parameters for a Connection Confirm TPDU:**

*Note.* — 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	ATNCNS/ATM-1 Package 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	<u>O</u> ATN20:M
I4CC9	Protection parameters	13.4.4	O	O
I4CC10	Additional option selection	13.4.4	O	M
I4CC11	Acknowledgement time	13.4.4	O	ATN23:M
I4CC12	Throughput	13.4.4	O	O
I4CC13	Residual error rate	13.4.4	O	O
I4CC14	Priority	13.4.4	O	ATN22:M
I4CC15	Transit delay	13.4.4	O	O
I4CC16	Preferred maximum TPDU size	13.4.4	I4CR18:O	<u>O</u> ATN24:M
I4CC17	Inactivity timer	13.4.4	O	ATN25:M

*I4CC10:: Note.* — 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	ATNCNS/ATM-1 Package 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	ATNCNS/ATM-1 Package Support
I4DT4	ROA	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 if an AK TPDU is issued in Class 4.

<b>Index</b>	<b>Supported parameter</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
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.*

<b>Index</b>	<b>Supported parameters</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
I4AK5	Subsequence number	13.9.4. b)	O	ATN8: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.*

<b>Index</b>	<b>Supported parameter</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
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**

<b>Index</b>	<b>Supported parameter</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
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:

**5.5.2.7.1.7.1.1 The ATN COTP shall implement the features marked "M" in the table.**

Index	TPDU	ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package 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:)**

The ATN COTP shall implement the features marked "M" in the table.

Index	User Data	ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package Support
D4ICR	User data of up to 32 octets in a CR with preferred class 4	13.3.5	M	M
D4ICC	User data of up to 32 octets in a CC	13.4.5	M	M
D4IDR	User data of up to 64 octets in a DR	13.5.5	M	M

**5.5.2.7.1.9 User Data in Received TPDU**

The transport layer shall be able to receive the following:

Index	User Data	ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package 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	ATNCNS/ATM-1 Package 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	ATNCNS/ATM-1 Package Supported values
NAC5	Class 4 over CLNS	6.5.5 j)	None	None

NAC5.—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	ATNCNS/ATM-1 Package 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	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	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	ATNCNS/ATM-1 Package 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, as defined in ISO 8073	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	ATNCNS/ATM-1 Package 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

*TS3, TS4:—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	Allowed Values	ATNCNS/ATM-1 Package 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	ATNCNS/ATM-1 Package 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

NEF3, NEF6:::Note.— This table does not preclude proposal of the extended format.

5.5.2.7.1.10.5 Expedited data Transport service

The ATN-COTP shall implement the feature marked "M" in the table.

Note.— Use of the feature is optional.

Index	Expedited data	ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package Supported values
TED1	Is the expedited data indication supported in CR and CC TPDU?	6.5.5 r)	M	MO

TED1:::Note.— Expedited data is proposed using the Additional Options Parameters in the CR and CC TPDU.

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	ATNCNS/ATM-1 Package 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

NUC1:::Note 1.— A Transport Layer is able to propose either use or non-use of checksum in a CR TPDU.

NUC2:::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**

<b>Index</b>	<b>Selective Acknowledgement</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
USA1	Is use of selective acknowledgement proposed in CR TPDU's ?	6.5.5 s)	O	ATN6:M
USA2	Is use of selective acknowledgement selected in a CC when it has been proposed in a CR ?	6.5.5 s)	O	ATN6:M

**5.5.2.7.1.10.8 Use of Request Acknowledgement**

<b>Index</b>	<b>Request of Acknowledgement</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
ROA1	Is use of request of acknowledgement proposed in CR TPDU's ?	6.5.5 t)	O	ATN7:M
ROA2	Is use of request of acknowledgement selected in a CC when it has been proposed in a CR ?	6.5.5 t)	O	ATN7:M

**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**

<b>Index</b>	<b>Item</b>	<b>ISO/IEC 8073 References</b>	<b>Values</b>	
			<b>ISO Allowed</b>	<b>ATNCNS/ATM-1 Package Supported</b>
PE4L	Class 4 over CLNS	6.22.2	ER, DR, Discard	ER, DR, Discard

*PE0-PE3:: Note.*— N/A

*PE4L:: 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

5.5.2.7.1.11.2.1 The ATN COTP shall implement the features marked "M" in the table.

Index	Event	ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package Support
RR1	A parameter not defined in ISO 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 h)	M	M

Index	Event	ISO/IEC 8073 Reference	Value	
			ISO Allowed	ATNCNS/ATM-1 Package Supported
RR7	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

RR7: 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****5.5.2.7.1.11.3.1 The ATN-COTP shall implement the features marked "M" in the table.**

<b>Index</b>	<b>Event</b>	<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
U11	A parameter not defined in ISO 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 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****The ATN-COTP shall implement the features marked "M" in the table.**

<b>Index</b>		<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
TA1	T1 (Local Retransmission)	12.2.1.1.4	M	M
TA2	N (Maximum Transmission)	12.2.1	M	M
TA3	I <sub>L</sub> (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

<b>Index</b>		<b>ISO/IEC 8073 References</b>	<b>ISO Status</b>	<b>ATNCNS/ATM-1 Package Support</b>
ATN-TA1	R (Persistence)	12.2.1.1.5	O	O
ATN-TA2	M <sub>LR</sub> (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA3	M <sub>RL</sub> (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA4	E <sub>LR</sub> (Maximum Transmission Delay)	12.2.1.1.2	O	O

ATN-TA5	$E_{RL}$ (Maximum Transmission Delay)	12.2.1.1.2	O	O
ATN-TA6	$A_L$ (Acknowledgement Time)	12.2.1.1.3	O	ATN15:M
ATN-TA7	$A_R$ (Acknowledgement Time)	12.2.1.1.3	O	ATN15:M
ATN-TA8	$I_R$ (Inactivity Time)	12.2.1.1.7	O	ATN17:M

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

Index		ISO/IEC 8073 References	ISO Status	ATNCNS/ATM-1 Package Support
OT9	Does IUT support optional timer TS2 when operating in class 4?	6.22.2.3	O	O

## 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 Internetwork.

*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 5.5.5.3.5.

### 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 OSI Transport Layer to its user is described in ISO/IEC 8072.

*Note 2.* — ISO/IEC 8072 limits CL user-data to a maximum of 63-488 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 Chapter 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 **Recommendation.**— The Transport Layer shall ~~o~~uld support the use dynamic selection 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 use the TSDU Ssecurity Llabel in —the T-UNITDATA request provided in the T-UNITDATA request as the value of the N-UNITDATA security parameter.

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

### Protocol Implementation

### 5.5.3.4 Encoding of Transport Protocol Data Units

5.5.3.4.1.1 The encoding of TPDU's 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.

#### General

The CLTP shall use the NS primitives described in Chapter 6 for the transmission and reception of TPDU's.

*Note.*— The method of parameter exchange between the TE and the NS is a local matter.

#### 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 TPDU(s).

**5.5.3.5.1.2 NS-user-data**

The length indicated shall be no different from the length of the TPDU(s).

*Note.*— *Transport Entities transmit TPDU(s) as NS-user-data of the N-UNITDATA Request primitive.*

**5.5.3.5.1.3 Network Service Access Point Addresses**

*Note.* — *The Ttransport Llayer 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 Sub-Volume 1, Table 1.2-2, (Relationship of communication priorities).

**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 Ssecurity Llabel 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 Ttransport Llayer receives TPDU(s) from the Nnetwork Llayer-provided N-UNITDATA Indication primitive.*

**Network Service Access Point Addresses**

*Note.*— *The source and destination address parameters supplied to the CLTP by the NS via the N-UNITDATA Indication primitive supports the ATN NSAP addressing plan as specified in Chapter 5.4.*

**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—application service priority to network layer priority, and shall perform the inverse operation on reception, using the mapping shown in Sub-Volume 1, Table 1.2-2, (Relationship of communication priorities).

**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 Before use in an ATN End System, the transport protocol implementor shall provide a completed PICS for the ISO transport protocol implementation, using the PICS proforma provided with ISO/IEC 8602, including any extensions to that proforma provided with this material. 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.

The ATN-CLTP shall implement the features marked "M" in the table.

Item	Protocol Function Support	ISO/IEC 8602 Reference	ISO Status	ATNCNS/ATM-1 Package Support
NS	Network service selection	5.3.2.2	M	M
AM	Address mapping	5.3.2.3	M	M
<b>PDU Support</b>				
UD1	Unitdata PDU supported on transmission	6.1.3	M	M
UD2	Unitdata PDU supported on reception	6.1.3	M	M
<b>Parameters of the Unitdata PDU on Transmission</b>				
TpTc	<t> TPDU UD Checksum	6.2.4.1	O	M
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	O	M
<b>Parameters of the Unitdata PDU on Reception</b>				
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
<b>Service Support</b>				
CL	Connectionless Mode Network Service	6.2	M	M

## 5.6. INTERNETWORK SERVICE AND PROTOCOL SPECIFICATION

### 5.6.1 Introduction

*Note.* The ATN Internetwork comprises a number of interconnected ATN routers and constituent subnetworks supporting packet data communication among host computers operating the ATN Internet protocols.

*Note.* All ATN NPDUs (Network Protocol Data Units) (packets) 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 all ATN Internet protocols is are connectionless, any information required to process a particular NPDU is must be carried within the header of that network protocol data unit for processing by ATN routers and host computers.

#### 5.6.1.1 Scope

*Note.* 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.* 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 sections 5.5.6.2, ATN Specific Features and 5.5.6.3, Mandatory and Optional Functions, in addition to all APRLs specified in section 5.5.6.4.

## 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, developed by ICAO, allows for the incorporation of differing Air/G-to-ground and Ground/G-to-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.

*Note.—The Security Registration ID identifies the authority that has specified the associated security policy.*

### 5.6.2.2 The Security Function

#### 5.6.2.2.3 Security Registration ID Length

#### 5.6.2.2.1 General

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.

5.6.2.2.1.1 ~~The~~The SECURITY Function of the ISO/IEC 8473, as defined in this specification, shall be supported by ATN End System or Intermediate System Network entities implementations receiving or transmitting inter-domain traffic other than Traffic Type as General Communications.

*Note .— The Security Registration ID identifies the authority that has specified the associated security policy.*

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

#### 5.6.2.2.4 Security Registration ID

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.

5.6.2.2.4.1 This variable field shall contain a Security Type object identifier encoded using ASN.1 Basic Encoding Rules with the following sequence of integer values:

{1 3 27 0 0} The ATN Security Registration Identifier

#### 5.6.2.2.2 Encoding of the Security Parameter

*Note.— The ATN Security Registration Identifier identifies the ATN Security Authority. ICAO has been assigned an International Code Designator (ICD) decimal value [00027] 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.*

5.6.2.2.2.1 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.*

#### 5.6.2.2.5 Security Information Length

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.

5.6.2.2.5.1 This field shall be one octet in length and shall define indicate 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 indicate a zero-length.

#### 5.6.2.2.6 Security Information

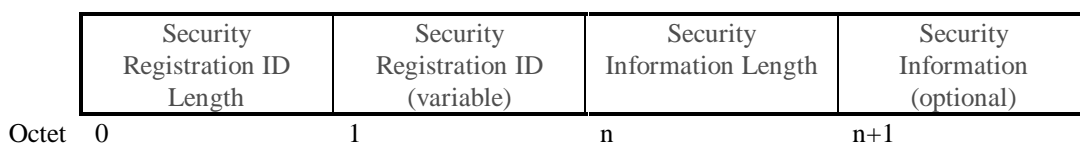


Figure 5.6-1: The ATN Security Label

**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

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



**Figure 5.6-2:** Security Tag Set Format

shall be as defined in the following sections below:

*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 Classification Registered Field Set**

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 field.

*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 5.5.6-1.

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

**ATSC Route Selection – Tie Breaking**

For a given ATSC class of service, route selection

shall be based upon the route's capability to meet or exceed the required level of service (e.g., if Class D is selected by the application, routes which

**Table 5.5.6-1 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.
		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 <sup>1</sup>	N/A
ATN Systems Management Communications	No category defined	011 00000	No Traffic Type Policy preference.

<sup>1</sup> Note 1. — 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.

<sup>1</sup> 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.

provide Class A, B, C, or D service) may be used). If multiple routes are available which meet or exceed the selected service, the route with the lowest relative cost shall be selected.

Note1.— For the CNS/ATM-1 Package, subnetworks may be allocated a service class and a relative cost on a local basis for local routing policy decisions only.

Note2.— Transit delay values allocated to each ATSC class of service are expected to be enforced only on the air/ground path selection for the CNS/ATM-1 package.

#### 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 Ttag Sset shall always follow the Tag Set for Traffic Type and Associated Routing Policies (see 5.5.6.2.2.6) if present, but otherwise shall be the first Ttag Sset 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 5.5.6-2 1- Encoding of the Traffic Type Security Classification – Tag 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

#### 5.6.2.3 Management of Network Priority

Note.— Network priority handling provisions are specified in Chapter 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 C/E bit

conveyed in the QoS Maintenance parameter of an ISO/IEC 8473 NPDU. Section 5.2.2.5 defines the Transport Layer will take measures that the Transport Layer implements upon receipt of to avoid congestion if a high proportion of NPDUs are received with the C/E 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  $\alpha$  (see Table 5.6-32), the ATN Intermediate System shall set the CE-flag in the NPDU header.

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:

- the first one,  $n$ -total, shall reflect the length of that sequence.
- 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 1.— 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 2. — The conveyance of — way how the congestion information associated with an NSDU is conveyed to the NS-User is a local matter.*

### 5.6.2.4.3 Required algorithm values

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

**Table 5.5.6-3 Required Value for  $\alpha$**

Name	Description	Required range
$\alpha$	Output queue threshold	1 packet

## 5.6.3 ATN Specific Requirements for ISO/IEC 8473 Compliance Statement

*Note . — This section defines ATN specific requirements on the ISO/IEC 8473 Protocol. All Network entities shall implement ISO 8473 CLNP protocol and comply with all mandatory and optional internetwork protocol functions as specified in this chapter.*

### **Mandatory Internetwork Protocol Functions**

*Note. — This section specifies the functions which are performed as part of the ATN Internetwork Protocol within all Network entities conforming to ATN requirements*

#### **PDU Composition Function**

ATN ESs and ISs shall perform the PDU Composition function.

#### **PDU Decomposition Function**

ATN ESs and ISs shall perform the PDU Decomposition function.

#### **Header Format Analysis Function**

ATN ESs and ISs shall perform the Header Format Analysis function.

#### **Route PDU Function**

ATN ESs and ISs shall perform the Route PDU function.

#### **Forward PDU Function**

ATN ESs and ISs shall perform the Forward PDU function.

### 5.6.3.1 Segmentation Function

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

5.6.3.1.2

5.6.3.1.3 ATN End Systems shall support the ISO/IEC 8473 segmenting subset.

5.6.3.1.4 **Recommendation.** — *ATN End Systems should use the non-segmenting ISO/IEC 8473 subset for NSDUs of up to 1024 octets.*

#### **Reassembly Function**

ATN ESs and ISs shall perform the Reassembly function.

#### **Discard PDU Function**

ATN ESs and ISs shall perform the Discard PDU function.

#### **Error Reporting Function**

ATN ESs and ISs shall perform the Error Reporting function.

#### **PDU Header Error Detection**

ATN ESs and ISs shall perform the PDU Header Error Detection function.

### **Optional Internetwork Protocol Functions**

*Note. — This section specifies the use of ISO CLNP optional functions within ATN ES and IS implementations.*

ISO 8473 internetwork protocol options shall be selected by the ATN end-system Network entity which originates ISO 8473 NPDUs.

#### **Padding Function**

ESs shall not support the transmission of ISO 8473 NPDUs with the Padding Function. ISs shall support the transmission of NPDUs with the Padding Function. ESs and ISs shall support the receipt of ISO 8473 NPDUs with the Padding Function

### 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. The SECURITY function shall be required for ATN ES or IS Network entity implementations receiving or transmitting traffic other than General Communications. ATN network entities shall therefore provide the Globally Unique Security format for all created NPDUs. The sole exception to this requirement is for General Communications traffic where no Security parameter information is required to be encoded in created NPDUs.*

#### Source Routing Function

The Source Routing function shall not be used by originating ATN ES Network entities. An ATN IS implementation shall process any NPDUs received with this option selected by discarding the NPDU. In the case that an NPDU is discarded, an ER NPDU shall be returned to the originating Network entity, if indicated by the Error Report flag in the discarded NPDU.

#### Record Route Function

5.6.3.2.1.1 ATN IS Network entities shall support the Partial Record Route Function. ISs and ESs shall not support the Complete Record Route Function.

#### Quality of Service Maintenance Function

ATN ES and IS Network entities shall support the Quality of Service Maintenance Function.

#### Priority Function

ATN ES and IS Network entities shall implement the Priority Function.

#### Congestion Notification Function

ATN ES and IS Network entities shall support the Congestion Notification Function.

### 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 Network Priority

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

#### Echo Response Function

ATN ES and IS Network entities shall perform the ECHO RESPONSE Function upon receipt of an Echo Request (ERQ) PDU that has reached its destination.

*Note.— When invoked, this function causes an Echo Response (ERP) PDU to be created and processed by all ES and IS Network entities.*

#### PDU Lifetime Control in Intermediate and End Systems

ATN ISs and ESs shall perform the PDU Lifetime Control function.

## 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 is 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 Recommendations

5.6.4.2.1 Does the implementation support the following ATN-specific features:

Index	Item	ATN SARPs Reference	ATN CNS/ATM-1 Package Support
ATN CLNP1	Encoding and use of the Security Parameter	5.5.6.2.2	M
ATN CLNP2	Management of Network Priority	5.6.2.3, 5.2.8.46	M
ATN CLNP3	Use of Non-Segmenting Subset	5.6.3.1	O
ATN CLNP4	Echo Request Function	5.6.3.3	O
ATN CLNP5	Congestion Management	5.6.3.4	O

### 5.6.4.3 Major Capabilities

5.6.4.3.1 An ATN IS or ES protocol implementation shall conform to the following APRLs.

Item	Capability	ISO/IEC 8473 Reference	Status	ATN CNS/ATM-1 Package 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 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 8208	8473-3: 5.4	O.2	O
ATN SNDCF	SNDCF for Mobile Subnetworks	ATN CNS/ATM- +SARPs Ref: Chapter 5.7	N/A	ISMOB:M ISGRD:O ^IS:O

ISMOB: If ISO/IEC 8473 is used over Mmobile 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 5.5.6.4.4 through 5.5.6.4.11. –The supported functions, NPDUs, associated parameters and timers required for Intermediate Systems are provided in APRLs 5.5.6.4.12 through 5.5.6.4.24.

O.2: –APRLs for the SNDCF for use with –ISO/IEC 8802-2 subnetworks are provided in 5.5.6.4.19 and 5.5.6.4.20. APRLs for the SNDCF for use with ISO/IEC 8208 subnetworks are provided in 5.5.6.4.21 through –5.5.6.4.24.

#### 5.6.4.4 End Systems - Supported Functions

5.6.4.4.1 An ATN ES protocol implementation shall conform to the following APRL for supported functions.

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package 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, CNS/ATM-1 SARPs Ref. 5.6.3.2.10	M	M
ePDUL-r	<r> PDU Lifetime Control	6.4, CNS/ATM-1 SARPs Ref. 5.6.3.2.10	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 CNS/ATM- 1 SARPs Ref: 5.6.2.2	O	M 
eSecu-r	<r> Security	6.13, ATN CNS/ATM- 1 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, CNS/ATM- 1 SARPs Ref. 5.6.3.2.3	O	OX 
ePSR	Partial Source Routing	6.14, CNS/ATM- 1 SARPs Ref. 5.6.3.2.3	O	OX 
ePRI-s	<s> Priority	6.17, ATNCNS/ATM-1 SARPs Ref. 5.6.3.42.6	O	M 

ePRI-r	<r> Priority	6.17, <u>ATNCNS/ATM-1</u> SARPs Ref. 5.6.3.42-6	O	M   
--------	--------------	--	---	------------

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package Support
eQOSM-s	<s> QOS Maintenance	6.16, CNS/ATM-1 SARPs Ref. 5.6.3.2.5	O	M
eQOSM-r	<r> QOS Maintenance	6.16, CNS/ATM-1 SARPs Ref. 5.6.3.2.5	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 CNS/ATM-1 SARPs Ref. 5.6.3.2.1	O	OX
ePadd-r	<r> Padding	6.12 CNS/ATM-1 SARPs Ref. 5.6.3.2.1	M	M
eEreq	Echo request	6.19, ATN SARPs Ref. 5.6.3.3	O	O
eErsp	Echo response	6.20	O	M
eSegS	Create segments smaller than necessary	6.8	O	O

### 5.6.4.5 End Systems - Supported NPDUs

5.6.4.5.1 An ATN ES protocol implementation shall conform to the following APRL for supported NPDUs.

Item	NPDU	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package 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
[type REQ]eIN-r	Inactive PDU receive	7.8	IAS-r:M	IAS-r:M
eERQ-t	ERQ transmit	7.10	eEerq: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

5.6.4.6.1 An ATN-ES protocol implementation shall conform to the following APRL for supported DT parameters:

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM- 1 Package Support
edFxFt-s	<s> Fixed Part	7.2	M	M
edFxFt-r	<r> Fixed Part	7.2	M	M
edAddr-s	<s> Address	7.3	M	M
edAddr-r	<r> Address	7.3	M	M
edSeg-s	<s> Segmentation Part	7.4	M	M
edSeg-r	<r> Segmentation Part	7.4	M	M
edPadd-s	<s> Padding	7.5.2	ePadd-s:M	-
edPadd-r	<r> Padding	7.5.2	M	M
edSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
edSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
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:M
edQOSM-r	<r> QOS Maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM 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	eP-r:M
edData-s	<s> Data	7.6	M	M
edData-r	<r> Data	7.6	M	M

edUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.21	M	M
edUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

### 5.6.4.7 End Systems - Supported ER Parameters

5.6.4.7.1 An ATN ES protocol implementation shall conform to the following APRL for supported ER parameters.

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN CNS/ ATM-1 Package Support
eeFxFt-s	<s> Fixed Part	7.2	M	M
eeFxFt-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
[type REQ]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
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

5.6.4.8.1 An ATN-ES protocol implementation shall conform to the following APRL for inactive DT parameters.

<b>Item</b>	<b>Parameter</b>	<b>ISO/IEC 8473-1 Reference</b>	<b>Status</b>	<b>ATN CNS/ATM- 1 Package Support</b>
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

5.6.4.9.1 An ATN-ES protocol implementation shall conform to the following APRL for supported ERQ parameters:

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN/CNS/ATM-1 Package Support
eqFxFt-s	<s> Fixed Part	7.2	M	M
eqFxFt-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	ePr-s:M	ePrr-s:M
eqPRR-r	<r> Partial Route Recording	7.5.5	ePr-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:M
eqQOSM-r	<r> QOS Maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM or eCong-r:M
eqPri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
eqPri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
eqData-s	<s> Data	7.6	M	M
eqData-r	<r> Data	7.6	M	M

eqUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.21	M	M
eqUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

### 5.6.4.10 End Systems - Supported ERP Parameters

5.6.4.10.1 An ATN ES protocol implementation shall conform to the following APRL for supported ERP parameters.

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN/CNS/ATM-1 Package Support
epFxFt-s	<s> Fixed Part	7.2	M	M
epFxFt-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	eSecu-s:M	eSecu-s:M
epSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
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	ePr-s:M	ePrr-s:M
epPRR-r	<r> Partial Route Recording	7.5.5	ePr-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	eQOSM-s or eCong-s:M	eQOSM:M
epQOSM-r	<r> QOS Maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM or eCong-r:M
epPri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
epPri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
epData-s	<s> Data	7.6	M	M
epData-r	<r> Data	7.6	M	M

epUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.21	M	M
epUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

### 5.6.4.11 End Systems - Timers

5.6.4.11.1 An ATN ES protocol implementation shall conform to the following APRL for timers.

Item	Timer	Ref	ISO Status	ISO Range	ATN CNS/ATM-1 Package Support	Values Supported
ELifReas	Is reassembly timer <= received derived PDU lifetime?	6.8	M		M	
eReasTim	Reassembly Timer	6.8		500ms to 127.5s		<= lifetime

### 5.6.4.12 Intermediate Systems - Supported Functions

5.6.4.12.1 An ATN IS protocol implementation shall conform to the following APRL for supported functions:

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package Support
iPDUC	PDU Composition	6.1	M	M
iPDUD	PDU Decomposition	6.2	M	M
iHFA	Header Format Analysis	6.3	M	M
iPDUL	<s> PDU Lifetime Control	6.4	M	M
iRout	Route PDU	6.5	M	M
iForw	Forward PDU	6.6	M	M
iSegm	Segment PDU	6.7	iDSNS:M	iDSNS:M
iReas	Reassemble PDU	6.8	O	O
iDisc	Discard PDU	6.9	M	M
iErep	Error Reporting	6.10	M	M
iEdec	<s> Header Error Detection	6.11	M	M
iSecu	<s>Security	6.13 ATN CNS/ATM-1 SARPs Ref: 5.6.2.2	O	M
iCRR	<s> Complete Route Recording	6.15 CNS/ATM-1 SARPs Ref:5.6.3.2.4	O	OX
iPRR	<s> Partial Route Recording	6.15 CNS/ATM-1 SARPs Ref:5.6.3.2.4	O	M
iCSR	Complete Source Routing	6.14 CNS/ATM-1 SARPs Ref: 5.6.3.2.3	O	OX
iPSR	Partial Source Routing	6.14	O	OX
iPri	<s> Priority	6.17, ATN CNS/ATM-1 SARPs Ref: 5.6.3.4.2.6	O	M

iQOSM	<s> QOS Maintenance	6.16, <del>CNS/ATM-1</del> SARPs Ref: 5.6.3.2.5	O		M
iCong	<s> Congestion Notification	6.18, <del>ATN</del> <del>CNS/ATM-1</del> SARPs Ref: 5.6.2.43.2.7	O		M
iPadd	<s> Padding	6.12	M		M
iEreq	Echo request	6.19, <del>ATN SARPs</del> Ref: 5.6.3.3	O		O
iErsp	Echo response	6.20	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



### 5.6.4.12.2 Supported Security Parameters

5.6.4.12.3 An ATN-IS protocol implementation shall conform to the following APRL for supported security parameters:

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package 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 CNS/ATM-1 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.

### 5.6.4.12.4 Quality of Service Maintenance Function

5.6.4.12.4.1 An ATN-IS protocol implementation shall conform to the following APRL for the Quality of Service Maintenance function:

Item	Function	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package 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:M
	<b>Which of the following formats of QOS are implemented?</b>			
iSADDQoS	Source Address Specific QoS	7.5.6.1	iQoSM:O.3	iQOSM:O
iDADDQoS	Destination Address Specific QoS	7.5.6.2	iQoSM:O.3	iQOSM:O
iGUNQoS	Globally Unique QoS	7.5.6.3	iQoSM:O.3	iQOSM:M
iSvTD	Sequencing versus Transit Delay	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4
iCongE	Congestion Experienced	7.5.6.3	iGUNQoS:O.4	iGUNQoS:M
iTDvCst	Transit Delay versus Cost	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4

iREPVTD	Residual Error Probability versus Transit Delay	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4
iREPVcst	Residual Error Probability versus Cost	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4

O.3: The Quality of Service Maintenance parameter within a single NPDU specifies a QoS format code indicating Source Address Specific, Destination Address Specific or Globally Unique QoS.

O.4: If the QoS format code indicates that the Globally Unique QoS maintenance function is employed, then each bit in the associated parameter value may be set to indicate the order of intra and inter domain routing decisions based on QoS. The parameter values which apply to inter-domain routing are provided in Table 4 of ISO/IEC 10747.

### 5.6.4.13 Intermediate Systems - Supported NPDUs

5.6.4.13.1.1 An ATN IS protocol implementation shall conform to the following APRL for supported NPDUs:

Item	Function	ISO/IEC 8473- 1 Reference	Status	ATN CNS/ATM- 1 Package 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	O
iERQ-r	ERQ receive	7.10	M	M
iERP-t	ERP transmit	7.11	iErs:M	O
iERP-r	ERP receive	7.11	M	M

### 5.6.4.14 Intermediate Systems - Supported DT Parameters

5.6.4.14.1.1 An ATN IS protocol implementation shall conform to the following APRL for supported DT parameters:

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM- 1 Package Support
idFxFt-s	<s> Fixed Part	7.2	M	M
idFxFt-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	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
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

5.6.4.15.1.1 An ATN IS protocol implementation shall conform to the following APRL for supported ER parameters.

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM- 1 Package Support
ieFxFt-s	<s> Fixed Part	7.2	M	M
ieFxFt-r	<r> Fixed Part	7.2	M	M
ieAddr-s	<s> Address	7.3	M	M
ieAddr-r	<r> Address	7.3	M	M
ieSeg-s	<s> Seg Part	7.4	M	M
ieSeg-r	<r> Seg Part	7.4	M	M
iePadd-s	<s> Padding	7.5.2	M	M
iePadd-r	<r> Padding	7.5.2	M	M
ieSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M
ieSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
ieCRR-s	<s> Complete Route Recording	7.5.5	M	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
ieUnsup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

### 5.6.4.16 Intermediate Systems - Supported ERQ Parameters

5.6.4.16.1.1 An ATN IS protocol implementation shall conform to the following APRL for supported ERQ parameters:

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package 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	-
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

5.6.4.17.1.1 An ATN IS protocol implementation shall conform to the following APRL for supported ERP parameters.

Item	Parameter	ISO/IEC 8473-1 Reference	Status	ATN CNS/ATM-1 Package Support
ipFxFt-s	<s> Fixed Part	7.2	M	M
ipFxFt-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
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	iSecu:M	iSecu:M
ipSecu-r	<r> Security	7.5.3	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	M	M
ipPRR-r	<r> Partial Route Recording	7.5.5	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	M	M
ipQOSM-r	<r> QOS Maintenance	7.5.6	iQOSM or iCong:M	iQOSM or iCong:M
ipPri-s	<s> Priority	7.5.7	M	M
ipPri-r	<r> Priority	7.5.7	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

5.6.4.18.1.1 An ATN IS protocol implementation shall conform to the following APRL for timers.

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

### 5.6.4.19 Subnetwork Dependent Convergence Functions SND CF for use with ISO/IEC 8802-2 Subnetworks - Functions

5.6.4.19.1 When ISO 8802-2 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Function	ISO/IEC 8473-2 Reference	Status	ATN CNS/ATM-1 Package Support
S802SNUD	Is subnetwork user data of at least 512 octets transferred transparently by the SND CF ?	5.2	M	M
S802SNTD	Is Transit Delay determined by the SND CF prior to the processing of User Data ?	5.2	M	M

### 5.6.4.20 Subnetwork Dependent Convergence Functions SND CF for use with ISO/IEC 8802-2 Subnetworks - Multi Layer Dependencies

5.6.4.20.1 When ISO 8802-2 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Dependency	ISO/IEC 8473-2 Reference	ATN CNS/ATM-1 Package 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

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

5.6.4.21.1 When ISO 8208 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Function	ISO/IEC 8473-3 Reference	Status	ATN/CNS/ATM-1 Package 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	5.31		
	Is a new call setup:			
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
XCalte	e. by other local means ?	5.3.1	O.3	O.3
	Call clearing considerations	5.3.2		
	Are calls cleared:			
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
------	-------------------------	-------	---	---

### 5.6.4.22 Subnetwork Dependent Convergence Functions SND CF for use with ISO/IEC 8208 Subnetworks - X.25 Call User Data

5.6.4.22.1 When ISO 8208 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Parameter	ISO/IEC 8473-3 Reference	Status	ATNCNS/ATM-1 Package 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

### 5.6.4.23 Subnetwork Dependent Convergence Functions SND CF for use with ISO/IEC 8208 Subnetworks - ISO/IEC 8208 SND CF Timers

5.6.4.23.1 When ISO 8208 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Timer	ISO/IEC 8473-3 Reference	Status	Values	ATNCNS/ATM-1 Package Support
XIDL	X25 VC Idle	5.3.4	XClra:O	Any	XClra:O
XNVC	additional VC	5.3.4	O	Any	M

### 5.6.4.24 Subnetwork Dependent Convergence Functions Sndcf for use with ISO/IEC 8208 Subnetworks - Sndcf Multi Layer Dependencies

5.6.4.24.1 When ISO 8208 is used as a subnetwork to support ATN service, the following APRLs shall apply.

Item	Dependency	ISO/IEC 8473-3 Reference	ATN CNS/ATM-1 Package Support	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 CNS/ATM-1 Package 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. SPECIFICATION OF SUBNETWORK DEPENDANT CONVERGENCE FUNCTIONS

### 5.7.1 Scope and Applicability

*Note 1.*— The Subnetwork Service (SN-Service) as specified in this chapter shall be provided to the ISO/IEC 8473 Internetwork Protocol and the ISO/IEC 9542 End-System to Intermediate-System Protocol entities.

*Note 2.*— The purpose of a Subnetwork Dependent Convergence Function (SNDCF) is to shall be provided where the available SNAeP does not provide the connectionless SN-Service assumed by the ATN Internet Protocols over real subnetworks.

*Note 3.*— The ATN Internetwork Layer, including CLNP and the routing protocols that support it, assume this common connectionless service to be provided by all subnetworks providing communications between ATN systems.

*Note 4.*— 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 layer. The assumed service provided by the subnetworks is described in ISO/IEC 8473 clause 5.5 and 8.

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

*Note.*— These procedures are defined in Chapter 5.3.

### 5.7.2 Service Provided by the SNDCF Primitives

*Note 1.*— This section specifies the assumed service provided internally by the SNDCF for the purpose of conveying Network Data PDUs between Network Entities. The mechanisms defined in this chapter, or equivalent mechanisms

**Table 5.5.7-1 SN-Service Primitives 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

shall be provided.

*Note 2.*— The service to support SN-Service-Users shall be defined by the primitives in Table 5.5.7-1. The SN-Source-Address, SN-Destination-Address and SNS-Userdata parameters shall be mandatory, while the SN-Priority and SN-Quality-of-Service parameter shall be optional.

### Mobile Subnetwork routing initiation and termination

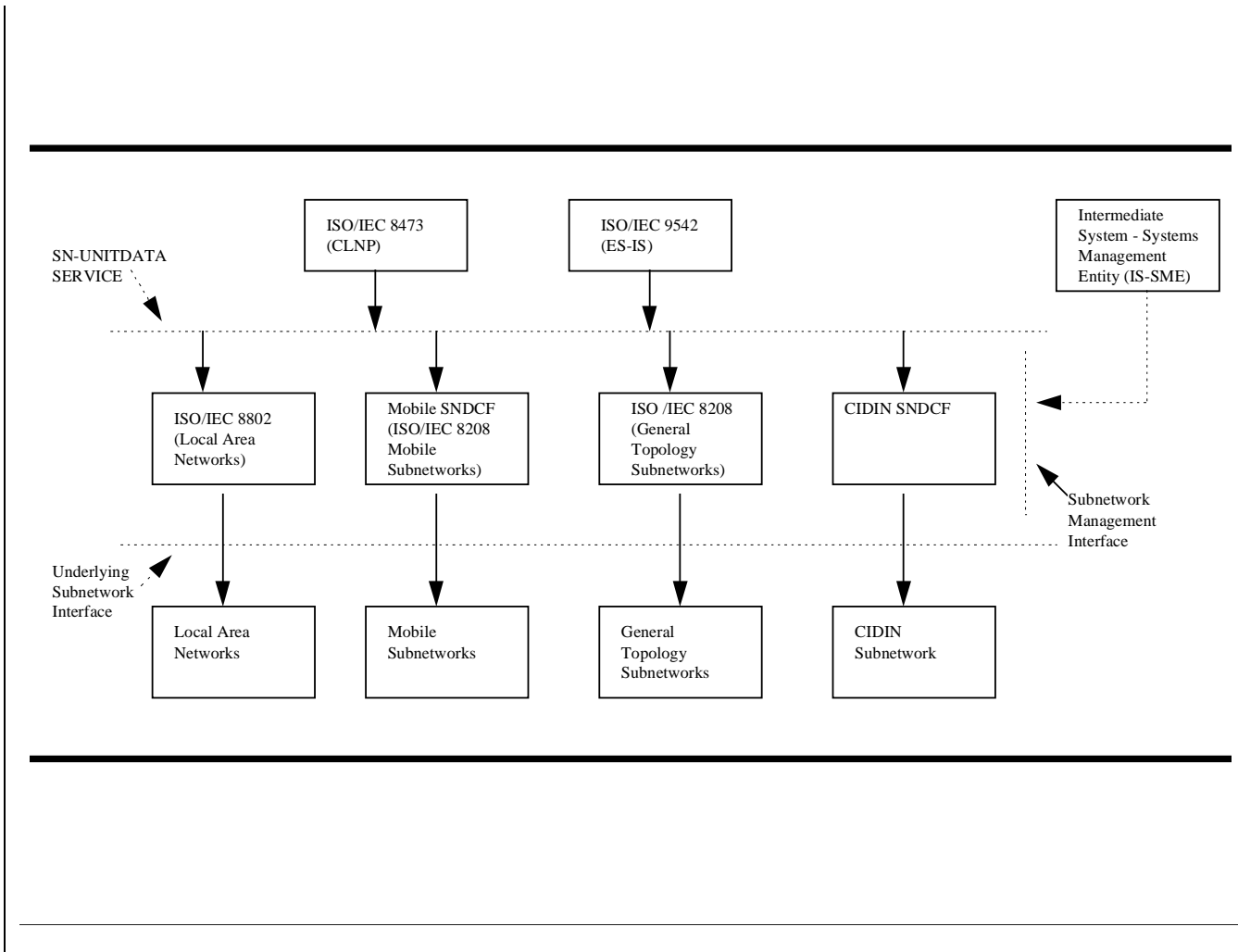


Figure 5.5.7-1.

**5.7.2.1 Subnetwork Service Primitives Parameters**

*Note. — The following section specifies 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 shall specify the points of attachment to a public or private subnetwork(s). The SN-Source-Address and SN-Destination-Address addresses shall 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 shall be those specified and administered by the authority responsible for administration of that subnetwork.*

**5.7.2.1.2 Subnetwork Priority**

5.7.2.1.2.1 If supported by the subnetwork, the SN-Priority parameter, as specified in Table 5.7-1, shall specify 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.

5.7.2.1.2.2 SN-Priority values shall be in the range [0000 0000] through [0000 1110], with higher values indicating higher priorities.

5.7.2.1.2.3 If no SN-Priority is indicated, the value [0000 0000] shall be assumed to be the default.

*Note. — Further requirements related to subnetwork priority are specified in 5.2.8.5.*

### 5.7.2.1.3 Subnetwork Quality of Service (SNQoS)

If supported, the SN-Quality-of-Service parameter shall comprise the following information:

1. Transit Delay;
2. Residual Error Probability;
3. Economic cost; and,
- a) 4. Protection against Unauthorized Access.

*Note 1. — The use of the SN-Quality-of-Service parameter is shall be optional, and depends shall be based on the needs of the SN-Service-User. If required by the SN-Service-User, the SN-Quality-of-Service parameter shall be used to influence the service requested from the Subnetwork Provider to support transfer of SN-UNITDATA requests. Techniques for mapping the semantic content of SN-Quality-of-Service parameter onto mechanisms provided for a particular underlying subnetwork shall be based on a priori information and local management options.*

*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.*

### 5.7.2.1.4 Subnetwork Service Userdata

5.7.2.1.4.1 The SNS-Userdata shall contain the ISO/IECISO 8473 or ISO/IECISO 9542 NPDU that have to be conveyed between adjacent network entities.

5.7.2.1.4.2 The SNS-Userdata shall be an ordered multiple of octets, and shall be transferred transparently between the subnetwork points of attachment specified in the SNS primitive.

### Subnetwork Service Data Units (SNSDUs)

ISO/IECISO 8473 and ISO/IECISO 9542 PDUs shall be conveyed between adjacent network entities as SNSDUs, through invocation of the SN-UNITDATA service with the ISO/IECISO 8473 or

ISO/IECISO 9542 NPDU provided as the SNS-Userdata parameter.

## Subnetwork Dependent Convergence Function (SND CF)

The SND CF shall provide a connectionless-mode service in the case where an underlying subnetwork does not inherently provide the connectionless-mode service assumed by the SNS-User. If an underlying subnetwork inherently provides a connection-mode service, the SND CF shall provide a mapping onto the underlying service.

## 5.7.3 Convergence Provisions for ISO/IECISO 8208 Subnetworks

### 5.7.3.1 General

5.7.3.1.1 The facility provided for convergence of ISO/IECISO 8473 and ISO/IECISO 9542 over the ISO/IECISO 8208 SNAcP shall establish, maintain and release ISO/IECISO 8208 virtual circuits as needed, and shall provide for the priority and QoS requirements of ISO/IECISO 8473 and ISO/IECISO 9542. The interface between the SND CF and the SN-Service-Users shall be the SN-UNITDATA request/indication primitives listed in Table 5.7-1.

### 5.7.3.2 Service Coordination between the SND CF and SN-Service-Users

5.7.3.2.1 On receipt of a SN-UNITDATA request, the SND CF shall either establish a new virtual circuit or make available an existing virtual circuit which meets the priority and QoS requirements of the SN-Service-User as specified by the SN-Priority and SN-Quality-of-Service parameters, if present.

5.7.3.2.2 If the SN-Priority and SN-Quality-of-Service parameters are not present in a received SN-UNITDATA request, the SND CF shall use local default parameter values; in this case, it shall be assumed that the SN-Service-User has accepted the default QoS available from the underlying subnetwork.

### 5.7.3.3 Service Coordination between the SND CF and ISO/IECISO 8208 Subnetwork Providers

### 5.7.3.3.1 General

5.7.3.3.1.1 If any combination of the Transit Delay Selection and Indication, Throughput Class Negotiation or ~~Priority ISO/IEC~~ 8208 optional user facilities are available from the Subnetwork Provider via the Subnetwork Access Protocol, then the SNDCF shall use them for service coordination at the time of establishment of virtual circuits, as described in 5.5.7.3.3.2, 5.5.7.3.3.6 and ~~5.5.7.3.3.7~~.

5.7.3.3.1.2 If one or more of these three ~~ISO/IEC~~ 8208 optional user facilities are not available from the Subnetwork Provider via the ~~ISO/IEC~~ 8208 Subnetwork Access Protocol, default values for transit delay, throughput class and priority shall be assumed by the SNDCF.

### 5.7.3.3.2 Transit Delay

#### 5.7.3.3.2.1 General

5.7.3.3.2.1.1 The SNDCF shall invoke the Transit Delay Selection and Indication Facility, if provided, when:

1. A new virtual circuit must be established;
2. Transit Delay is indicated in the SN-UNITDATA request primitive causing establishment of the new virtual circuit; and,
3. Expected Transit Delay for the selected subnetwork is unknown.

5.7.3.3.2.1.2 If the requested maximum transit delay is less than the transit delay available from the Subnetwork Provider, the SNDCF shall attempt to transfer the SN-UNITDATA request at a greater transit delay than requested.

5.7.3.3.2.1.3 If the indicated value is equal to or greater than the transit delay available from the Subnetwork Provider, the SNDCF shall transfer the SN-UNITDATA request.

5.7.3.3.2.1.4 The requested maximum transfer delay shall apply to both directions of transfer.

#### 5.7.3.3.2.2 Transit Delay Selection and Indication Facility

5.7.3.3.2.2.1 The SNDCF shall indicate the requested transit delay by means of the Transit Delay Selection and Indication Facility in the CALL REQUEST packet.

5.7.3.3.2.2.2 **Recommendation.**— *The Subnetwork Provider, when able to do so, should allocate resources and route the Virtual Circuit in a manner such that the transit delay applicable to that circuit does not exceed the desired transit delay.*

5.7.3.3.2.2.3 When the Transit Delay Selection and Indication Facility is invoked, the INCOMING CALL packet transmitted to the called SNDCF and the CALL CONNECTED packet transmitted to the calling SNDCF shall ~~both~~ contain the indication of the transit delay applicable to the Virtual Circuit.

### 5.7.3.3.3 Residual Error Probability

5.7.3.3.3.1 The SNDCF shall discard an SN-UNITDATA request primitive and its associated SN-Userdata parameter if the requested maximum residual error probability is less than the residual error probability known to be available from the Subnetwork Provider.

5.7.3.3.3.2 If the requested value is equal to or greater than the residual error probability known to be available from the Subnetwork Provider, the SNDCF shall transfer the SN-UNITDATA request.

5.7.3.3.3.3 The requested maximum residual error probability shall apply to both directions of transfer.

### 5.7.3.3.4 Economic cost

5.7.3.3.4.1 The SNDCF shall discard an SN-UNITDATA request primitive and its associated SN-Userdata parameter if the requested maximum economic cost is less than the economic cost known to be available from the Subnetwork Provider.

5.7.3.3.4.2 If the requested value is equal to or greater than the economic cost known to be available from the Subnetwork Provider, the SNDCF shall transfer the SN-UNITDATA request.

5.7.3.3.4.3 The requested maximum cost determinant shall apply to both directions of transfer.

### 5.7.3.3.5 Protection against Unauthorized Access

5.7.3.3.5.1 The Subnetwork Provider shall inform the SN-Service-User of the level of protection provided for data in transit.

5.7.3.3.5.2 The level of protection shall be specified as one of the following four qualitative options:

- a) No protection.
- b) Protection against passive monitoring of SNSDU traffic flow.
- c) Protection against active modification of SNSDU traffic flow.
- d) Protection against both passive monitoring and active modification of SNSDU traffic flow.

5.7.3.3.5.3 If the SN-Service-User includes information in the SN-Quality-of-Service parameter indicating the required level of protection in the SN-UNITDATA request primitive and the Subnetwork Provider cannot satisfy this requirement, then the SNDCF shall discard the SN-UNITDATA request primitive and its associated SN-Userdata parameter.

### 5.7.3.3.6 Throughput

#### 5.7.3.3.6.1 General

5.7.3.3.6.1.1 Subnetwork throughput shall be determined or negotiated in one of two ways:

1. Throughput information may be available as a priori information from the Subnetwork Provider; or,
2. Throughput information may be dynamically indicated and/or negotiated by the SNDCF, using the ISO/IEC 8208 Throughput Class Negotiation Facility.

5.7.3.3.6.1.2 **Recommendation.**— *If the throughput required by the SN-Service-User is greater than the throughput which can be provided, the SNDCF should opt for another Subnetwork Provider, if available.*

#### 5.7.3.3.6.2 Throughput Class Negotiation Facility

5.7.3.3.6.2.1 **Recommendation.**— *The SNDCF should make use of the ISO/IEC 8208 Throughput Class Negotiation Facility for indication and/or negotiation of Throughput Class, if offered by the subnetwork service provider.*

5.7.3.3.6.2.2 If Throughput Class Negotiation is used by the SNDCF, the calling SNDCF shall

request throughput classes for both directions of data transmission via the ISO/IEC 8208 Call Request packet.

5.7.3.3.6.2.3 The throughput class indicated to the called SNDCF shall not be greater than the default throughput classes, for each direction of transmission, at the calling and called SNDCF Subnetwork Provider interfaces respectively.

*Note.*— *The supplied throughput may be less than indicated throughput.*

### 5.7.3.3.7 Priority

#### 5.7.3.3.7.1 General

5.7.3.3.7.1.1 The SNDCF shall have a priori information regarding the use of priority by the Subnetwork Provider.

5.7.3.3.7.1.2 If the Subnetwork Provider supports priority and specifies the mapping of Network Service to Subnetwork Service priorities:

1. The SNDCF shall convey the priority to the Subnetwork Provider by means of the ISO/IEC 8208 priority facility, as described in 5.5.7.3.3.7.2. If the subnetwork supports priority values ranging from [0000 0000] to [0000 1110], the subnetwork priority value shall be the same as the priority value in the ISO/IEC 8473 or ISO/IEC 9542 header, respectively to provide a one-to-one mapping between the Network and Subnetwork Layer priorities. If fewer (or more) than fourteen levels of subnetwork priority are supported, the priority value in the ISO/IEC 8473 or ISO/IEC 9542 header shall be mapped onto the subnetwork priority value according to the requirements of the subnetwork provider.
2. The SNDCF shall establish a SN-connection for each requested priority.—A SN-connection shall only be used for SNSDUs for which the indicated priority corresponds with the priority associated with the connection.

5.7.3.3.7.1.3 If the Subnetwork Provider does not require connections to be prioritized, then the SNDCF shall not convey priority information to the Subnetwork Provider and the provisions of 5.7.3.3.7.1 and 5.5.7.3.3.7.2 shall not apply.

#### 5.7.3.3.7.2 Use of the Priority Facility

5.7.3.3.7.2.1 If no SN-connection with the requested priority is available, the SNDCF shall

establish a connection by sending a CALL REQUEST containing the appropriate priority facility to the Subnetwork Provider.

5.7.3.3.7.2.2 Upon receipt of an INCOMING CALL packet from the Subnetwork Provider the called SNDCF shall map the contents of the priority parameter field into the priority parameter of the CALL ACCEPTED packet.

*Note 1.— The Priority Option is mandatory within an ISO/IEC ISO 8473 NPDU as specified in Chapter 5.6.*

*Note 2.— Neither the priority to gain a connection nor to keep a connection are specified.*

### 5.7.3.4 Convergence Provisions for ISO/IEC ISO 8208 General Topology Subnetworks

5.7.3.4.1 ~~Over The subnetwork service specified in 5.7.1 shall be provided using ISO/IEC ISO 8208 General Topology Subnetworks, the subnetwork service described in 5.7.2 shall be provided using the SNDCF for ISO/IEC 8208 General Topology Subnetworks —as specified in ISO/IEC ISO 8473-3; and as qualified by 5.7.6.2.~~

5.7.3.4.2 **Recommendation.**— *All ATN End SystemEs and Intermediate SystemEs using ISO/IEC ISO 8208 General Topology Fixed Subnetworks for communication with other ATN End SystemEs and Intermediate SystemEs shall/should comply with implement the requirements SNDCF as specified in 5.6.4.20.*

### 5.7.3.5 Convergence Provisions for ISO/IEC ISO 8208 Mobile Subnetworks

#### 5.7.3.5.1 General

5.7.3.5.1.1 ~~Over The subnetwork service specified in 5.7.1 shall be provided using the SNDCF for ISO/IEC ISO 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 —as specified in this clause and its subordinate paragraphs, and as qualified by 5.5.7.3.3.~~

*Note 1.— The SNDCF specified below is only applicable when providing the SN-UNITDATA service to ISO/IEC ISO 8473, ISO/IEC ISO 9542, ISO/IEC 11577 and ISO/IEC 10589 Nnetwork Llayer protocols. Unpredictable behavior may result if used to support other Network Layer Entities.*

*Note 2.— An optional feature of the SNDCF provides for "local reference cancellation".*

5.7.3.5.1.2 **Recommendation.**— *Implementations using this SNDCF for Aair/ir- Gground communications should only implement the optional facility for local reference cancellation when the lifetime of the virtual circuits is of the same order as the flight time.*

5.7.3.5.1.3 **Recommendation.**— *Implementations using this SNDCF for Gground/Gground communications should use the optional local reference cancellation mechanism.*

#### Scope and Applicability

The mobile SNDCF shall be used solely for the provision of the SN-UNITDATA service to ISO/IEC ISO 8473, ISO/IEC ISO 9542 and ISO/IEC 10589 network layer entities.

#### 5.7.3.5.2 Conformance

5.7.3.5.2.1 All ATN Intermediate SystemEs using Mmobile ISO/IEC ISO 8208 subnetworks for communication with other Intermediate SystemEs shall implement the SNDCF procedures and local reference header compression of the DT and Error PDU headers, as specified below.

#### 5.7.3.5.3 Call Setup

##### 5.7.3.5.3.1 General

5.7.3.5.3.1.1 On receipt of a SN-UNITDATA request or based on local Ssystem Mmanagement action, and lacking a suitable existing virtual circuit, the SNDCF shall establish a new virtual circuit meeting, where supported by the subnetwork, the priority and QoS requirements expressed in the SN-UNITDATA request service primitive.

##### 5.7.3.5.3.2 Call Setup Mechanism and Timing

5.7.3.5.3.2.1 The mechanism and timing for opening a virtual circuit to a known SNDCF prior to the transmission of SNSDUs shall be determined:

- a) 1.—dynamically, or
- b) 2.—by the explicit intervention of Systems Management, identifying the destination SNDCF's SNPA address.;

##### 5.7.3.5.3.3 Call Setup Functions

5.7.3.5.3.3.1 When it has been determined that a

Note 3.—The mapping between SNSDU priority and subnetwork priority is specified separately for each subnetwork type.

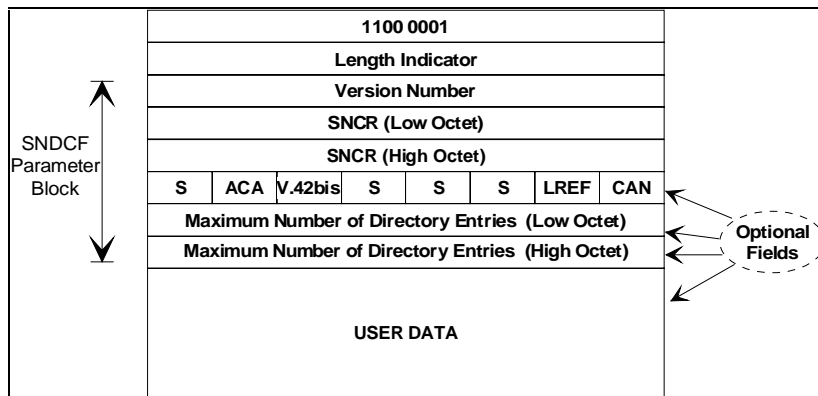


Figure 5.5.7-2 Format for Call Request User Data.

virtual circuit is to be made available, the calling SNDCF shall perform all functions associated with establishing a virtual circuit.

5.7.3.5.3.3.2 The SNDCF shall send an ISO/IEC ISØ 8208 CALL REQUEST packet to the DTE Address specified as the SN-Destination-Address, with the following optional user facilities and CCITT-specified DTE facilities:

- Priority shall be set if the subnetwork provider supports priority and specifies the mapping of Network Service to Subnetwork Service priorities.—The priority value passed in the SN-UNITDATA request shall apply to priority of data on a connection. If the priority to gain a connection and/or priority to keep a connection is conveyed within the ISO/IEC ISØ 8208 Facility Parameter Field, these priorities shall be consistent with the priority of data on a connection.
- Non-standard default packet size to the maximum supported by the subnetwork.
- Fast Select shall be used if available.

Note 1.—Other optional user facilities and CCITT-specified DTE facilities may be required by subnetworks. The use of these facilities is a local matter.

Note 2.—The SNDCF is assumed to know, a priori, if a given subnetwork supports prioritization of virtual circuits, the number of discrete priority levels supported and the relationship between the subnetwork priority and SNSDU priority.

Note 4.—If Fast Select is not supported, the compression algorithms cannot be negotiated.

#### 5.7.3.5.3.4 Format of Call Request and Call Accept User Data

Note.—The following sections specify the format of Call Request and Call Accept User Data.

##### 5.7.3.5.3.4.1 Call Request User Data

5.7.3.5.3.4.1.1 The call user data field layout shall be as illustrated in Figure 5.5.7-2.

5.7.3.5.3.4.1.2 The field is variable in length, and shall be constructed as follows:

- The first octet of the call user data field of the Call Request packet (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 1.—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. However, it is not guaranteed to be unambiguous outside of the scope of the ATN.

- The second octet is a length indicator giving the number of octets in the SNDCF parameter block (including this length indicator—up to and including (if present) the maximum number of directory entries field).
- The third octet is the SNDCF version indicator and shall be set to [0000 0001] to indicate this version of the SNDCF protocol.
- The fourth and fifth octets form the Subnetwork Connection Reference (SNCR).—The value encoded in this field shall be the number of virtual circuits currently established between the calling and called DTEs (i.e. the originating and the responding SNDCFs) at this call priority.
- The sixth octet identifies the compression techniques supported by this ATN SNDCF. The bit fields in this octet are defined in the



Tables below indicates the following as shown in Figure 5.7-1.

Note 2f.— Multiple compression techniques may be supported.

**Table 5.5.7-2. Stream Compression Options**

bit number	option
bit 8	Spare (S)
bit 7	ICAO Address Compression Algorithm (ACA)
bit 6	V.42 BIS
bit 5	Spare (S)

bit 8: Spare (S)  
 bit 7: ICAO Address Compression Algorithm (ACA)  
 bit 6: V.42 BIS  
 bit 5: Spare (S)

Note 2.— The use of the stream compression algorithms referenced above is subject to validation.

**Table 5. 5.7-3. Dictionary Compression Options**

bit number	option
bit 4	Spare (S)
bit 3	Spare
bit 2	Local Reference (LREF) option
bit 1	Local Reference Cancellation Option (CAN) supported

bit 4: Spare (S)  
 bit 3: Spare  
 bit 2: Local Reference (LREF) option  
 bit 1: Local Reference Cancellation Option (CAN) supported

Note 3.— If When bit 2 is set in the ISO/IEC 8208 Call Request, the LREF CLNP Header Compression is offered.

Note 4.— Bit 1 may only be set if bit 2 is also set.

Note 5.— When bit 2 is set the local reference cancellation procedures are also offered.

Note 6.— At most, one of the stream compression algorithms can be used, so bits 6 and 7 can both be offered in the call request packet, but both cannot be set in the call response packet.

f) When the LREF compression algorithm is used, i.e if bit 2 in octet six is set, the seventh and eighth octet (Maximum Directory Entries) shall identify the maximum number of directory entries supported for the local reference (minimum size 128), as an unsigned even number.

When the LREF compression algorithm is not used, the seventh octet shall be the first octet of the additional User Data field.

g) When the LREF compression algorithm is option is used, the ninth octet shall be the first octet of the Additional User Data field, starts at octet nine.

Note 7.— When the fast select facility is available, the Additional User Data field may be used to convey the ISO/IEC 9542 ISH PDU as part of the routing initiation sequence.

Note 7.— 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. However, it is not guaranteed to be unambiguous outside of the scope of the ATN.

**5.7.3.5.3.4.2 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.

5.7.3.5.3.4.2.1 When fast select is available and has been selected in the Call Request, then a Call Accept User Data shall be inserted in the Call Accept packet.

5.7.3.5.3.4.2.2 The Call Accept User Data field layout shall be as illustrated in Figure 5.7-32. The field shall be variable in length, and shall be constructed as follows:

a) The first octet identifies the compression techniques supported by this ATN SNDCF. The bit fields have the same meaning as the ones used for the sixth octet of the Call Request User Data. (See Note 1 and 2 in the previous section)

- b) The Second octet is the first octet of the Additional User Data field.

*Note.— ~~The~~ When the fast select facility is available, the Additional User Data field may be used to convey the ISO/IECISO 9542 ISH PDU as part of the routing initiation sequence.*

**5.7.3.5.3.5 Application of Compression Procedures**

5.7.3.5.3.5.1 The order in which compression algorithms and ISO/IECISO 8208 segmentation are applied shall be as follows:-

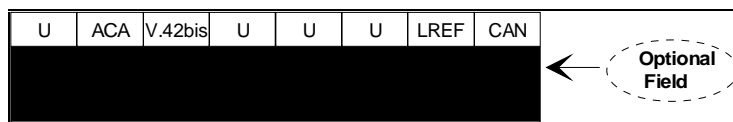
- a) If the LREF compression algorithm is used , it shall be applied to the ISO/IECISO 8473 PDU first;-
- b) If the stream compression algorithm is used , it shall be applied next;-
- c) Finally, if the PDU is still large enough to need M-bit sequencing procedures, these shall then be applied.

5.7.3.5.3.5.2 This sequence shall be inverted on the receiving end as follows:-

- a) If Re-segmentation is required , Re-segmentation based on the M-bit shall be done first;-
- b) If a stream decompression algorithm is used it shall be applied next;
- c) Finally if the LREF compression is used, the LREF decompression algorithm shall then be applied.

**5.7.3.5.3.6 Call acceptance and compression negotiation**

5.7.3.5.3.6.1 When a Call Indication is received, the called SNDCF first shall check for a call



**Figure 5.5.7-3 Format for Call Accept User Data**

collision. If the SNDCF has an outstanding Call Request to the same DTE Address, as specified given as the calling DTE in this Call Indication, and the call priority and SNCR are identical, then a call collision has occurred, and the call collision resolution procedures specified in

~~ISO/IECISO 8473-3 Clause 8.4.3.5~~ shall be invoked to resolve the call collision.

5.7.3.5.3.6.2 The called SNDCF shall then performs those operations associated with accepting a call, provided that none of the reasons for rejection listed in 5.5.7.3.5.3.7 occurs, but shall not generate any SN-UNITDATA indication. The priority on call acceptance shall be that proposed by the calling SNDCF.

5.7.3.5.3.6.3 If the call is acceptable, then the Called SNDCF shall accept the call and indicate the combination of compression techniques acceptable to the SNDCF, out of those proposed by the Calling SNDCF, by including the one-octet field shown in Figure 5.5.7-3, in the ISO/IECISO 8208 Call Accept User Data. The Called SNDCF shall indicate support for no more than one stream compression option.

5.7.3.5.3.6.4 If the called SNDCF accepts the call indicating that a proposed compression procedure is not supported, then the Calling SNDCF shall maintain the virtual circuit and shall not apply this compression procedure.

5.7.3.5.3.6.5 If the Called SNDCF accepts the call and if the Call User Data contains the User Data fields then the Called SNDCF shall process the PDU in the User Data field according to 5.5.7.3.5.7.

5.7.3.5.3.6.6 On receipt of User Data in the Call Accept User Data field, then the Calling SNDCF shall process the PDU in the User Data field according to 5.5.7.3.5.7.

**5.7.3.5.3.7 Call rejection**

5.7.3.5.3.7.1 If the call is not accepted by the called SNDCF due to the local permitted by the effective security policy of the called SNDCF, then the call shall be rejected with a diagnostic code of [1000 0101] (see Table 5.7-8). This call shall also be rejected for the following reasons:-

- a) The proposed ISO/IECISO-8208 facility, priority or Fast Select is not available;
- b) Fast Select was not selected in the received Call Request not supported and a proposed compression algorithm is not supported;
- c) The format of the call user data is invalid;

- d) The version number is not supported;
- e) The Local Reference compression is supported and the called SNDCF does not support the proposed directory size.

**5.7.3.5.3.7.2 Recommendation.** — *If a call is rejected due to the proposed directory size being too large, the caller should re-attempt the call using the default directory size, thus ensuring that the call will not be rejected again due to the requested directory size.*

**5.7.3.5.3.7.3** If the calling SNDCF receives a Clear Indication indicating call rejection, other than as part of a call collision resolution or directory size negotiation, then a Systems Management notification shall be generated, and any SN-UNITDATA queued for this call shall be discarded.

**5.7.3.5.3.7.4** The diagnostic code listed in Table 5.7-8 shall be used when an SNDCF rejects an incoming Call Request.

#### **5.7.3.5.4 Local Directory Initialization**

**5.7.3.5.4.1** Both calling and called SNDCFs shall create a local directory to be associated with each newly established virtual circuit.

**5.7.3.5.4.2** 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 (see ISO/IEC 8473 Clause 7.5.3), which may be empty;

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

#### **5.7.3.5.5 Action following an SN-UNITDATA Request**

##### **5.7.3.5.5.1 General**

**5.7.3.5.5.1.1** 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.

**5.7.3.5.5.1.2** 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 adequate security and with the PDU priority.

**5.7.3.5.5.1.3** If a suitable virtual circuit can be established, then the PDU shall then 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.

**5.7.3.5.5.1.4** 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.*

**5.7.3.5.5.1.5** 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 3.—Virtual Circuits between Intermediate SystemESs and between Intermediate SystemESs and End SystemESs 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.*

##### **5.7.3.5.5.2 Identification of Network Layer Protocol**

5.7.3.5.5.2.1 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.

5.7.3.5.5.2.2 If the IPI contains binary ~~[1000 0001]~~ indicating ISO/IEC 8473, then the procedures in 5.5.7.3.5.5.3 shall be performed.

5.7.3.5.5.2.3 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. 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 possibility 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, it should be noted that 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.*

### 5.7.3.5.5.3 Identification of Option Parameter and Local Directory Look-up

5.7.3.5.5.3.1 The options part of the ISO/IEC 8473 NPDU header contained in the SN-Userdata shall then be inspected. If ~~one~~either of the following is true:

- a) Source Routing option is present,
- b) Recording of Route options is present,
- c) ~~the~~ QoS Maintenance option is anything other than the globally unique format,
- d) padding option is present, a
- e) priority option is present with a value greater than 14,
- f) ~~or~~ an unknown parameter is present,

then the SN-Userdata shall be sent unchanged over the virtual circuit using M-bit segmentation procedures as appropriate.

5.7.3.5.5.3.2 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.

5.7.3.5.5.3.3 If an entry is found, then the NPDUs shall be sent in the compressed form constructed according to 5.5.7.3.5.6, using the local directory entry number as the local reference.

5.7.3.5.5.3.4 If no entry is found, then a new directory entry shall be created and the SN-Userdata shall be modified as specified in 5.7.3.5.5.4.

### 5.7.3.5.5.4 Establishing a New Local Reference

5.7.3.5.5.4.1 A new directory entry shall be created containing the NPDUs source NSAP Address as the inward NSAP Address, and the NPDUs destination NSAP Address as the outward NSAP Address.

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

5.7.3.5.5.4.3 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 virtual circuit, or **[64..127]** or **[16448..32767]**, if the SNDCF is the responder.

5.7.3.5.5.4.4 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.

5.7.3.5.5.4.5 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.*

5.7.3.5.5.4.6 **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.*

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

5.7.3.5.5.4.8 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.

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

5.7.3.5.5.4.10 This option shall be specified as follows:

Parameter Code:	<b>[0000 0101]</b>
Parameter Length:	variable
Parameter Value:	the entry number of the local directory entry created above and expressed as an unsigned integer.

*Note . — The entry number is therefore assigned as a so called Local Reference.*

5.7.3.5.5.4.11 The ~~C~~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.

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

#### 5.7.3.5.5.5 Reference Cancellation Option

5.7.3.5.5.5.1 When the optional ~~I~~Local ~~R~~reference ~~C~~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.

5.7.3.5.5.5.2 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 5.5.7.3.5.9 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.

#### 5.7.3.5.5.6 Transfer of the Modified ~~ISO/IECISØ 8473~~ PDU

5.7.3.5.5.6.1 The modified ~~ISO/IECISØ 8473~~ NPDU (i.e. the NPDU with the added Local Reference Option) shall be inserted in the User Data field of an ~~ISO/IECISØ 8208~~ Data packet and shall be sent over the virtual circuit, using the ~~ISO/IECISØ 8208~~ M-bit segmentation procedure if appropriate.

#### 5.7.3.5.6 Compression of SN-Userdata

##### 5.7.3.5.6.1 General

5.7.3.5.6.1.1 An Initial DT NPDU shall be compressed according to the procedures specified in 5.5.7.3.5.6.2.

5.7.3.5.6.1.2 A Derived DT NPDU shall be compressed according to the procedures specified in 5.5.7.3.5.6.3.

5.7.3.5.6.1.3 An ER NPDU shall be compressed according to the procedures specified in 5.5.7.3.5.6.4.

##### 5.7.3.5.6.2 Initial DT PDU Compression

###### 5.7.3.5.6.2.1 General

*Note.— An Initial DT PDU is an ~~ISO/IECISØ 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.

5.7.3.5.6.2.1.1 The original Initial DT PDU shall be compressed into the Compressed Initial Data PDU as shown in Figure 5.7-4.

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

#### 5.7.3.5.6.2.2 Type Field

5.7.3.5.6.2.2.1 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 5.5.7-4.

**Table 5.5.7-4 Initial DT PDU 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

#### 5.7.3.5.6.2.3 PDU Priority Field

5.7.3.5.6.2.3.1 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.

#### 5.7.3.5.6.2.4 PDU Lifetime Field

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

#### 5.7.3.5.6.2.5 P bit Field

5.7.3.5.6.2.5.1 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.

#### 5.7.3.5.6.2.6 Q bit Field

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

5.7.3.5.6.2.6.2 This field shall be set to zero otherwise.

#### 5.7.3.5.6.2.7 R bit Field

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

5.7.3.5.6.2.7.2 This field shall be set to zero otherwise.

#### 5.7.3.5.6.2.8 S/T, CE C/E, T/C, E/T, and E/C Fields

5.7.3.5.6.2.8.1 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.

5.7.3.5.6.2.8.2 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.

5.7.3.5.6.2.8.3 The CE C/E field shall be set to the value of bit 4 in the Quality of Service Maintenance parameter value field.

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

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

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

#### 5.7.3.5.6.2.9 EXP, Local-REF/A and Local-REF/B Fields

5.7.3.5.6.2.9.1 If the value of the Local Reference determined according to the procedure

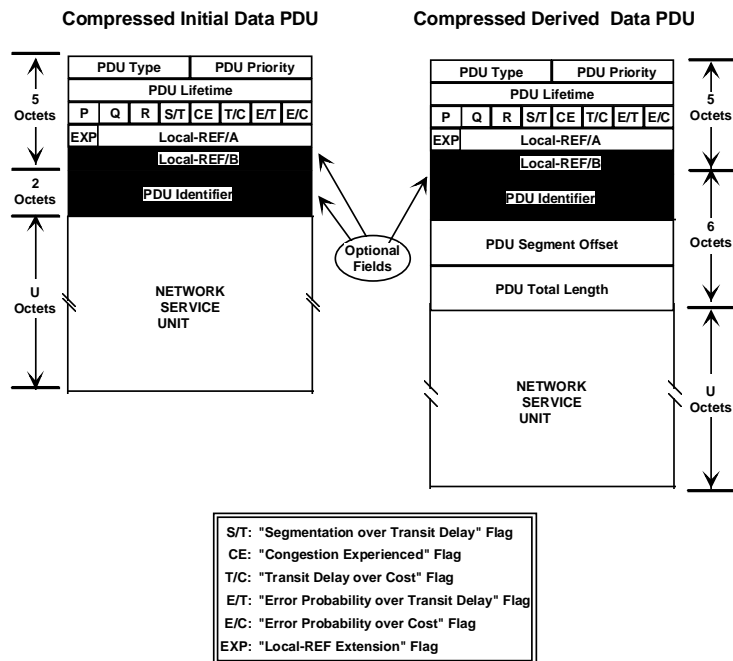


Figure 5.5.7-4 Compressed Initial and Derived PDU Formats

specified in 5.5.7.3.5.5.4 is less than 128, then the EXP field shall be set to zero.

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

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

5.7.3.5.6.2.9.4 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.

5.7.3.5.6.2.9.5 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.

**5.7.3.5.6.2.10 PDU Identifier**

5.7.3.5.6.2.10.1 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.

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

5.7.3.5.6.2.10.3 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.

**5.7.3.5.6.2.11 PDU Segment Offset**

5.7.3.5.6.2.11.1 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 SNDCE.

**5.7.3.5.6.2.12 PDU Total Length**

5.7.3.5.6.2.12.1 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.

#### 5.7.3.5.6.2.13 Network Service Data Unit Field

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

#### 5.7.3.5.6.3 Derived DT PDU Compression

##### 5.7.3.5.6.3.1 General

5.7.3.5.6.3.1.1 The original Derived DT PDU shall be compressed into the Compressed Derived Data PDU as shown in Figure 5.5.7-4.

5.7.3.5.6.3.1.2 The fields of the Compressed Derived Data PDU\_ shall be set as defined in the following sections follows.

##### 5.7.3.5.6.3.2 Type Field

5.7.3.5.6.3.2.1 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 5.5.7-5.

**Table 5.5.7-5 Derived PDU Type Codes**

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

##### 5.7.3.5.6.3.3 PDU Priority Field

5.7.3.5.6.3.3.1 This field shall be set as defined in 5.5.7.3.5.6.2.3.

##### 5.7.3.5.6.3.4 PDU Lifetime Field

5.7.3.5.6.3.4.1 This field shall be set as defined in 5.5.7.3.5.6.2.4.

##### 5.7.3.5.6.3.5 P bit\_Field

5.7.3.5.6.3.5.1 This field shall be set as defined in 5.5.7.3.5.6.2.5.

##### 5.7.3.5.6.3.6 Q bit\_Field

5.7.3.5.6.3.6.1 This field shall be set as defined in 5.5.7.3.5.6.2.6.

##### 5.7.3.5.6.3.7 S/T, CE C/E, T/C, E/T, and E/C Fields

5.7.3.5.6.3.7.1 These fields shall be set as defined in 5.5.7.3.5.6.2.8.

##### 5.7.3.5.6.3.8 EXP, Local-REF/A and Local-REF/B Fields

5.7.3.5.6.3.8.1 These fields shall be set as defined in 5.5.7.3.5.6.2.9.

##### 5.7.3.5.6.3.9 PDU Identifier Field

5.7.3.5.6.3.9.1 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.

##### 5.7.3.5.6.3.10 PDU Segment Offset Field

5.7.3.5.6.3.10.1 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.

##### 5.7.3.5.6.3.11 PDU Total Length Field

5.7.3.5.6.3.11.1 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.

#### 5.7.3.5.6.4 Error Report PDU Compression

##### 5.7.3.5.6.4.1 General

5.7.3.5.6.4.1.1 The original ER PDU shall be compressed into the Compressed Error Report PDU as shown in Figure 5.7-5.



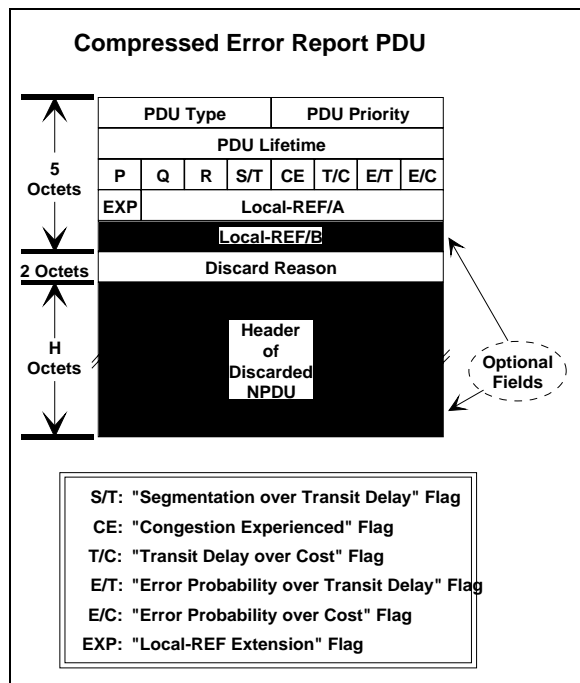


Figure 5.5.7-5 Compressed Error Report PDU

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

**5.7.3.5.6.4.2 PDU Type Field**

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

**5.7.3.5.6.4.3 PDU Priority Field**

5.7.3.5.6.4.3.1 This field shall be set as defined in 5.5.7.3.5.6.2.3.

**5.7.3.5.6.4.4 PDU Lifetime Field**

5.7.3.5.6.4.4.1 This field shall be set as defined in 5.5.7.3.5.6.2.4.

**5.7.3.5.6.4.5 P bit Field**

5.7.3.5.6.4.5.1 This field shall be as defined in 5.5.7.3.5.6.2.5.

**5.7.3.5.6.4.6 Q bit Field**

5.7.3.5.6.4.6.1 This field shall be set as defined in 5.5.7.3.5.6.2.6.

**5.7.3.5.6.4.7 S/T, CE, T/C, E/T and E/C Fields**

5.7.3.5.6.4.7.1 These fields shall be set as defined in 5.5.7.3.5.6.2.8.

**5.7.3.5.6.4.8 EXP, Local-REF/A, Local-REF/B Fields**

5.7.3.5.6.4.8.1 These fields shall be set as defined in 5.5.7.3.5.6.2.9.

**5.7.3.5.6.4.9 Discard Reason Field**

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

**5.7.3.5.6.4.10 Header of Discarded NPDU Field**

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

**5.7.3.5.6.4.11 Transfer of Compressed ISO/IEC 8473 PDUs**

5.7.3.5.6.4.11.1 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.

**5.7.3.5.7 Processing of Packets Received from the Subnetwork Service Provider**

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

**5.7.3.5.7.1 Initial Processing of NPDU**

5.7.3.5.7.1.1 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 5.5.7-6).

- 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 5.5.7.3.5.7.2.2.
- 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 5.5.7.3.5.7.3.
- 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 5.5.7.3.5.7.3.
- 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 5.5.7.3.5.7.4.
- 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 5.5.7.3.5.7.5, 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 5.5.7.3.5.9 and no SN-UNITDATA indication generated.

In all other cases, the PDU shall be discarded and an SNDCF Error Report Generated (see 5.5.7.3.5.8).

### 5.7.3.5.7.2 Incoming ISO/IEC 8473 PDU with Uncompressed Header

#### 5.7.3.5.7.2.1 General

5.7.3.5.7.2.1.1 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.

#### 5.7.3.5.7.2.2 Processing of Unmodified ISO/IEC 8473 PDUs

5.7.3.5.7.2.2.1 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.

#### 5.7.3.5.7.2.3 Processing of Modified ISO/IEC 8473 PDUs

5.7.3.5.7.2.3.1 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.

5.7.3.5.7.2.3.2 If a Local Reference options field was 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.

5.7.3.5.7.2.3.3 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

**Table 5.5.7-6 Mapping between Compressed PDU Type Fields and Uncompressed PDU Types**

Compressed PDU Type Field	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

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.

5.7.3.5.7.2.3.4 An SNDCF Error Report (see 5.5.7.3.5.8) 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~~permitted and given on the call request.~~

5.7.3.5.7.2.3.5 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.

5.7.3.5.7.2.3.6 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.

### 5.7.3.5.7.3 Incoming Compressed Data PDU

#### 5.7.3.5.7.3.1 General

5.7.3.5.7.3.1.1 If the most significant four bits of the ~~first~~<sup>second</sup> octet of a received PDU (i.e. the PDU Type field) are in the range [0000] to [0011] binary, excluding [1000] binary, then the packet is a compressed ISO/IEC 8473 Initial DT NPDU.

5.7.3.5.7.3.1.2 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.

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

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

5.7.3.5.7.3.1.5 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,~~the SNDCF shall generate a SNDCF Error Report (see 5. and the PDU shall be discarded. This report shall be sent to the peer SNDCF via an SN-UNITDATA indication with SN-Source Address and SN-Destination Address set to the local and remote DTE addresses for the virtual circuit, and the SN-Userdata shall contain the SNDCF Error Report.~~

5.7.3.5.7.3.1.6 If the Local-REF is valid, the original uncompressed NPDU shall be recreated by the procedures defined in 5.5.7.3.5.7.3.2 through 5.5.7.3.5.7.3.6.

5.7.3.5.7.3.1.7 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.

#### 5.7.3.5.7.3.2 Fixed Part

*Note 1. — The Fixed Part of the NPDU header shall consist 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.*

5.7.3.5.7.3.2.1 ~~The value of the local reference shall be extracted from the compressed header and the corresponding entry in the local directory located.~~

*Note 2. — If the EXP field is set to zero, the Local Reference ~~is~~ shall be the seven bit integer value of the Local-REF/A field. — If the EXP field is set to one, the Local Reference value shall consist 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. — The value of the Version/Protocol Identifier Extension and Source and Destination NSAP addresses shall be set the*

*the values provided in the corresponding directory entry.*

#### **5.7.3.5.7.3.2.2 Network Layer Protocol Identifier**

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

#### **5.7.3.5.7.3.2.3 Length Indicator**

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

#### **5.7.3.5.7.3.2.4 Version/Protocol Identifier Extension**

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

#### **5.7.3.5.7.3.2.5 PDU Lifetime**

5.7.3.5.7.3.2.5.1 The eight bits of the PDU Lifetime ~~f~~field shall be set to the eight bits of the PDU Lifetime field of the Compressed Data PDU.

#### **5.7.3.5.7.3.2.6 Segmentation Permitted, More Segments, Error Report Flags**

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

5.7.3.5.7.3.2.6.2 These flag values shall be determined according to Table 5.5.7-4 for an Initial Data PDU and ~~Table 5.5.7-5~~ for a Derived Data PDU.

#### **5.7.3.5.7.3.2.7 Type Code**

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

#### **5.7.3.5.7.3.2.8 Segment Length**

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

5.7.3.5.7.3.2.8.2 The value of this field shall be computed by the SND CF.

5.7.3.5.7.3.2.8.3 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.

#### **5.7.3.5.7.3.2.9 PDU Checksum**

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

5.7.3.5.7.3.2.9.2 Otherwise, a Checksum field ~~sh~~will 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.~~

#### **5.7.3.5.7.3.3 Address Part**

*Note.*—~~The Address Part shall~~ consist of the Destination Address Length Indicator, Destination Address, Source Address Length Indicator and Source Address as defined in ISO/IECISO 8473.

#### **5.7.3.5.7.3.3.1 Destination and Source Address Length Indicators and Addresses**

5.7.3.5.7.3.3.1.1 ~~The Source and Destination NSAP addresses shall be set to~~extracted from the values provided in the corresponding entry of ~~in~~ the local directory for the Local Reference number calculated.

5.7.3.5.7.3.3.1.2 The source NSAP Address shall be set to the value of the outward NSAP Address, and the destination NSAP Address ~~shall be~~ set to the value of the inward NSAP Address.

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

#### **5.7.3.5.7.3.4 Segmentation Part**

##### **5.7.3.5.7.3.4.1 General**

5.7.3.5.7.3.4.1.1 If ~~the~~ ISO/IECISO 8473 SP field is set to one, then the Segmentation Part shall be generated.

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

##### **5.7.3.5.7.3.4.2 Data Unit Identifier**

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

**5.7.3.5.7.3.4.3 Segment Offset**

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

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

**5.7.3.5.7.3.4.4 PDU Total Length**

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

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

**5.7.3.5.7.3.5 Options Part****5.7.3.5.7.3.5.1 General**

5.7.3.5.7.3.5.1.1 If the Q bit field is set to one, the Globally Unique QoS option shall be recreated according to 5.5.7.3.5.7.3.5.3.

5.7.3.5.7.3.5.1.2 If the Security option is present in the local reference directory entry, the Security option shall be recreated according to 5.5.7.3.5.7.3.5.4.

5.7.3.5.7.3.5.1.3 If the P bit field is set to one, the Priority option shall be recreated according to 5.5.7.3.5.7.3.5.2.

**5.7.3.5.7.3.5.2 Priority**

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

5.7.3.5.7.3.5.2.2 The four most significant bits of the Parameter Value shall be set to zero, and the four least significant bits shall be set to the PDU Priority field as provided in the compressed DT PDU.

**5.7.3.5.7.3.5.3 Quality of Service Maintenance**

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

5.7.3.5.7.3.5.3.2 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 shall be set to the S/T, CE E/E, T/C, E/T and E/C fields respectively as provided in the compressed Data PDU.

**5.7.3.5.7.3.5.4 Security**

5.7.3.5.7.3.5.4.1 This field shall be set to the value of the Ssecurity parameter contained in the corresponding Llocal Reference directory entry.

**5.7.3.5.7.3.6 Data Part**

5.7.3.5.7.3.6.1 The Data Part shall be copied from the NSDU as provided in the Compressed Data PDU data part.

**5.7.3.5.7.4 Incoming Compressed Error Report PDU****5.7.3.5.7.4.1 General**

5.7.3.5.7.4.1.1 The original uncompressed header shall be recreated as defined in the following sections follows.

*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 ISO 8473 ER NPDU.*

**5.7.3.5.7.4.2 Fixed Part**

5.7.3.5.7.4.2.1 The Fixed Part of the ER PDU shall be composed in the same manner as defined in 5.5.7.3.5.7.3.2 except for the Type Code which shall be set to binary [0001101] to indicate an ER PDU, and except for the SP and MS flags which shall be set to zeros.

**5.7.3.5.7.4.3 Address Part**

5.7.3.5.7.4.3.1 The Address Part of the ER PDU shall be composed in the same manner as defined in 5.5.7.3.5.7.3.3.

**5.7.3.5.7.4.4 Options Part**

5.7.3.5.7.4.4.1 The Options Part of the ER PDU shall be composed in the same manner as defined in 5.5.7.3.5.7.3.5 for an Initial DT PDU.

**5.7.3.5.7.4.5 Reason for Discard**

5.7.3.5.7.4.5.1 To compose this field, the Parameter Code shall be set to binary [1100 0001], the Parameter Length shall be set to two octets, and the Parameter Value set to shall contain the Discard Reason field as provided in the Compressed Error Report PDU.

**5.7.3.5.7.4.6 Error Report Data Part**

5.7.3.5.7.4.6.1 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.

**5.7.3.5.7.5 Incoming SNDCF Error Report**

5.7.3.5.7.5.1 On receipt of an SNDCF Error Report, the virtual circuit shall be reset (see 5.5.7.3.5.11), and ~~Systems Management informed of the problem,~~ unless the reason is "compressed PDU with unrecognized local reference".

5.7.3.5.7.5.2 In this case, the directory entry corresponding to the local reference returned in the SNDCF Error Report shall be reset to the unused state, ~~and~~

5.7.3.5.7.5.3 **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 5.5.7.3.5.8).~~

**5.7.3.5.8 SNDCF Error Report**

5.7.3.5.8.1 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.

5.7.3.5.8.2 The SNDCF Error Report PDU shall be constructed as follows:

- a) 1. — 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) 2. — The second octet is a discard reason encoded as an unsigned integer, with the following reason codes defined in the Table below:

**Table 5.5.7-7 SNDCF Error Report Diagnostic Codes**

<u>Code</u>	<u>Reason</u>
[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

~~reason = [0000 0000] — compressed NPDU with unrecognized local reference~~

~~reason = [0000 0001] — creation of directory entry outside of sender's permitted range~~

~~reason = [0000 0010] — directory entry exists~~

~~reason = [0000 0011] — local reference greater than maximum value accepted.~~

~~reason = [0000 0100] — Data Unit Identifier missing when SP=1.~~

~~reason = [0000 0101] — reserved.~~

~~reason = [0000 0111] — Compressed ISO/IEC ISO 8473 PDU with unrecognized Type.~~

~~reason = [0000 1000] — local reference cancellation error~~

- c) 3. — 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.

5.7.3.5.8.3 The data portion of the SNDCF Error Report shall be used to return a copy of the PDU in error, similarly to the ISO/IEC ISO 8473 Error Report PDU.

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

**5.7.3.5.9 Local Reference Cancellation Option**

**5.7.3.5.9.1 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.*

5.7.3.5.9.1.1 When an SNDCF invokes the procedures for Local Reference cancellation it shall format a Cancellation Request PDU, as specified below, and shall send the PDU to the other SNDCF over the virtual circuit to which it applies.

5.7.3.5.9.1.2 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.

5.7.3.5.9.1.3 When a Cancellation Accept PDU is received, the corresponding local references are now available for re-use and the corresponding

PDU Type	unused
Cancellation Reference	
L1	
EXP	Local-REF/A
	Local-REF/B
	.
	.
L2	
EXP	Local-REF/A
	Local-REF/B
	.

**Figure 5.5.7-6 Cancellation Request PDU**

directory entries shall be cleared, and the Local References therefore become available for re-use.

5.7.3.5.9.1.4 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.

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

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

**5.7.3.5.9.2 The Cancellation Request PDU**

5.7.3.5.9.2.1 The PDU format shall be as illustrated in Figure 5.5.7-6. 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 1.—In most cases uniqueness will be assured if the reference is implemented as a sequence number starting at zero and incremented by one ((modulo MOD 256)), each time a Cancellation Request is sent.*

- b) A length octet (L1) given as an unsigned integer (0 to 255), which indicates the length in octets of the set of individual Local References to cancel.

- c) One or more Local References expressed as one or two octets each, as appropriate, and encoded in successive octets, with the total number of octets containing such local references given by L1.

- d) A length octet (L2) given as an unsigned integer (0 to 255), which indicates the length in octets of the set of inclusive Local Reference ranges to cancel.

- e) One or more pairs of Local Reference ranges expressed as one or two octets each, as appropriate, and encoded in successive octets, with the total number of octets containing such Local References given by L2.

5.7.3.5.9.2.2 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

beis set to zero, and the remaining seven bits set to the value of the Local Reference encoded as an unsigned integer.

5.7.3.5.9.2.3 The extended Local Reference octet ~~shall~~is not ~~be~~ present.

5.7.3.5.9.2.4 Otherwise, bit eight ~~shall~~ beis set to one, and the remaining seven bits and the next octet ~~are~~ 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 2.—This format allows for the Local References to ~~be cancelled,~~ ~~to be expressed as either a set of individual references to be cancelled,~~ or a set of inclusive ranges of individual references to be cancelled, or both.*

### 5.7.3.5.9.3 The Cancellation Accept PDU

5.7.3.5.9.3.1 The PDU format ~~shall be as is~~ illustrated in Figure 5.5.7-7.

5.7.3.5.9.3.2 The first octet shall be set to binary **[0101 0000]**, and the second octet ~~set to~~shall contain the Cancellation Reference of the Cancellation Request which is being accepted.

### 5.7.3.5.10 Call Clearing Provisions

5.7.3.5.10.1 The Mobile SNDCF shall clear a virtual circuit when:

- a) System Management requests call clearing, or
- b) The expiration of a timeout period following the transmission or receipt of SN-UNITDATA, or
- c) The resources are required by another virtual circuit with a higher priority.

5.7.3.5.10.2 ~~Events~~Options b)2 or c)3 above shall only apply to those virtual circuits that have been dynamically established ~~—(see 5.5.7.3.5.5).~~

5.7.3.5.10.3 When it has been determined that a virtual circuit ~~is to~~shall be cleared, the SNDCF shall perform all functions associated with call clearing.

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

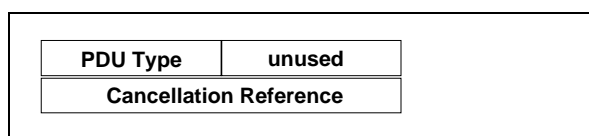
5.7.3.5.10.5 The same actions shall apply to the receipt of a Clear Indication.



**Table 5.5.7-8 Diagnostics values for ATN call clearing**

	Hexadecimal value	Decimal value	Clearing Cause
1	1111 1001	249	Connection Rejection - unrecognized protocol identifier in user data
2	1000 0000	128	Version number not supported
3	1000 0001	129	Length field invalid
4	1000 0010	130	Call Collision Resolution
5	1000 0011	131	Proposed Directory Size too large
6	1000 0100	132	Local Reference Cancellation Not Supported
7	1000 0101	133	Received DTE refused, received NET refused or invalid NET selector
8	1000 0110	134	Invalid SNCR field
9	1000 0111	135	ACA compression not supported
10	1000 1111	143	V42bis compression not supported
11	1111 0000	240	System lack of resources
12	0000 0000	0	Cleared by System Management
13	1001 0000	144	Idle Timer expiration
14	1001 0001	145	Need to re-use the circuit
15	1001 0010	146	By local means (to be used for system local error)
16	1001 0011	147	Invalid NSEL field value in received NET

When a virtual circuit has been terminated, then the local directory associated with the virtual



**Figure 5.5.7-7 Cancellation Accent PDU**

circuit shall be discarded.

5.7.3.5.10.6 The value of the Clearing Cause octet in the ISO/IEC ISO-8208 Cause/Diagnostic field which shall be set to used is [1000 0000].

5.7.3.5.10.7 The reason for clearing the code shall be placed in the Diagnostic field.

5.7.3.5.10.8 The diagnostic values listed in Table 5.5.7-8 shall be used when an SND CF rejects a Call Request or clears a virtual circuit.

*Note.*— If a virtual connection is cleared due to a network problem, the SND CF 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.

#### 5.7.3.5.11 Call Reset Provisions

5.7.3.5.11.1 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, there shall be no impact on this SNDCF.~~

5.7.3.5.11.2 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.

### 5.7.4 Convergence Provisions for ISO/IECISO 8802-2 Broadcast Subnetworks

5.7.4.1 The SNDCF for use with ISO/IEC 8802-2 Broadcast Subnetworks subnetwork service specified in 5.7.4 shall be implemented according to provided using ISO/IECISO 8473-28802-2 Broadcast Subnetworks as specified in Clause 8.4.2 of ISO/IECISO 8473.

### 5.7.5 Convergence Provisions for Common ICAO Data Interchange Network (CIDIN)

#### General Considerations

*Note.* — ~~CIDIN provides a Connectionless Mode transmission Service so that the functionality provided by CIDIN at level 4 is already very close to what is required by the ATN network protocol.~~

#### Mapping of the ATN Service Primitives to CIDIN

5.7.5.1.1 The SNDCF for CIDIN shall be as specified in the following sections: relationship between the ATN subnetwork primitives, their parameters, and the CIDIN protocol parameters shall be as follows.

#### 5.7.5.2 SN-UNITDATA Request and Indication Primitives

5.7.5.2.1 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.

5.7.5.2.2 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.~~

#### 5.7.5.3 SN Source Address

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

#### 5.7.5.4 SN Destination Address

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

#### 5.7.5.5 SN Quality of Service

5.7.5.5.1 *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.

#### 5.7.5.6 SN Priority

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

#### 5.7.5.7 SNS-Userdata

5.7.5.7.1 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.~~

### 5.7.6 ATN NSAP Compression Algorithm (ACA)

#### 5.7.6.1 General Overview

5.7.6.1.1 ~~When negotiated in the Mobile SND CF Call establishment phase, the optional ACA algorithms shall be applied as follows: compression processing (5.7.6.5) shall~~

- a) ~~the compression processing (5.7.6.5) be applied to data octets being output to the subnetwork, and~~ while

- b) the ACA decompression processing (5.5.7.6.6) shall be applied to data octets input from the subnetwork.

### 5.7.6.2 Address Length Determination

5.7.6.2.1 The address length for the address or address prefix to be compressed shall be extracted from the octet preceding the AFI octet in the uncompressed data stream.

5.7.6.2.2 If the extracted length lies in the range 7 through 20, the extracted length shall be used as the address "octet length" and the address length type shall be indicated as "normal".

5.7.6.2.3 If the extracted length lies in the range 56 through 160 and is an integral multiple of 8, the extracted length shall be divided by 8 to compute the length in octets of the address prefix and the address length type shall be indicated as "IDRP".

5.7.6.2.4 If the extracted length does not lie in either of these ranges, the input data does not form a compressible ATN NSAP address and the ACA shall not further process the current data as a compressible ATN NSAP address.

5.7.6.2.5 The octet length for ACA compressed address prefixes shall be encoded in the first header octet LEN/SEL subfield and the FP subfield shall be set to one.

5.7.6.2.6 If the octet length for the ACA compressed address is 20 (indicating a full address instead of a prefix) the FP subfield shall be set to zero.

5.7.6.2.7 The explicit address length octet shall be removed as part of the ACA compression processing.

*Note 1.—No length octet is required for compressed ACA addresses. All information concerning address length and the presence or length of variable-length fields is contained in the header octets.*

*Note 2.—The shortest ATN NSAP address prefix that can be compressed is 7 octets and the length of a full ATN address is 20 octets.*

*Note 3.—Address lengths for normal addresses and prefixes are expressed in octet units. The address lengths for IDRP addresses and prefixes are expressed in bit units (even though the address lengths are always in full octets).*

*Note 4.—The IDRP subfield in the first header octet indicates whether the expanded address used octet or bit length units. Internal (compressed) addresses assume octet lengths for encoding.*

### 5.7.6.3 Compressed Address Structure

#### 5.7.6.3.1 General

5.7.6.3.1.1 An ACA compressed address or address prefix shall consist of the following components in the order shown below:

**Table 5.5.7-9 Compressed NSAP Address Format**

Name	Length (octets)	Reference
Address Marker	2	7.9.4
Header Octet 1	1	7.9.3.1.1
Header Octet 2	1	7.9.3.1.2
Compressed ADM	2 or 3	7.9.3.2
Variable Fields	0 to 14	7.9.3.3

The coding and use of each component shall be as defined below.

*Note.—Multi-octet uncompressed ATN address fields (ADM, ARS, LOC, and SYS) are processed from left to right, i.e. from most-significant to least-significant octet.*

#### 5.7.6.3.2 Address Header Octets

##### 5.7.6.3.2.1 General

5.7.6.3.2.1.1 Two header octets shall begin each compressed address or address prefix.

5.7.6.3.2.1.2 All bits of these header octets shall be set to zero unless otherwise specified in the following subparagraphs.

5.7.6.3.2.1.3 Bits in each header octet shall be assigned from the high-order (most-significant or left-most).

*Note.—The value of the first header octet is never zero for any compressed address. This prevents confusing a compressed address with an embedded address marker (5.5.7.6.4.3).*

##### 5.7.6.3.2.2 First Header Octet

###### 5.7.6.3.2.2.1 General

5.7.6.3.2.2.1.1 The first header octet of a compressed address shall be subdivided into four subfields as follows:

19	5	end with SYS
--	6, 7	unassigned

**Table 5.7-10.**

Name	Length Nb of (bits)	Comments
IDRP	1	Units of address length
FP	1	Full address of prefix
LEN/SEL	3	Address length or SEL code
CVER	3	Compressed VER value

The coding and use of each subfield shall be as defined below

#### 5.7.6.3.2.2.2 IDRP Subfield

5.7.6.3.2.2.2.1 If the address length determination process (5.5.7.6.1, 5.5.7.6.2) indicates that the address to be compressed expresses length in octet units, the IDRP subfield shall be set to zero.

5.7.6.3.2.2.2.2 If the address expresses length in bit units (i.e. IDRP address), the IDRP subfield shall be set to one.

#### 5.7.6.3.2.2.3 FP Subfield

5.7.6.3.2.2.3.1 The FP subfield shall be set to one if the address to be compressed is an address prefix.

5.7.6.3.2.2.3.2 The FP subfield shall be set to zero if the address to be compressed is a full address (i.e. its octet length is 20).

#### 5.7.6.3.2.2.4 LEN/SEL Subfield

5.7.6.3.2.2.4.1 If the address to be compressed is an address prefix (the FP subfield is set to one), the LEN/SEL subfield shall be set to the the prefix length encoded using the encodings in the following table:

**Table 5.7-11.**

Length	Encoding	Comments
--	0	reserved
7	1	end with ADM
8	2	end with RDF
11	3	end with ARS
13	4	end with LOC

5.7.6.3.2.2.4.2 If the length is not found in this encoding table then the input data does not form an ATN NSAP address prefix that can be compressed and the address prefix shall not be further processed.

5.7.6.3.2.2.4.3 If the address to be compressed is a full address (the FP subfield is set to zero), the LEN/SEL subfield shall be set to the encoded value of the address SEL field (5.4.2.45-9.3) using encodings in the following table:

**Table 5.7-12.**

SEL	Encoding	Comments
--	0	reserved
00 hex	1	NET
fe hex	2	NET of an airborne router not supporting IDRP
--	3, 4, 5, 6	unassigned
--	7	other SEL codes

If the SEL field value in the address to be compressed is not one of the table entries above, the LEN/SEL encoding value shall be set to 7.

*Note* .— A LEN/SEL subfield value of zero is not allowed in either encoding to insure that the first header octet can never have the value [00] hexadecimal. Hence, no compressed address can be confused with an embedded address marker (5.5.7.6.4.3).

#### 5.7.6.3.2.2.5 CVER Subfield

5.7.6.3.2.2.5.1 If the value of the VER field in the address is in the range [01]-[07], [41]-[47], [81]-[87], or [c1]-[c7], then the CVER subfield shall be set to the low-order 3 bits of the VER value.

5.7.6.3.2.2.5.2 If the value of the VER field in the address is not in one of the above ranges, then the CVER subfield shall be set to zero.

*Note*.— The encoding of the version numbers in ATN addresses is defined in 5.4.2.45.3.4.

#### 5.7.6.3.2.3 Second Header Octet

##### 5.7.6.3.2.3.1 General

5.7.6.3.2.3.1.1 The second header octet of a compressed address shall be subdivided into 8 subfields as follows:

**Table 5.7-13.**

Name	LengthNb of (bits)	Comments
ADMF	1	Flag compressed ADM value
T/I	1	ATSC/AINSC
F/M	1	Fixed/Mobile
ARSD	1	Flag defaulted ARS value
LOCD	1	Flag defaulted LOC value
SYS6	1	Flag octet 6 of SYS = 0
SYS5	1	Flag octet 5 of SYS = 0
SYS4	1	Flag octet 4 of SYS = 0

5.7.6.3.2.3.1.2 The encodings and use of each subfield shall be as defined below.

**5.7.6.3.2.3.2 ADMF Subfield**

5.7.6.3.2.3.2.1 The ADMF subfield shall be set to one if the ADM value in the address to be compressed may be encoded into two octets using the identifier metacharacter syntax (5.4.2.34.7).

5.7.6.3.2.3.2.2 The ADMF subfield shall be set to zero if the ADM value in the address to be compressed cannot be expressed using the identifier metacharacter syntax.

*Note.— The ADM value can be compressed if each of its three octets contain a character from one of the following character classes:*

- a) An upper-case letter "A-Z"
- b) A decimal digit "0-9"
- c) The "@" character.

**5.7.6.3.2.3.3 T/I Subfield**

5.7.6.3.2.3.3.1 The T/I subfield shall be set to zero if the VER value in the address to be compressed lies in the ranges [01]-[3f] or [41]-[7f], indicating that the address is in the AINSC domain.

5.7.6.3.2.3.3.2 The T/I subfield shall be set to one if the VER value in the address to be compressed lies in the ranges [81]-[bf] or [c1]-[ff], indicating that the address is in the ATSC domain.

5.7.6.3.2.3.3.3 If the VER value in the address to be compressed is either [00], [40], [80], or [c0], then the T/I subfield shall be set to zero.

*Note. — The encoding of the VER field in an ATN address is defined in 5.4.2.4.3.45.3.3.*

**5.7.6.3.2.3.4 F/M Subfield**

5.7.6.3.2.3.4.1 The F/M subfield shall be set to zero if the VER value in the address to be compressed lies in the ranges [01]-[3f] or [81]-[bf], indicating that the address is a fixed system.

5.7.6.3.2.3.4.2 The F/M subfield shall be set to one if the VER value in the address to be compressed lies in the ranges [41]-[7f] or [c1]-[ff], indicating that the address is a Mmobile system.

*Note.— The values [00], [40], [80] and [c0] are not used in the VER field of an ATN address (see 5.4.2.45.3.3)*

**5.7.6.3.2.3.5 ARSD Subfield**

5.7.6.3.2.3.5.1 The ARSD subfield shall be set to zero if the ARS value in the address to be compressed is not the default value ([000001] hexadecimal) or if the address prefix to be compressed does not include an ARS field.

5.7.6.3.2.3.5.2 The ARSD subfield shall be set to one if the ARS value in the address to be compressed has the default value (5.4.2.45.6.5).

**5.7.6.3.2.3.6 LOCD Subfield**

5.7.6.3.2.3.6.1 The LOCD subfield shall be set to zero if the LOC value in the address to be compressed is not the default value ([0001] hexadecimal) or if the address prefix to be compressed does not include a LOC field. The LOCD subfield shall be set to one if the LOC value in the address to be compressed has the default value (5.4.2.45.7.5).

**5.7.6.3.2.3.7 SYS6 Subfield**

5.7.6.3.2.3.7.1 The SYS6 subfield shall be set to zero if the value of the high-order (6th) octet of the SYS field in the address to be compressed is zero or if the address prefix to be compressed does not include a SYS field.

5.7.6.3.2.3.7.2 The SYS6 subfield shall be set to one if the value of the high-order (6th) octet of the SYS field in the address to be compressed is nonzero.

**5.7.6.3.2.3.8 SYS5 Subfield**

5.7.6.3.2.3.8.1 The SYS5 subfield shall be set to zero if the value of the second to high-order (5th) octet of the SYS field in the address to be compressed is zero or if the address prefix to be compressed does not include a SYS field.

5.7.6.3.2.3.8.2 The SYS5 subfield shall be set to one if the value of the second to high-order (5th) octet of the SYS field in the address to be compressed is nonzero.

**5.7.6.3.2.3.9 SYS4 Subfield**

5.7.6.3.2.3.9.1 The SYS4 subfield shall be set to zero if the value of the third to high-order (4th) octet of the SYS field in the address to be compressed is zero or if the address prefix to be compressed does not include a SYS field.

5.7.6.3.2.3.9.2 The SYS4 subfield shall be set to one if the value of the third to high-order (4th) octet of the SYS field in the address to be compressed is nonzero.

**5.7.6.3.3 Compressed ADM Field**

5.7.6.3.3.1 If the ADM field value of the address to be compressed follows the syntax of an identifier (5.4.2.34.7) then the compressed ADM field shall consist of two octets and shall contain the encoded value of the identifier obtained by applying the definitions in 5.4.2.34.7 to the ADM field value.

5.7.6.3.3.2 If the ADM field value of the address to be compressed does not follow the identifier syntax then the compressed ADM field shall consist of three octets and shall contain the 3-octet ADM value unchanged.

*Note.— The value of the ADMF subfield in the second header octet indicates whether the compressed ADM field has the 2-octet (compressed) or 3-octet (uncompressed) format.*

**5.7.6.3.4 Variable Fields**

5.7.6.3.4.1 The variable fields shall have a minimum length of 0 octets and a maximum length of 13 octets. Variable field data octets shall be concatenated when required in the order that their fields occur in the ATN address (Figure 5.7-32) as follows:

- a) VER value (if > 7), 1 octet
- b) ARS value (if not default), 3 octets

- c) LOC value (if not default), 2 octets
- d) SYS octet 6 value (if nonzero), 1 octet
- e) SYS octet 5 value (if nonzero), 1 octet
- f) SYS octet 4 value (if nonzero), 1 octet
- g) SYS octets 3-1, 3 octets
- h) SEL value (if not defined in 5.4.2.45.9.3), 1 octet

5.7.6.3.4.2 The ACA compression of address prefixes shall omit those variable fields b) through h) which are not present in the uncompressed address prefix.

**5.7.6.4 Compressed Address Marker****5.7.6.4.1 General**

5.7.6.4.1.1 The ACA shall prefix each compressed address or address prefix with an address marker.

5.7.6.4.1.2 The address marker shall consist of two octets with the value [55aa] hexadecimal.

5.7.6.4.1.3 The ACA shall process the case of the address marker value occurring in the input octet stream as defined in 5.5.7.6.4.3 below.

**5.7.6.4.2 Normal Address Case**

5.7.6.4.2.1 In the case of a normal compressed address or address prefix, the header octets of the compressed address format (5.5.7.6.3) shall follow the address marker.

*Note.— The first header octet of a compressed address can never have the value [00]. This distinguishes the normal address case from the embedded address case.*

**5.7.6.4.3 Embedded Address Marker Case**

5.7.6.4.3.1 If two octets with the value of an address marker occur in data, a padding octet with value [00] hexadecimal shall be inserted into the data stream following the embedded address marker octets.

*Note 1.—The likelihood of embedded address markers in the input data stream is very low. When they occur, however, the ACA algorithm must add the extra padding octet. Hence, it is possible*

(although highly unlikely) for the ACA to expand data.

*Note 2.— The design of the ACA requires that the first header octet of a compressed address can never have the value [00] hexadecimal. Hence, the first header octet of a compressed address cannot be confused with the padding octet of an embedded address marker.*

## 5.7.6.5 Compression Algorithm

### 5.7.6.5.1 General

5.7.6.5.1.1 The ACA shall perform compression by replacing ATN addresses or address prefixes identified in the input octet stream with compressed, encoded equivalents as defined below.

5.7.6.5.1.2 The format of a compressed address shall be as defined in 5.5.7.6.3.

5.7.6.5.1.3 Each compressed address shall be prefixed with a compressed address marker (5.5.7.6.4).

5.7.6.5.1.4 Any embedded address markers found in the input octet stream shall be padded with a null-value octet (5.5.7.6.4.3).

5.7.6.5.1.5 The overall logic flow of the ACA compression processing shall be as defined in 5.5.7.6.5.3.

### 5.7.6.5.2 Address Encoding Process

#### 5.7.6.5.2.1 General

5.7.6.5.2.1.1 The process of encoding an ATN address or address prefix into the ACA compressed format (5.5.7.6.3) shall be performed using the sequence of steps defined in this paragraph.

5.7.6.5.2.1.2 The steps shall be performed in the order they are listed.

5.7.6.5.2.1.3 If any step of the encoding process fails, the ACA compression processing shall not consider the current input octets as an address and shall continue with the compression logic.

#### 5.7.6.5.2.2 Encoding Address Length

5.7.6.5.2.2.1 Determination of the length in octets of an address to be compressed shall be performed as defined in 5.7.6.2, 10.9.2.

5.7.6.5.2.2.2 If the address length is of type "normal", the IDRP subfield in the first header octet shall be set to zero.

5.7.6.5.2.2.3 Otherwise, the IDRP subfield shall be set to one.

5.7.6.5.2.2.4 If the octet length of the address is 20 (indicating a full ATN address), the FP subfield in the first header octet shall be set to zero.

5.7.6.5.2.2.5 If the octet length of the address is less than 20 (indicating an address prefix), the FP subfield shall be set to one and the address length shall be encoded in the LEN/SEL subfield of the first header octet according to the table in 5.5.7.6.3.2.2.4.

5.7.6.5.2.2.6 If the address length is not found in the length table, the encoding process shall halt and the current input octet string shall not be treated as an ATN address.

#### 5.7.6.5.2.3 Encoding the AFI and IDI Fields

5.7.6.5.2.3.1 No encoding shall be performed on the constant values of the address AFI and IDI fields.

5.7.6.5.2.3.2 These fields shall be omitted from the compressed address encoding.

#### 5.7.6.5.2.4 Encoding the VER Field

5.7.6.5.2.4.1 If the VER value in the address to be compressed lies within the range [01]-[3f], the T/I subfield in the second header octet shall be set to zero and the F/M subfield in the second header octet shall be set to zero.

5.7.6.5.2.4.2 If the VER value lies within the range [01]-[07], then the low-order 3 bits of the VER value shall be stored in the CVER subfield of the first header octet.

5.7.6.5.2.4.3 If the VER value lies in the range [08]-[3f], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded address.

5.7.6.5.2.4.4 If the VER value in the address to be compressed lies within the range [41]-[7f], the T/I subfield in the second header octet shall be set to zero and the F/M subfield in the second header octet shall be set to one.

5.7.6.5.2.4.5 If the VER value lies within the range [41]-[47], then the low-order 3 bits of the

VER value shall be stored in the CVER subfield of the first header octet.

5.7.6.5.2.4.6 If the VER value lies in the range [48]-[7f], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded address.

5.7.6.5.2.4.7 If the VER value in the address to be compressed lies within the range [81]-[bf], the T/I subfield in the second header octet shall be set to one and the F/M subfield in the second header octet shall be set to zero.

5.7.6.5.2.4.8 If the VER value lies within the range [81]-[87], then the low-order 3 bits of the VER value shall be stored in the CVER subfield of the first header octet.

5.7.6.5.2.4.9 If the VER value lies in the range [88]-[bf], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded address.

5.7.6.5.2.4.10 If the VER value in the address to be compressed lies within the range [c1]-[ff], the T/I subfield in the second header octet shall be set to one and the F/M subfield in the second header octet shall be set to one.

5.7.6.5.2.4.11 If the VER value lies within the range [c1]-[c7], then the low-order 3 bits of the VER value shall be stored in the CVER subfield of the first header octet.

5.7.6.5.2.4.12 If the VER value lies in the range [c8]-[ff], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded address.

5.7.6.5.2.4.13 If the VER value is either [00], [40], [80], or [c0], the encoding process shall halt and the current input octet string shall not be treated as an ATN address.

#### 5.7.6.5.2.5 *Encoding the ADM Field*

5.7.6.5.2.5.1 If the three octets of the ADM field in the address to be compressed do not follow the rules for Identifier Syntax (5.4.2.34.7), the ADMF subfield in the second header octet shall be set to zero and the three octets of the ADM field value shall be concatenated to the compressed ADM of the encoded address.

5.7.6.5.2.5.2 If the ADM field value does follow the Identifier Syntax rules, the ADMF subfield shall be set to one and the two-octet compressed

ADM value (5.5.7.6.3.3) shall be concatenated to the compressed ADM of the encoded address.

#### 5.7.6.5.2.6 *Encoding the RDF Field*

5.7.6.5.2.6.1 If the address length indicates an address prefix whose length is less than or equal to 7, no RDF field value shall be encoded and the encoding process shall halt.

5.7.6.5.2.6.2 If the RDF value in the address to be compressed is not [00], the encoding process shall halt and the current input octet string shall not be treated as an ATN address.

#### 5.7.6.5.2.7 *Encoding the ARS Field*

5.7.6.5.2.7.1 If the address length indicates an address prefix whose length is less than or equal to 8, no ARS field value shall be encoded and the encoding process shall halt.

5.7.6.5.2.7.2 If the ARS value of the address to be compressed has the default value ([000001] hexadecimal), the ARSD subfield in the second header octet shall be set to one.

5.7.6.5.2.7.3 If the ARS value of the address to be compressed is not default, the ARSD subfield shall be set to zero and the three octets of the ARS value shall be concatenated to the variable field data of the encoded address.

#### 5.7.6.5.2.8 *Encoding the LOC Field*

5.7.6.5.2.8.1 If the address length indicates an address prefix whose length is less than or equal to 11, no LOC field value shall be encoded and the encoding process shall halt.

5.7.6.5.2.8.2 If the LOC value of the address to be compressed has the default value ([0001] hexadecimal), the LOCD subfield in the second header octet shall be set to one.

5.7.6.5.2.8.3 If the LOC value of the address to be compressed is not default, the LOCD subfield shall be set to zero and the two octets of the LOC value shall be concatenated to the variable field data of the encoded address.

#### 5.7.6.5.2.9 *Encoding the SYS Field*

5.7.6.5.2.9.1 If the address length indicates an address prefix whose length is less than or equal to 13, no SYS field value shall be encoded and the encoding process shall halt.



5.7.6.5.2.9.2 If the high-order (6th) octet of the SYS field of the address to be compressed has a nonzero value, the SYS6 subfield in the second header octet shall be set to zero and the value of the SYS field octet shall be concatenated to the variable field data of the encoded address. Otherwise, the SYS6 subfield shall be set to one.

5.7.6.5.2.9.3 If the second to high-order (5th) octet of the SYS field of the address to be compressed has a nonzero value, the SYS5 subfield in the second header octet shall be set to zero and the value of the SYS field octet shall be concatenated to the variable field data of the encoded address.

5.7.6.5.2.9.4 Otherwise, the SYS5 subfield shall be set to one.

5.7.6.5.2.9.5 If the third to high-order (4th) octet of the SYS field of the address to be compressed has a nonzero value, the SYS4 subfield in the second header octet shall be set to zero and the value of the SYS field octet shall be concatenated to the variable field data of the encoded address.

5.7.6.5.2.9.6 Otherwise, the SYS4 subfield shall be set to one.

5.7.6.5.2.9.7 The three remaining octets of the SYS field shall be concatenated to the variable field data of the encoded address.

#### 5.7.6.5.2.10 *Encoding the SEL Field*

5.7.6.5.2.10.1 If the address length indicates an address prefix whose length is less than or equal to 19, no SEL field\_value shall be encoded and the encoding process shall halt.

5.7.6.5.2.10.2 Since the address length indicates a full ATN address, the FP subfield in the first header octet shall be set to zero.

5.7.6.5.2.10.3 The SEL value shall be encoded into the LEN/SEL subfield in the first header octet according to the table in 5.5.7.6.3.2.2.4.

5.7.6.5.2.10.4 If the SEL value is not one of the table entries, the LEN/SEL subfield shall be set to 7 and the SEL value octet shall be concatenated to the variable field data of the encoded address.

#### 5.7.6.5.3 **Compression Logic Flow**

5.7.6.5.3.1 The ACA compression logic shall process octets sequentially from the uncompressed data input stream.

5.7.6.5.3.2 For each input octet, a test shall be performed to determine if the current octet and the subsequent octets form an ATN address or address prefix.

5.7.6.5.3.3 If they do form an ATN address, the ACA shall attempt to encode the address into the compressed address format (5.5.7.6.3) as defined in the steps of 5.5.7.6.5.2.

5.7.6.5.3.4 If the encoding process is successful, a compressed address marker (5.5.7.6.4) shall be output to the compressed octet stream followed by the compressed address octets.

5.7.6.5.3.5 The compression processing shall then continue with the next uncompressed data octet not a part of the address just processed.

5.7.6.5.3.6 If the encoding process fails, or if the current octet does not begin an ATN address, the ACA processing shall check at the current uncompressed octet position in the input data stream for an embedded address marker (5.5.7.6.4.3).

5.7.6.5.3.7 If an embedded address marker is found, the ACA shall copy the address marker octets to the compressed output octet stream. A padding zero-valued octet shall be output as well as the address marker.

5.7.6.5.3.8 The compression processing shall then continue with the next uncompressed data octet not a part of the embedded address marker.

5.7.6.5.3.9 If neither an ATN address or embedded address mark is found, the ACA shall copy the current uncompressed input octet to the compressed output octet stream and shall continue processing with the next sequential input octet.

*Note.— Since the ACA compression logic may not recognize the appearance of an ATN address or prefix in the data stream until after the uncompressed length octet has been processed (the length octet precedes the fixed-value ATN AFI and IDI fields that distinguish an ATN address), the ACA compression process will need to be able to recall the value of the previous input octet during compression processing. Hence, a one-octet "backup" may be necessary in the implementation of the ACA compression logic.*

#### 5.7.6.6 **Decompression Algorithm**

##### 5.7.6.6.1 **General**

5.7.6.6.1.1 The ACA shall perform decompression by replacing compressed ATN addresses or address prefixes in the ACA compressed format (5.5.7.6.3) with their expanded equivalent as defined below. Address markers and padding octets shall be removed from the data stream during ACA decompression processing.

5.7.6.6.1.2 The overall logic flow of the ACA decompression processing shall be as defined in 5.5.7.6.5.3.

### 5.7.6.6.2 Address Decoding Process

#### 5.7.6.6.2.1 General

5.7.6.6.2.1.1 The process of decoding a compressed ATN address or address prefix from the ACA compressed format (5.5.7.6.3) shall be performed using the sequence of steps defined in the following paragraphs.

5.7.6.6.2.1.2 The steps shall be performed in the order listed below. The expanded address or prefix shall include the decoded address length octet and the decoded 7-20 address octets.

#### 5.7.6.6.2.2 Decoding Address Length

5.7.6.6.2.2.1 If the FP subfield in the first header octet is zero, the octet length of the compressed address shall be set to 20 (a full ATN address).

5.7.6.6.2.2.2 Otherwise, the octet length of the compressed address prefix shall be decoded from the LEN/SEL subfield in the first header octet according to the table in 5.5.7.6.3.2.2.4.

5.7.6.6.2.2.3 The address octet length shall be used in the further decoding process steps.

5.7.6.6.2.2.4 If the IDRP subfield in the first header octet is zero, the output address length shall be the address octet length.

5.7.6.6.2.2.5 Otherwise, the output address length shall be 8 times the address octet length.

*Note.— The address octet length is an internal variable used in the decoding process. The output length prefixed to the expanded address after the decoding process is completed is either the same as the octet length (normal case) or 8 times the octet length (IDRP case, length in bits).*

#### 5.7.6.6.2.3 Decoding the AFI and IDI Fields

5.7.6.6.2.3.1 The AFI field of the decoded address shall be set to its constant value of [47] hexadecimal.

5.7.6.6.2.3.2 The IDI field of the decoded address shall be set to its constant value of [0027] hexadecimal.

#### 5.7.6.6.2.4 Decoding the VER Fields

5.7.6.6.2.4.1 If the CVER subfield in the first header octet is zero, the VER octet shall be extracted from the next octet in the variable field of the compressed address.

5.7.6.6.2.4.2 If the CVER subfield is non-zero, then the VER field value in the expanded address shall be computed as follows:

- a) If the T/I subfield in the second header octet is zero and the F/M subfield in the second header octet is zero, then the VER field value shall be set to the CVER value.
- b) If the T/I subfield in the second header octet is zero and the F/M subfield in the second header octet is one, then the VER field value shall be set to the CVER value plus 64.
- c) If the T/I subfield in the second header octet is one and the F/M subfield in the second header octet is zero, then the VER field value shall be set to the CVER value plus 128.
- d) If the T/I subfield in the second header octet is one and the F/M subfield in the second header octet is one, then the VER field value shall be set to the CVER value plus 192.

#### 5.7.6.6.2.5 Decoding the ADM Fields

5.7.6.6.2.5.1 If the ADMF subfield in the second header octet is set to zero, the three octets of the ADM field shall be extracted from the next three octets in the variable field data.

5.7.6.6.2.5.2 Otherwise, the ADM field value shall be decoded from the compressed ADM which is extracted from the next two octets in the variable field data of the compressed address.

5.7.6.6.2.5.3 The decoding of the compressed ADM value shall be performed as defined in 5.4.2.34.7.

#### 5.7.6.6.2.6 Decoding the RDF Fields

5.7.6.6.2.6.1 The RDF field in the expanded address shall be set to zero.

**5.7.6.6.2.7 Decoding the ARS Fields**

5.7.6.6.2.7.1 If the address length indicates an address prefix whose length is less than or equal to 8, no ARS field value shall be decoded and the decoding process shall halt.

5.7.6.6.2.7.2 If the ARSD subfield in the second header octet of the compressed address is set to one, the expanded ARS field shall be set to the default value ([000001] hexadecimal).

5.7.6.6.2.7.3 Otherwise, the expanded ARS field value shall be extracted from the next three octets in the variable field data of the compressed address.

**5.7.6.6.2.8 Decoding the LOC Fields**

5.7.6.6.2.8.1 If the address length indicates an address prefix whose length is less than or equal to 11, no LOC field value shall be decoded and the decoding process shall halt.

5.7.6.6.2.8.2 If the LOCD subfield in the second header octet of the compressed address is set to one, the expanded LOC field shall be set to the default value ([0001] hexadecimal).

5.7.6.6.2.8.3 Otherwise, the expanded LOC field value shall be extracted from the next two octets in the variable field data of the compressed address.

**5.7.6.6.2.9 Decoding the SYS Fields**

5.7.6.6.2.9.1 If the address length indicates an address prefix whose length is less than or equal to 13, no SYS field value shall be decoded and the decoding process shall halt.

5.7.6.6.2.9.2 If the SYS6 subfield in the second header octet has the value one, the high-order (6th) octet of the expanded SYS field shall be extracted from the next octet in the variable data field of the compressed address.

5.7.6.6.2.9.3 Otherwise, the high-order (6th) octet of the expanded SYS field shall be set to zero.

5.7.6.6.2.9.4 If the SYS5 subfield in the second header octet has the value one, the second to high-order (5th) octet of the expanded SYS field shall be extracted from the next octet in the variable data field of the compressed address. Otherwise, the second to high-order (5th) octet of the expanded SYS field shall be set to zero.

5.7.6.6.2.9.5 If the SYS4 subfield in the second header octet has the value one, the third to

high-order (4th) octet of the expanded SYS field shall be extracted from the next octet in the variable data field of the compressed address.

5.7.6.6.2.9.6 Otherwise, the third to high-order (4th) octet of the expanded SYS field shall be set to zero.

5.7.6.6.2.9.7 The remaining three octets of the expanded SYS field shall be extracted from the next three octets in the variable data field of the compressed address.

**5.7.6.6.2.10 Decoding the SEL Fields**

5.7.6.6.2.10.1 If the address length indicates an address prefix whose length is less than or equal to 19, no SEL field value shall be decoded and the decoding process shall halt.

5.7.6.6.2.10.2 If the FP subfield in the first header octet has the value zero (indicating a full ATN address), then the value of the SEL field shall be decoded from the LEN/SEL subfield in the first header octet.

5.7.6.6.2.10.3 If the value of the LEN/SEL subfield lies in the range 1-2 the SEL value shall be decoded using the SEL encoding table in 5.5.7.6.3.2.2.4.

5.7.6.6.2.10.4 If the LEN/SEL subfield encoding has the value 7, the SEL field value shall be extracted from the next octet in the variable data field of the compressed address.

*Note.— Only a full ATN address (not a prefix) includes a SEL field.*

**5.7.6.6.3 Decompression Logic Flow**

5.7.6.6.3.1 The ACA decompression logic shall process octets sequentially from the compressed data input stream.

5.7.6.6.3.2 If the octet at the current input position and the next octet do not form a compressed address marker (5.5.7.6.4), the current input octet shall be copied to the decompressed output octet stream and decompression processing shall continue with the next input octet.

5.7.6.6.3.3 When a compressed address marker is found in the input octet stream, the decompression processing shall examine the value of the next octet beyond the address marker.

5.7.6.6.3.4 If the value of this octet is zero (indicating an embedded address mark

(5.5.7.6.4.3), the compressed address marker octets shall be copied to the decompressed output octet stream and the zero-value octet shall be dropped from the output stream.

5.7.6.6.3.5 If the value is nonzero (indicating a compressed ATN address), the compressed address shall be decoded according to 5.5.7.6.6.2.

5.7.6.6.3.6 The decoded address octets shall be copied to the decompressed octet output stream and decompression processing shall continue with the next input octet beyond those that formed the compressed ATN address.

5.7.6.6.3.7 The compressed address marker octets shall not be copied to the output.

## 5.7.7 ATN SNDCF Protocol Requirements List--introduction

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 the following sections. The Requirements for the ATN SNDCF are provided in the form of an ATN Profile Requirements List (APRLs). Three types of tables have been created :

A first set of APRLs tables has been defined for mobile subnetworks, to summarize the requirements defined in the present Chapter of the ATNCNS/ATM-1 Package SARPs and to indicate the strength of the requirements (mandatory, optional, conditional). The syntax used to describe these APRLs is the same as the one used by ISO for the ISO protocols PICS description.

- A second set of APRLs tables has been defined to summarize the SNDCF requirements relating to Subnetwork Routing Initiation and Termination.

## 5.7.8 ATN Requirements for Mmobile S~~N~~DCF~~s~~

*Note . This section specifies the requirements for the Mmobile SNDCF infor the relevantATN CNS/ATM-1 Package Airborne and Air/Ground RoutersIntermediate Systems's.*

### 5.7.8.1 Major Capabilities

Item	Capability	<u>ATNCNS/A TM-1 SARPs Ref.</u>	<u>ATNCNS/ATM-1 Package Support</u>
*mcNego	Negotiation of Compression Algorithm	5.7.3.5.3.3	M
*mcLocRef	Local Reference Header Compression	5.7.3.5	M
*mcCan	Local Reference Cancellation	5.7.3.5.5.5	O
*mcACA	ICAO Address Compression Algorithm ( <u>ACA</u> )	5.7.3.5	O
mcV42	V.42bis Compression	5.7.3.5	O

### 5.7.8.2 Call Setup and Clearing Procedures

Item	Function	<u>ATNCNS/A TM-1 SARPs Ref.</u>	<u>ATNCNS/ATM-1 Package Support</u>
csDynam	Dynamic Call Setup	5.7.3.5.3.3	M
csSys	Call Setup by Systems Management	5.7.3.5.3.3	O

csDef	Use of non-standard Default packet size	5.7. 3.5.3.3	M
csFast	Use of Fast Select <sup>1</sup>	5.7. 3.5.3.3	M
csOther	Use of other optional User Facilities and CCITT-specified DTE facilities	5.7. 3.5.3.3	O
csCol	Call Collision Resolution	5.7. 3.5.3.3	M

continued..

---

<sup>1</sup> Only required if supported by subnetwork

Call Setup and Clearing Procedures continued..

<b>Item</b>	<b>Function</b>	<b>ATNCNS/ATM-1 SARPs Ref.</b>	<b>ATNCNS/ATM-1 Package Support</b>
csAcp	Call Acceptance Procedures	5.7.3.5.3.6	M
csRej	Call rejection Procedures	5.7.3.5.3.7	M
csOrd	Order of _compression Procedures	5.7.3.5.3.5	M
csDiag	Use of call rejection diagnostic codes	5.7.3.5.3.7	M
csReset	Call Reset Procedures	5.7.3.5.11	M

### 5.7.8.3 Negotiation of Compression Algorithm

<b>Item</b>	<b>Function</b>	<b>ATNCNS/ATM-1 SARPs Ref.</b>	<b>ATNCNS/ATM-1 Package Support</b>
caMaxd	Indication of the maximum of directories entries in the call user Data	5.7.3.5.3.4.1	mcNego:O

### 5.7.8.4 Local Reference Header Compression

<b>Item</b>	<b>Function</b>	<b>ATNCNS/ATM-1 SARPs Ref.</b>	<b>ATNCNS/ATM-1 Package Support</b>
lrVC	Opening additional virtual circuits	5.7.3.5.5	M
*lrDirSize	Local Directory with more than 128 entries	5.7.3.5.4	O
lrProt	Identification of Network Layer Protocol	5.7.3.5.5.2	M
lrMod	Processing of SN-UnitData Requests	5.7.3.5.5.3	M
lrEst	Establishment of new local reference	5.7.3.5.5.4	M
lrTransfer	Transfer of modified ISO 8473 PDU	5.7.3.5.5.6	M
lrInitial	Initial DT PDU Compression	5.7.3.5.6.2	M
lrDerived	Derived DT PDU Compression	5.7.3.5.6.3	M
*lrError-s	Generation of Error PDU Compression	5.7.3.5.6.3	M

IrDiscard	Compression of discarded PDU encapsulated within Error PDU	5.7.3.5.6.4	IrError-s:M
IrCompTr	Transfer of compressed PDUs	5.7.3.5.6.4.1 1	M
IrReceived	Processing of received PDUs	5.7.3.5.7	M
IrUncomp-r	Processing of received uncompressed PDUs	5.7.3.5.7.2	M
LrReset	Purging directories entries on Reset	5.7.3.5.11	mcMocRef:M

continued..



Local Reference Header Compression continued..

<b>Item</b>	<b>Function</b>	<b><u>ATNCNS/A</u> <u>TM-1</u> <b>SARPs Ref.</b></b>	<b><u>ATNCNS/ATM-1</u> <b>Package Support</b></b>
IrUnMod-r	Processing of received unmodified PDUs	5.7.3.5.7.2.2	M
IrComp-r	Processing of received compressed data PDUs	5.7.3.5.7.3	M
IrError-r	Processing of received compressed Error PDUs	5.7.3.5.7.4	M
IrSNDCFerr-s	Generation of SNDCF Error Report	5.7.3.5.8	M
IrSNDCFerr-r	Processing of received SNDCF Error Report	5.7.3.5.7.5	M

### 5.7.8.5 Local Reference Cancellation

<b>Item</b>	<b>Function</b>	<b><u>ATNCNS/AT</u> <u>M-1</u> <b>SARPs</b> <b>Ref.</b></b>	<b><u>ATNCNS/ATM-1</u> <b>Package</b> <b>Support</b></b>
IrcMgmt	Management of local references	5.7.3.5.5.5	mcCan:M
IrcRequest-s	Generation of Cancellation Request PDU	5.7.3.5.9	mcCan:M
IrcRequest-r	Processing of incoming Cancellation Request PDU	5.7.3.5.9	mcCan:M
IrcReliable	Reliable transfer of Cancellation Request	5.7.3.5.9	mcCan:M
IrcAccept-s	Generation of Cancellation Accept PDU	5.7.3.5.9	mcCan:M
IrcAccept-r	Processing of incoming Cancellation Accept PDU	5.7.3.5.9	mcCan:M

### 5.7.8.6 ICAO Address Compression Algorithm

<b>Item</b>	<b>Function</b>	<b><u>ATNCNS/A</u> <u>TM-1</u> <b>SARPs</b> <b>Ref.</b></b>	<b><u>ATNCNS/ATM-1</u> <b>Package</b> <b>Support</b></b>
acOut	Compression of outgoing PDUs	5.7.6.1	mcACA:M
acIn	Decompression of incoming PDUs	5.7.6.1	mcACA:M
acAddr	Address Length Determination	5.7.6.2	mcACA:M
acComp	Compression of NSAP Addresses and address prefixes	5.7.6.5	mcACA:M

acDecomp	Decompression of NSAP Addresses and address prefixes	5.7.6.6	mcACA:M
----------	--	---------	---------

### 5.7.8.7 PDU Formats

#### 5.7.8.7.1 Call Request User Data

Item	Description	<u>ATNCNS/ATM-1 SARPs Ref.</u>	<u>ATNCNS/ATM-1 Package Support</u>
crLen	Length Indicator	5.7.3.5.3.4	M
crVersion	Version Indicator	5.7.3.5.3.4	M
crSNCR	Subnetwork Connection Reference (SNCR)	5.7.3.5.3.4	M
crComp	Offered Compression Techniques	5.7.3.5.3.4	M
crDir	Maximum Directory Size	5.7.3.5.3.4	M <sup>2</sup>
crAdd-s	Additional User Data on send	5.7.3.5.3.4	O
crAdd-r	Additional User Data on receive	5.7.3.5.3.4	O
MaxDir	Maximum number of directory entries supported	5.7.3.5.3.4	≥128

#### 5.7.8.7.2 Call Accept User Data

Item	Description	<u>ATNCNS/ATM-1 SARPs Ref.</u>	<u>ATNCNS/ATM-1 Package Support</u>
caComp	Offered Compression Techniques	5.7.3.5.3.4	mcNegot:M
caAdd-s	Additional User Data on send	5.7.3.5.3.4	mcNegot:O
caAdd-r	Additional User Data on receive	5.7.3.5.3.4	mcNegot:O

#### 5.7.8.7.3 Modified ISO/IECISO 8473 NPDU

Item	Description	<u>ATNCNS/ATM-1 SARPs Ref.</u>	<u>ATNCNS/ATM-1 Package Support</u>
npLocRef-s	Local Reference Option field	5.7.3.5.5.3	M

<sup>2</sup> Dynamically, this field is only generated if Local Reference Compression is offered.

**5.7.8.7.4 Compressed Initial PDU**

<b>Item</b>	<b>Description</b>	<b><u>ATNCNS/ATM-1</u> SARPs Ref.</b>	<b><u>ATNCNS/ATM-1</u> Package Support</b>
inType	PDU Type	5.7.3.5.6.2.2	M
inPri	Priority	5.7.3.5.6.2.3	M
inLifetime	Lifetime	5.7.3.5.6.2.4	M
inFlags	Flag Bits	5.7.3.5.6.2.5 to 5.7.3.5.6.2.9	M
inLocRef	Local Reference (1 octet)	5.7.3.5.6.2.9	M
inLocRef2	Local Reference (2 octet)	5.7.3.5.6.2.9	lrDirSize:M ^lrDirsize:X
inPDUId	PDU Identifier	5.7.3.5.6.2.10	M
inNSDU	User Data	Figure 5.7-4	M

**5.7.8.7.5 Compressed Derived PDU**

<b>Item</b>	<b>Description</b>	<b><u>ATNCNS/ATM-1</u> SARPs Ref.</b>	<b><u>ATNCNS/ATM-1</u> Package Support</b>
drType	PDU Type	5.7.3.5.6.3.2	M
drPri	Priority	5.7.3.5.6.3.3	M
drLifetime	Lifetime	5.7.3.5.6.3.4	M
drFlags	Flag Bits	5.7.3.5.6.3.5 to 5.7.3.5.6.3.8	M
drLocRef	Local Reference (1 octet)	5.7.3.5.6.2.8	M
drLocRef2	Local Reference (2 octet)	5.7.3.5.6.2.8	lDirSize:M ^lDirsize:X
drPDUId	PDU Identifier	5.7.3.5.6.3.9	M
drSegOff	Segment Offset	5.7.3.5.6.3.10	M
drTotalLen	Total Length	5.7.3.5.6.3.11	M
drNSDU	User Data	Figure 5.7-4	M

**5.7.8.7.6 Compressed Error PDU**

<b>Item</b>	<b>Description</b>	<b><u>ATNCNS/ATM-1 SARPs</u> Ref.</b>	<b><u>ATNCNS/ATM-1 Package</u> Support</b>
erType	PDU Type	5.7.3.5.6.4.2	M
erPri	Priority	5.7.3.5.6.4.3	M
erLifetime	Lifetime	5.7.3.5.6.4.4	M
erFlags	Flag Bits	5.7.3.5.6.4.5 to 5.7.3.5.6.4.8	M
erLocRef	Local Reference (1 octet)	5.7.3.5.6.2.8	M
erLocRef2	Local Reference (2 octet)	5.7.3.5.6.2.8	lDirSize:M ^lDirSize:X
erReason	Discard Reason	5.7.3.5.6.4.9	M
erNSDU	Compressed Header of discarded PDU	5.7.3.5.6.4	M

**5.7.8.7.7 SNDCF Error Report PDU**

<b>Item</b>	<b>Description</b>	<b><u>ATNCNS/ATM-1 SARPs</u> Ref.</b>	<b><u>ATNCNS/ATM-1 Package</u> Support</b>
sfType	PDU Type	5.7.3.5.8	M
sfReason	Discard Reason	5.7.3.5.8	M
sfLocRef	Local Reference	5.7.3.5.8	M
sfLocRef2	Local Reference (2 octet)	5.7.3.5.6.2.9	lDirSize:M ^lDirSize:X

**5.7.8.7.8 Cancellation Request**

<b>Item</b>	<b>Description</b>	<b><u>ATNCNS/ATM-1 SARPs</u> Ref.</b>	<b><u>ATNCNS/ATM-1 Package</u> Support</b>
cqType	PDU Type	5.7.3.5.9	mcCan:M
cqRef	Cancellation Reference	5.7.3.5.9	mcCan:M
cqLocRef	Local Reference	5.7.3.5.9	M

cqLocRef2	Local Reference (2 octet)	5.7.3.5.6.2.9	lDirSize:M ^lDirsize:X
-----------	---------------------------	---------------	---------------------------

#### 5.7.8.7.9 Cancellation Accept

<b>Item</b>	<b>Description</b>	<b><u>ATNCNS/ATM-1 SARPs</u> Ref.</b>	<b><u>ATNCNS/ATM-1 Package</u> Support</b>
ccType	PDU Type	5.7.3.5.9	mcCan:M
ccRef	Cancellation Reference	5.7.3.5.9	mcCan:M

## 5.8. ROUTING INFORMATION EXCHANGE PROTOCOL 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 Chapter 5.3.*

#### 5.8.1.2 Applicability of Requirements

5.8.1.2.1 All ATN Airborne Routers, with the exception of Airborne Routers implementing the procedures for the optional non-use of IDRPs, shall comply with the provisions contained in 5.5.8.2, 5.5.8.3, 5.5.8.3.2.2 to 5.5.8.3.2.5 inclusive, 5.5.8.3.2.8 to 5.5.8.3.2.11 inclusive, 5.5.8.3.3.2.1, 5.5.8.3.3.3 and the APRLs specified for an Airborne Router in 5.5.8.3.4.

5.8.1.2.2 Airborne Routers implementing the procedures for the optional non-use of IDRPs shall be compliant with 5.5.8.2.

5.8.1.2.3 All ATN Air/Ground Routers shall comply with the provisions contained in 5.5.8.2, 5.5.8.3, 5.5.8.3.2.2 to 5.5.8.3.2.11 inclusive, 5.5.8.3.3.2.2, 5.5.8.3.3.3 and the APRLs specified for an Air/Ground Router in 5.5.8.3.4.

5.8.1.2.4 All Ground/Ground Inter-Domain Routers shall comply with the provisions contained

in 5.5.8.2, 5.5.8.3.2.2 to 5.5.8.3.2.11 inclusive, 5.5.8.3.3.2.2, 5.5.8.3.3.3 and the APRLs specified for an Ground/Ground Router in 5.5.8.3.4.

### 5.8.2 End System to Intermediate System Routing Information Exchange Protocol (ES-IS) over Mobile Subnetworks

#### 5.8.2.1 General

##### ISO/IEC 9542 over Mobile Air-to-Ground Subnetwork

5.8.2.1.1 ATN Airborne and Air/Ground ATN 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 ATN Routers over each Mobile Subnetwork connection supporting an adjacency between them.

*Note.— The use of ISO/IEC 9542 Configuration Information over Mobile Subnetworks in support of Air/Ground route initiation is specified in Chapter 5.3.*

5.8.2.1.3 Route Redirection information shall not be exchanged between an ATN Air/Ground and an Airborne Router.

#### 5.8.2.2 ATN Protocol Requirements List - ISO/IEC 9542

5.8.2.2.1 In ATN Airborne and Air/Ground Routers, 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 –implementation shall conform to the APRL given in Table 5.8-1.–

*Note.— The requirements for ISO/IEC 9542 are provided in the form of a Protocol Requirements List.*



Table 5.5.8-1\_–ISO/IEC 9542 - Intermediate System

Item	Protocol Function	Clauses	ISO Status	ATN CNS/ATM-1 Package Support
CI	Is configuration information supported over the associated subnetwork?	ATN CNS/ATM-1 SARPs Ref.: 5.8.2-1	O	M
RI	Is redirection information supported over the associated subnetwork?	ATN CNS/ATM-1 SARPs Ref.: 5.8.2-1	O	OX
	<b>Are the following functions supported?</b>			
ErrP	Protocol Error Processing	6.13	M	M
HCsV	PDU Header Checksum Validation	6.12	M	M
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
FICf	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
	<b>Are the following PDUs Supported?</b>			
ESH-r	<r> End System Hello	7.1, 7.5	CI:M	O
ISH-<r>	<r> Intermediate System Hello	7.1, 7.6	CI:O	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

**Table 5.8-1 (continued...)**

	<b>Are the following PDU fields supported?</b>			
FxDt	<s> Fixed Part	7.2.1 <sub>2</sub> -7.2.7	M	M
	<r> Fixed Part	7.2.1 <sub>2</sub> -7.2.7	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
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
ESCT-s	<s> Suggested ES Configuration Timer	7.4.7	CI:O	O
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
	<b>Parameter Ranges</b>			
HTv	What range of values can be set for the Holding Time Field in transmitted PDUs ?	<u>ATN SARPs</u> <u>Ref.: 5.3.5.2.9</u>	M	M  from: 0 seconds to: 65535 seconds  with a tolerance of: 10%

CTv	If configuration information is supported, what range of values can be set for the Configuration Timer ?	<u>ATN SARPs</u> <u>Ref.: 5.3.5.2.5</u>	CI:M	M	<u>from: 0 seconds</u> <u>to: 65535 seconds</u> <u>with a tolerance</u> <u>of: 10%</u>
-----	--	--	------	---	---

*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 5.3.5.2.9. 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 IDRP is used over the Air/Ground link, the Configuration Timer may therefore be set to a large value so that the regular generation of ISH PDUs is inhibited.*

*Note 3. — 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 ~~optional~~ 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 5.8.3.4.

### 5.8.3.2 ATN Specific Features

#### 5.8.3.2.1 Purpose of ATN Specific Features

*Note . — ATN Airborne, Air-Ground and Ground-Ground Inter-Domain Routers shall implement the ATN Specific Features specified in the following subsections in order to support user requirements concerned with:*

- a) *Ensuring that application data passed over Aair/G-ground data links conforms with any national and/or ITU restrictions applicable to that Aair/G-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 Aair/G-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 distributed for the above changes that report negative changes (e.g. a downgrading of the classification of a route) are reported in a timely manner.*

#### 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 Ssecurity Ttag Sset defined in 5.6.2.2.6.*

5.8.3.2.2.5 When a route is available over more than one Aair/G-ground subnetwork type, then a separate Security Tag Sset shall be encoded into this field to identify each Aair/G-ground subnetwork that may support the route.

5.8.3.2.2.6 When an Aair/G-ground Ssubnetwork is restricted to carrying data of only certain traffic types, then the Security Tag Sset that identifies that Aair/G-ground Ssubnetwork 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 Security Tag Sets are also present, and when none of these Air/Ground Subnetwork Security Tag Sets indicates support of ATN Operational Communications traffic type ~~and~~ 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 Sset format defined for use with CLNP in Chapter 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 be always be two octets in length.

5.8.3.2.3.2.2 The first (lowest numbered) octet of the Security Tag shall define/indicate the Air/-Ground subnetwork type over which the route may be available according to Table 5.8-2.

**Table 5.5.8-2 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 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.

5.8.3.2.3.2.4 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.

5.8.3.2.3.2.5 The assignment of bits to Traffic Type shall be according to Table 5.8-3, where bit 0 is the low order bit:

**Table 5.5.8-3 Identification of Permissible Traffic Types**

Bit Number	Traffic Type
0	ATN Operational Communications - Air Traffic Service Communications
1	ATN Operational

Bit Number	Traffic Type
	Communications - Aeronautical Operational Control
2	ATN Administrative Communications
3	General Communications
4	ATN Systems Management Communications

5.8.3.2.3.2.6 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]** and the Security Tag shall be always be one octet in length. If a Security Tag with this Tag Set Name is received which is longer than one octet, then all octets after the first octet shall be ignored.

5.8.3.2.3.3.2 When this Security Tag Set is present, the Security Tag shall identify the ATSC Class(es) supported by the route.

5.8.3.2.3.3.3 The ATSC Class(es) supported shall be identified according to Table 5.8-4, where bit 0 is the low order bit, and setting a bit to one shall indicate that the corresponding ATSC Class is supported.

5.8.3.2.3.3.4 A bit set to zero shall indicate that the corresponding ATSC Class is not supported.

**Table 5.5.8-4 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 is:

- a) either advertised or received by an Air/Ground Router over an adjacency supported by one or more Air/-Gground Subnetworks, and
- b) contains a Security Path Attribute, and
- c) has the ATN Security Policy Identifier, as the Security Path Attribute's Security Registration Identifier, then;

The Security Path Attribute's Security Information shall be updated as follows:

- 1) An Air/-Gground Subnetwork Type Security Tag shall be added for each Air/G-ground Subnetwork supporting the adjacency and which is not already contained in the Security Information;
- 2) For each Air/-Gground 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/-Gground Subnetwork.

**5.8.3.2.4.2 The ATSC Class**

5.8.3.2.4.2.1 When a route is advertised to an adjacent BIS, 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/Gground 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/Gground 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 has
  - 1) has been originated locally (i.e. within the same Routing Domain), by a Router other than an Airborne Router, and
  - 2) if the route is to be advertised to an adjacent BIS over an adjacency supported by one or more subnetworks approved for ATSC Class traffic, then

an ATSC Class security tag shall be added to the route identifying the ATSC Class(es) supported by the Adjacency;

*Note. — 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/Gground data links are approved for ATSC use.*

- d) if the route
  - 1) has been received from another BIS, and
  - 2) the route 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 present in the route, 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) the route 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.

5.8.3.2.4.2.2 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.

5.8.3.2.4.2.3 An ATSC Class Security Tag shall not be present in a route's security information, if an Air/Ground Subnetwork Security Tag is also present indicating that the Air/Ground Subnetwork does not support ATSC Traffic.

#### 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 1.— ISO/IEC 10747 clause 7.16.2 permits a Loc-RIB that is identified by a RIB\_Attr 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 2.— The purpose of this statement is to permit, within the limitations imposed by ISO/IEC 10747 IDRP, 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\_Attr 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\_Attr 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.

**Table 5.8-5. ATN Routers and Route Aggregation**

Class	Name	Aggregation of Routes with identical NLRI	Policy Based Route Aggregation	Policy Based Route Information Reduction
1.	Static Router	N/A	N/A	N/A
2.	Level-1 Router	N/A	N/A	N/A
3.	Level-2 Router	N/A	N/A	N/A
4.	Ground-Ground Router	M	⊖	⊖
5.	Air/Ground Router (ground based)	M	⊖	⊖
6.	Airborne Router with IDRP	N/A	N/A	N/A
7.	Airborne Router without IDRP	N/A	N/A	N/A

**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 5.8.3.4.2 Table 5.8-5.

*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 their 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 rRoute’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 1.*—*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 2.*—*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 and 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, and their

5.8.3.2.6.3.2 Such routes shall be consequently being copied to the associated Adj-RIB-Output.

5.8.3.2.6.3.3 For each adjacent BIS, the resulting aggregated route shall be inserted into the associated Adj-RIB-Output.

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-Output. For each Adj-RIB-Output, 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-Output, 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 The aggregation rules for the security information field contained in security path attributes that include the ATN Security Registration Identifier shall be as follows:

- a) The aggregated security path attribute shall comprise each air-ground subnetwork security tag contained in the security path attribute of the component routes.
- b) When an air-ground subnetwork type security tag for the same air-ground subnetwork type occurs in more than one both component routes, then these shall be combined by a logical "OR" of the second octet of the Air/Ground Subnetwork type security tags. Only a single air-ground subnetwork type security tag for

each distinct air/ground subnetwork type shall be present in the aggregated route.

- c) When aggregating an ATSC Class Security Tag,
  - 1) If the NLRI of the component routes is not identical then, when an ATSC Class security tag occurs in all component routes the aggregated route shall contain an ATSC Class security tag. 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. All the other bits in this tag shall be set to zero. If at least one of the component routes does not contain an ATSC Class security tag is not present in any component route, then the aggregated route shall not contain an ATSC Class security tag.
  - 2) Otherwise, 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. 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 contain an ATSC Class security. -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.
- d) -When a Security Classification security tag occurs in all component routes, then the aggregated route shall contain a Security Classification security tag. This tag shall be set to the lowest classification from the classifications given to the aggregated route's component routes. 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 Routing Domain.*

*Note 1.— 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 with~~ 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 5.8-56, and shall be assumed to have the semantics given there:

**Table 5.5.8-5 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.

### 5.8.3.2.9 Network Layer Reachability Information (NLRI)

#### 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 IDRPs, 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 ATN Routers shall support the validation of BISPDU's using Authentication Type 1.

5.8.3.2.10.2 When an ATN Router initiates a BIS-BIS connection, it shall set the value of the Authentication Code in the OPEN PDU to 1, in order to indicate that the Validation field in the header of all BISPDU sent over the BIS-BIS connection will contain an unencrypted checksum.

5.8.3.2.10.3 When an authentication code of 1 is specified in the Authentication Code of the OPEN BISPDU 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 BISPDU's on such a connection.

*Note 1.*— The use of ISO/IEC 10747 type 2 authentication is under consideration for specification in future versions of these SARPs. Support of Authentication Codes 2 and 3 is outside of the scope of this specification and their use is a local matter.

5.8.3.2.10.4 The type 1 authentication code shall be generated according to the MD4 specification published in RFC 1320.

*Note 2.*— The interpretation of MD4 given in Annex B of ISO/IEC 10747 is open to ambiguous interpretation and may lead to interoperability problems.

*Note 3.*— 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.

### 5.8.3.2.11 Restrictions on Route Advertisement

5.8.3.2.11.1 A route shall not be advertised to a BIS in another RD when where:

- 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).

5.8.3.2.12.2 The semantics of the empty RIB\_Att shall be taken as implying that routes advertised under the empty RIB\_Att:

**Table 5.5.8-6 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 <u>BIS</u> per routing domain <del>Boundary Router</del> on board an aircraft, and hence, internal update is not applicable.
2.	Operation of <u>minRouteAdvertisementInterval</u> Timer	Note 2.— An <u>a</u> Aircraft is always an End Routing Domain, and hence will never re-advertise routes.
3.	Recognition of Next Hop Attribute	Note 3.— No <u>r</u> Requirement for <u>s</u> Support in <u>the</u> 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 <u>u</u> User <u>r</u> Requirements to control the distribution of routes to or from Mobile Systems. Implementation may also be problematic due to changing point of attachment to <u>the</u> Fixed –ATN.
7.	Support of Partial Source Routing	Note 7.— There are no known user requirements for partial source routing.

**5.8.3.2.12 RIB\_Att TT Support**

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.

- a) -have a classification of “Unclassified”,
- b) -have not passed over any mMobile sSubnetworks ,and
- c) -have been classed as ATSC Class H.

**5.8.3.2.13 Additional Update PDU Error Handling**

5.8.3.2.13.1 When an UPDATEupdate PDU is received with a Security Path Attribute containingwith 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 IDRPs 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.

### 5.8.3.3 Compliance with ISO/IEC 10747

#### 5.8.3.3.1 General

5.8.3.3.1.1 The IDRPs protocol exchange shall use the connectionless network service provided by ISO/IEC 8473<sub>2</sub> 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 5.8-67, for which support is optional.

*Note 17.— 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.*

*Note 28.— Representations are being made to ISO regarding possible over-specification in ISO/IEC 10747.*

##### 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~~ are specifically excluded from 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 APRLs

#### 5.8.3.4.1 General

5.8.3.4.1.1 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 IDR 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.*

## 5.8.3.4.2 ATN Specific Protocol Requirements

Index	Item	ATNCNS/ATM-1 SARPs Ref	G-G Router	A/G Router	Airborne Router
ATNIDRP1	Encoding and use of the Security Path Attribute	5.5.8.3.2.2, 5.5.8.3.2.3	M	M	M
ATNIDRP2	Additional procedures for non-use of the <b>minRouteAdvertisementInterval</b> Timer	5.8.3.2.5	M	M	-
ATNIDRP3	Support of « policy based route aggregation »	5.5.8.3.2.6.2	O	O	-
ATNIDRP4	Support of « policy based route information reduction »	5.5.8.3.2.6.5	O	O	-
ATNIDRP5	Support of aggregation of routes with identical NLRI using « true route aggregation »	5.5.8.3.2.6.3	O.1	O.1	-
ATNIDRP6 3	Support of <u>Route Aggregation of routes with identical NLRI using « route merging »</u> ion and Route Information Reduction	5.8.3.3.3	O.1	O.1	-
ATNIDRP7 4	Support of aggregation of security path attribute information fieldfor Route Merging Procedures	5.8.3.2.6	M	M	-

## 5.8.3.4.3 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 <sup>1</sup> 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 <u>ROUTE_SEPARATOR</u> attribute?	7.12.1	M	M	M	M
HOPS	Does this BIS support the <u>RD_HOP_COUNT</u> attribute?	7.12.13	M	M	M	M
PATH	Does this BIS support the <u>RD_PATH</u> attribute?	7.12.3	M	M	M	M

<sup>1</sup> The interpretation of this Item 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 version of the SARPs CNS/ATM-1 Package](#) and hence it is not reasonable to require mandatory support for this requirement.

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
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
ERROR	Does this BIS handle error handling for IDRPs?	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

**5.8.3.4.4 IDRPs 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?	7.17.3.1	M	M	M	O
RTORG	Does this BIS support the MinRDOriationInterval 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	M

**5.8.3.4.5 IDRPs 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 BISPDU's correctly?	7.14	M	M	M	M
INCONS	Does this BIS detect inconsistent routing information?	7.15.1	M	M	M	M

#### 5.8.3.4.6 IDRPs 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	ATNIDRP 3^ATNID RP5:M	ATNIDRP 3^ATNID RP5: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

#### 5.8.3.4.7 IDRPs Receive

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
RCV	Does the BIS process incoming BISPDU's and respond correctly to error conditions?	7.14, 7.20	M	M	M	M
OSIZE	Does this BIS accept incoming OPEN PDU's whose size in octets is between MinBISPDULength and 3000?	6.2,7.20	M	M	M	M
MXPDU	Does the BIS accept incoming UPDATE, IDRPs ERROR and RIB REFRESH PDU's 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

#### 5.8.3.4.8 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.

**5.8.3.4.9 IDRPs 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 NPDUs-derived Distinguishing Attributes from an ISO/IEC 8473 NPDUs?	8.2	M	M	M	M
MATCH	Does the BIS correctly match the NPDUs-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

**5.8.3.4.10 IDRPs Receive Process**

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
RCV	Does the BIS process incoming BISPDU 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, IDRП ERROR and RIB REFRESH PDUs whose size in octets is between minBISPDULength and maxBISPDULength?	6.2,7.20	M	M	M	M
-------	---	----------	---	---	---	---

#### 5.8.3.4.11 IDRП 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

#### 5.8.3.4.12 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:O X ^IDRPAG: O	O
NHSN	Does the BIS support generation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	O	IDRPAG:O X ^IDRPAG: 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:O X ^IDRPAG: O	O
TDLY	Does the BIS support generation of the TRANSIT DELAY attribute?	7.12.8	O	O	IDRPAG:O X ^IDRPAG: O	O
RERR	Does the BIS support generation of the RESIDUAL ERROR attribute?	7.12.9	O	O	IDRPAG:O X ^IDRPAG: O	O

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
EXP	Does the BIS support generation of the EXPENSE attribute?	7.12.10	O	O	IDRPAG:O X ^IDRPAG: O	O
LQOSG	Does the BIS support generation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	OX	OX	OX
HREC	Does the BIS support generation of the HIERARCHICAL RECORDING attribute?	7.12.12	O	OX	OX	OX
SECG	Does the BIS support generation of the SECURITY attribute?	7.12.14	O	M	M	M
PRTY	Does the BIS support generation of the PRIORITY attribute?	7.12.16	O	O	IDRPAG:O X ^IDRPAG: O	O

**IDRPAG:** if Air/Ground adjacency **then** true **else** false

**5.8.3.4.13 Propagating Well-Known Discretionary Attributes**

<b>Item</b>	<b>Description</b>	<b>ISO/IEC 10747 Ref.</b>	<b>ISO Status</b>	<b>G-G Router</b>	<b>A/G Router</b>	<b>Airborne Router</b>
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:O X ^IDRPAG: O	-
NHNSP	Does the BIS support propagation of the NEXT_HOP attribute to advertise SNPs?	7.12.4	O	O	IDRPAG:O X ^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:O X ^IDRPAG: M	-
TDLYP	Does the BIS support propagation of the TRANSIT DELAY attribute?	7.12.8	O	O	IDRPAG:O X ^IDRPAG: O	-
RERRP	Does the BIS support propagation of the RESIDUAL ERROR attribute?	7.12.9	O	O	IDRPAG:O X ^IDRPAG: O	-
EXPP	Does the BIS support propagation of the EXPENSE attribute?	7.12.10	O	O	IDRPAG:O X ^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:O X ^IDRPAG: O	-

**5.8.3.4.14 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
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

**5.8.3.4.15 IDRP Timer**

Item	Description	ISO/IEC 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
Ta	KeepAlive time	7.6.5	M	M	M	M
Tr	Retransmission (tr) timer	7.6.5	M	M	M	M
Tmr	maxRIBIntegrityCheck timer	7.10.2	M	M	M	M
Tma	MinRouteAdvertisement timer	7.17.3.1	M	M	M	O
Trd	MinRDOriationInterval timer	7.17.3.2	M	M	M	M
Tcw	closeWaitDelay timer	7.6.4	M	M	M	M

## 5.9. SYSTEMS MANAGEMENT PROVISIONS

### 5.9.1 Introduction

5.9.1.1 **Recommendation.**—*ATN managed resources should be grouped into Management Domains in order to assign responsibility for control of the resources. An organization should assign an administrative authority to establish and maintain the respective management authorities of each of its Management Domains, and to manage the transfer of control of resources from one Management Domain to another.*

*Note 1.*—*Given the current lack of well identified operational requirements regarding Systems Management for the ATN Internet, the definition and implementation of a global ATN Systems Management solution will be specified in future of this SARP. cannot be achieved within the timeframe foreseen for the CNS/ATM-1 Package SARPs. Currently Consequently within this timeframe:*

- a) *No exchange of Systems Management information is will be required between routers of different Administrative Domains.*
- b) *No exchange of Systems Management information is will be required by means of a management protocol over the Air/G-ground links. This does not preclude the exchange of routing information, by means of routing information exchange protocols.*
- c) *The exchange of Systems Management information within an Administrative Domain is considered a local matter and can be achieved by any means deemed appropriate.*

*Note 2.*—*Nevertheless, it is desirable to implement provisions which enable the exchange of Systems Management information across Administrative Domain boundaries as long as it does not compromise the safety and regularity of flight.*