ATNP/WG2-IP/132
18 May 1995

INFORMATION PAPER

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Washington 15.5.95-19.5.95

CNS/ATM-1 Package Operational and Technical Requirements

Presented By Forrest Colliver

Prepared by Tony Whyman, Forrest Colliver, and Jean-Michel Crenais

SUMMARY

This document proposes an architectural and technical profile for the Aeronautical Telecommunication Network (ATN) Internet SARPs for CNS/ATM-1 Package, including proposed text for Guidance Material and SARPs for CNS/ATM-1 Package, and providing background material setting the contribution in context. The approach proposed for CNdS/ATM-1 Package is intended to allow implementation of ATN SARPs-compliant aircraft and ground-based equipment requiring a minimum of new technology, while retaining essential features of the ATN architecture, such as dynamic recognition of mobile routers.

TABLE OF CONTENTS

1. Introduction

1.1 Scope

This document includes proposed text for Guidance Material and SARPs for CNS/ATM-1 Package and also provides background material setting the contribution in context.

1.2 Purpose of Document

The Paris CISEC Meeting (10-11/4/95) did not make a definite conclusion as to how to satisfy the Routing Policy requirements raised at the preceding Toulouse Meeting of WG1 (20-24/3/95). However, it was agreed that the approach known to that meeting as “Option #2” was technically the best. This working paper elaborates option #2 to the point where a complete specification is now available for inclusion in the draft SARPs and Guidance Material. This working paper also includes material on Route Initiation, the optional non-use of IDRP over air/ground subnetworks, and the ATN Internet Architecture for CNS/ATM-1 Package. This is so that the full impact of “option #2” is clearly understood.

1.3 Overview of Paper

This paper proposes an architectural profile for CNS/ATM Package 1. This profile is intended to allow construction of aircraft and ground-based Aeronautical Telecommunication Network (ATN) equipment implementations requiring a minimum of new technology, while retaining essential features of the ATN architecture, such as dynamic recognition of mobile routers.

This architecture is designed to allow implementations of airborne and ground-based ATN Boundary Intermediate Systems (BISs) and End-Systems (ESs) to proceed immediately, using currently available technology, in order to support ATN validation and pre-operational trials. This profile is especially suited for early trials implementations of both airborne and ground-based routers (i.e. BISs) and ESs, and forms the basis for the European contribution to the North Atlantic Automatic Dependent Surveillance (ADS) trials.

1.4 References

	Reference	Title
1	ATNP/1/WP-4	ATN Manual (2nd Edition)
2	Draft 1.0 ATN SARPs and Guidance Material	Draft ATN Standards and Recommended Practices (SARPs) and Guidance Material (GM): Version 0.0

1.5 Conformance to Applicable Documents

The profile is in general compatible with requirements detailed in the ATN Manual (Reference 1) and in Draft 1.0 of the ATN SARPs and Guidance Material (Reference 2).

This paper focuses on the elements of the ATN provisions (i.e. the provisions documented in the ATN Manual) that are of particular significance in the context of CNS/ATM-1 Package, i.e. those elements directly related to the services provided to CNS/ATM-1

Package ESs and services related to the establishment of dynamic routing information exchange with mobile BISs where the implementation of IDRP in those mobile BISs is optional. As such, this paper details certain extensions to or constraints upon the ATN provisions as documented in the ATN Manual. Elements of ATN provisions not explicitly noted or discussed in this paper are assumed, generally, to be implemented in the CNS/ATM-1 Package in the manner indicated in the ATN Manual.

2. Background

2.1 ATN Manual Status

The 2nd edition of the ATN Manual was approved by the SICAS Panel at its fifth meeting in November 1993. At the first meeting of the newly constituted ATN Panel in June 1994, it was then agreed to implement the ATN in a progressive fashion as a series of packages; the first - Package 1 - was intended to be a proper subset of the functionality of the ATN Manual. The aim of Package 1 was to provide a set of early ATM Applications, supported by an ATN Internet, that would provide early operational benefits, and could be implemented and validated by the 2nd ATN Panel Meeting at the end of 1996.

2.2 Package 1 Application Support Objectives

ATNP/WG1 considered the above decision and, as a result, specified the *CNS/ATM-1 Package* comprising six Operational ATM Applications. These are:

1. Automated Data Surveillance (ADS)
2. Controller to Pilot Data Link Communications (CPDLC)
3. Flight Information Services (FIS)
4. ATS Inter-facility Data Communications (AIDC)
5. Context Management (CM)
6. Electronic Messaging (MHS)

It then became the responsibility of ATNP/WG3 to develop the SARPs for these applications. ATNP/WG2 was also tasked with the development of SARPs for an ATN Internet that would support these applications.

2.3 Package 1 Implementation Objectives

2.3.1 Explicitly-Stated Objectives

A common set of explicitly-stated goals and associated statements of goal objectives, evolving from a comparative analysis of the various proposals made within the ATN Panel and its Working Groups during the past year, can be summarized as follows:

Simplified Avionics Implementations	Reduction of the complexity of air/ground ATN protocol operations, in order to improve the odds of successful near-term avionics implementations in limited capability software environments;
Optimization of Routing Updates	Reduction of the scale of required ground-based routing information exchanges to support the ATN mobility management techniques without crippling the underlying ground-based infrastructure;

Utility of Off-the-Shelf Software	Alignment of ATN standards with OSI industrial software practices, to enhance the possibility of non-adapted commercial solutions;
Minimal Obsolescence of Procurements	Minimization of deviation from particular ATN routing policy solutions, on which procurements in several States and Organizations have been respectively based.

2.3.2 Implicit Objectives

An additional set of implicit objectives derived from experts' discussions during the same period may be summarized as follows:

a) Package 1 validation must be completed without a slip in schedule, i.e. prior to the end of 1996, in order to support timely SARPs approval and in order to support existing implementation plans.

b) Air Traffic Management benefits (i.e. services supporting the safety and regularity of flight) must be possible using a Package 1 ATN Internet implementation.

c) Airline Operational Control applications must be possible using a Package 1 ATN Internet implementation, with no loss of existing capabilities (i.e. no loss of capabilities provided in the current ACARS environment).

d) Traffic related to the safety and regularity of flight must be treated in a manner so as to attain the greatest possible chance of successful delivery, while other traffic *may* be subjected to restrictive policies (i.e. related to subnetwork access control or economic considerations) that reduce the chances of successful delivery.

2.4 Attempts made at Optimisation

ATNP/WG2 was therefore tasked with developing SARPs for the ATN Internet, derived from the ATN Manual, that could both be validated by ATNP/2 and would support the CNS/ATM-1 Package applications identified by WG1. Attention was concentrated on the problem of developing certifiable airborne routers and hence developing a minimal implementation specification for air-ground routing.

Given consideration of the application support and implementation objectives presented above, an initial proposal was made by European states for the optional non-use of IDRP over air-ground data links (San Diego - October 1995). The aim was to minimise the validation and certification work on airborne routers, with a strategy that did not preclude evolutionary enhancement to the original specification, and which only imposed acceptable near term limitations. There was some initial reluctance to progress down this route, but this approach was eventually agreed at the Toulouse WG2 Meeting (March 1995).

During the same timeframe, proposals were also made to use addressing strategies to signal and manage ITU and User Requirements i.e. to restrict access to some air-ground data links to only certain classes of traffic. This is instead of the ATN Manual specification which makes use of security mechanisms in both IDRP and CLNP. The justification for the change was that greater use could be made of existing software if the security mechanisms were not used, and that it would avoid a risk that the ground ATN could be overloaded with routing updates. There was again reluctance to accept this simplification, due to perceived limitations in the addressing approach in respect of future extensibility. However, the proposal was also accepted at the Toulouse WG2 Meeting.

Route selection based on dynamically indicated QoS Requirements has also been a simplification issue. The ATN Manual required the support of dynamic QoS Maintenance in the sense that an application could specify whether a route was chosen on the basis of lowest cost or lowest transit delay. Concern has been raised in WG2 that this is predicated on the assumption that it is possible to dynamically assigned network resources such that there will exist routes with lower transit delay provided at a higher cost. It has been doubted whether, in a connectionless internet, it is possible to assign resources in this way. The recent Paris WG2/CISEC meeting came to the conclusion that dynamic QoS Maintenance is a research issue that cannot be realistically validated by ATNP/2 and hence should not be included in Package 1.

2.5 Routing Policy Requirements Raised in Toulouse

The ATNP/WG1 meeting that immediately followed the concurrent WG2 and WG3 meetings in Toulouse (March 1995), reviewed and endorsed requirements raised initially by airline representatives, that were concerned with applications specifying routing policy requirements on a per application basis. In particular, the application requirement is to be able to specify which air-ground data links may be used to convey that application's data and, when more than one is specified, to be able to specify an order of preference. Requirements similar to these had been discussed previously, but not believed to be essential for the ATN. However, the airlines made clear that in order to justify the investment in ATN technology, backwards compatibility with the functionality of existing data links had to be provided. This is an existing function provided by ACARS and must be present in the ATN.

2.6 Consideration by WG2

As these “new requirements” only came to the surface after WG2 had met in Toulouse, it has not been possible to discuss them in WG2 itself. They have, however, been discussed in the Paris CISEC Meeting (10-11/4/95), where it was agreed that there were two issues that needed to be discussed and agreed before these requirements could be met. The first was how the policy requirements were expressed in the CLNP Header. The second was how routing information supporting the meeting of these requirements was distributed by IDRP.

2.6.1 Conveying Routing Policy Requirements in the CLNP Header

Two options were discussed:

1. The user's requirements are expressed in the Security Parameter (essentially expanding upon the specification in the ATN Manual)

2. The user's requirements are expressed through addressing conventions i.e. each End System has many alias addresses, each one of which corresponds to a different Routing Policy (expanding on the addressing convention approach agreed in Toulouse).

There was initially strong support for the use of an addressing mechanism. The reason is a desire to use commercially available L1 and L2 Routers within ATN Ground Routing Domains. It is understood that no such router currently supports the security parameter, and will discard packets that contain such a parameter. It was also recognised that End Systems also rarely support this parameter.

However, the meeting also recognised that use of the addressing conventions may cause problems with commercial systems, if they are unable to cope with the many alias addresses that would now be involved. This consideration affects where in the address the information is encoded.

Furthermore, if the routing policy requirements are encoded in the first part of the NSAP Address (the eleventh octet is proposed), and which is necessary if policy information is also to be distributed by IDRP by means of an addressing convention, then this also has an impact on L1 Routers. This is because each encoded routing policy results in a different alias area address at the intra-domain routing level. Although the ISO 10589 routing information exchange protocol used within ATN Routing Domains, permits up to 254 possible alias areas addresses, most implementations are understood to have a pragmatic limitation of 3. An alternative encoding in the System Identifier portion of the address avoids this problem, but does constrain how the supporting information is distributed by IDRP.

Since the meeting, vendors have been contacted and it is now believed that commercial intra-domain routers, with up-to-date software, can be configured to be transparent to the CLNP Security Parameter. This therefore appears to be a workable approach and has been adopted by this paper.

2.6.2 Distribution of Route Information by IDRP

In respect of how information in support of these routing policy requirements can be distributed by IDRP, it was recognised by the Paris Meeting that in the early Package 1 timeframe, the problem is restricted to Ground based Routers. This is because for airborne routers, support IDRP is optional and initial implementations are expected to satisfy the user's requirements directly by routing the user's data over the appropriate air-ground subnetwork. In order to give avionics vendors a clear specification by July 1995 for such early implementations, it is only necessary to agree the mechanism for identifying the user's routing policy requirements in the CLNP header.

In support of ground to air routing, three options emerged as candidates:

1. An Addressing convention in a route's NLRI to indicate which policies are satisfied, supported by information on the actual subnetworks traversed, by additional conventions defined for the RD_Path. This is an extension of the addressing convention adopted at the Toulouse WG2.

2. The use of the IDRP Security Path Attribute to report the air-ground subnetwork through which a route is available, but under a single "Security Registration Identifier" for the ATN as a whole. Information on Security Types supported and air-ground subnetworks traversed would then be encoded in the value field of the Security Path Attribute. Appropriate FIB information may then be synthesised from this information e.g. to construct a separate FIB for each user policy request.

3. The use of the IDRP Security Path Attribute to report the air-ground subnetwork that a route passes over, and the definition of a "Security Registration Identifier" for each combination of Security Type and air-ground subnetwork. Appropriate FIB information may then be synthesised from this information e.g. to construct a separate FIB for each user policy request. This is an extension of the ATN Manual approach.

There was considerable discussion on these options. Option #1 was recognised as resulting in an explosive growth in the amount of addressing information handled and in large numbers of alias addresses. This last point may make it unworkable with COTS routers. Option #3 similarly resulted in an exposive growth in the numbers of routes and routing updates that a router would have to handle, raising questions over whether it would be workable in practice. Neither option was extensible.

Option #2 was recognised as being the technically best option, albeit in need of validation. It did not result in a large increase in addressing or routing information and, indeed, would reduce the routing overhead compared with the ATN Manual. The solution was also extensible and would extend naturally to permit aircraft to be transit routing domains, or to allow routing policy requirements to be expressed for any ATN subnetwork, including those on the ground. However, in order to work successfully, the solution requires that a defect is fixed in IDRP, concerning the relationship between the Security Path Attribute and the Hold Down Timer - the minRouteAdvertisementInterval. This is a general defect that affects all uses of the Security Path Attribute.

In the current ISO specification, if there is a change in the value of the Security Path Attribute, then the route cannot be re-advertised until the Hold Down timer expires. However, if the security information changed, for example, in order to report a change in the protection offered, then the lack of timely advertisement might then cause data to be sent on a route that was no longer appropriate for the effective Security Policy. The proposed use of the Security Parameter under option #2 has essentially the same problem. If the air-ground connectivity of a route changes then this fact does not become known downstream until the expiry of this timer, thus resulting in either a route which is sub-optimal from the user's point of view, or one over which the data cannot actually traverse and will be discarded at some point on the route.

The fix is simple enough. It is to add a further condition to the existing list of exceptions for the Hold Down Timer. Such a defect resolution will probably be accepted by ISO, and can be an ATN specific exception if not. However, the need to correct the standard was used as an argument against this option. What was quite clear from the discussion is that the other options are really ways round the Hold Down Timer problem, each with consequential disadvantages. Either "fix it or fool it" seem to be the only available options, with "fix it" being the only one free of downside implications.

This was how the meeting concluded on this issue. A consensus was not reached, and it was clear that "Option #2" could not be accepted without a detailed specification being available. Only then could the risks of adopting it be clearly assessed. Such a specification is the remainder of this paper.

3. CNS/ATM-1 Package ATN Internet Operational Requirements

3.1 Operational Requirements Statement

In order to evaluate the proposals presented above, a list of the known requirements to be placed on the ATN Internet to support the noted applications is presented in this section.

3.1.1 Protocol Service Requirements

There are only two known protocol service requirements for the ATN Internet:

1. The ATN Internet must provide the ISO 8072 Transport Service to the Transport Service User (TS-User) by means of the ISO Connection-Mode Transport Protocol (COTP), as specified in ISO 8073. In this context, the TS-User is either a user application using the Transport Service directly, or an upper-layer protocol stack acting on behalf of a user application.

2. The ATN Internet must provide the ISO 8348 Network Service to the Network Service User (NS-User) by means of the ISO Connectionless-Mode Network Protocol (CLNP), as specified in ISO 8473 and its addenda. In this context, the NS-User is the ISO 8073 COTP.

3.1.2 General Design Requirements

1. Transit Delay shall be specified as a design parameter, for each application.

2. Residual Error Rate shall be specified as a design parameter, for each application. All ATN applications will have the same value.

3. Service Loss Reporting shall be specified as a design parameter, for each application. All ATN applications will have the same value.

4. Availability shall be specified as a design parameter, for each application.

5. Service Restoration Time shall be specified as a design parameter, for each application.

3.1.3 Message Sequencing Requirements

Sequentially ordered message delivery capability is required (e.g., where succeeding message delivery is dependent upon the successful delivery of preceding messages).

3.1.4 Communication Service Termination Requirements

1. The communications service shall provide an orderly termination of service upon indication by the application (e.g. if messages have been passed to the communications service and then a termination of service is requested, the preceding messages are to be delivered as per normal operations before the service is terminated). It is noted that the ATN Upper Layer Architecture will provide this service.

2. Upon failure of orderly termination an indication shall be provided to the application. It is noted that the ATN Upper Layer Architecture will provide this service.

3.1.5 Priority Requirements

1. Applications shall use priority in accordance with ICAO ANNEX 10, and in accordance with ITU radio regulations.

2. There shall be a one-to-one relationship between application specified priority and any communication service priorities (e.g. transport layer, network layer, etc.).

3. Note that for the CNS/ATM-1 package, application specified priority will not necessarily invoke processing within the transport service entity (e.g. will not result in the reordering of transport entity queues), but will be used internally by the network layer to reorder transmission queues. Transport priority is only of significance between the end-users of the transport service; thus, there is no requirement in Package 1 that transport priority be used by the transport protocol layer for internal processing purposes or for internal resource allocation (connection and buffer management) purposes although this is not precluded

3.1.6 Routing Policy Requirements

A summary of the routing policy requirements set as defined in the March 1995 WG1 Flimsy 3 is included below:

1. Applications shall be able to set routing policies based on a) QOS requests, and on b) Traffic Type identification.

2. QOS policies shall be applied on a “best effort” basis. In the terminology of the Working Group 2 experts, this means that “Weak QOS” is required. Traffic Type policies shall be applied on a “must be enforced” basis. In the terminology of the Working Group 2 experts, this means that “Strong Traffic Typing” is required.

3. Policy information must be indicated by the application to the communication service and will be conveyed on end-to-end basis in the CLNP NPDU header.

4. Airlines have a further requirement that, for any air/ground subnetwork that supports multiple simultaneous router-to-router connections (e.g. as is possible via the Satellite data link), a mechanism must be defined whereby the correct ground-based air/ground router is selected based on local aircraft policy decisions.

3.1.6.1 QOS Policy Requirements

Applications shall be able to specify that message traffic be routed to achieve one of the following QOS policies:

1. Minimal Transit Delay.

2. Minimal Cost.

3. No Policy on QOS (i.e. “don’t care”).

3.1.6.2 Traffic Type Policy Requirements

Applications shall be able to specify that message traffic be routed to achieve one of the following Traffic Type policies:

1. ATN Operational Communications

   a) Air Traffic Service Communications (ATSC)

      i) No Traffic Type Policy Preference.

      ii) Traffic only follows ATSC route(s).

      iii) Route Traffic using an ordered preference of Mode S first, then VHF Data Link, then Satellite Data Link, then HF Data Link.

   b) Aeronautical Operational Control (AOC)

      i) No Traffic Type Policy Preference.

      ii) Route Traffic only via Gatelink.

      iii) Route Traffic only via VHF Data Link.

      iv) Route Traffic only via Satellite Data Link.

      v) Route Traffic only via HF Data Link.

      vi) Route Traffic only via Mode S Data Link.

      vii) Route Traffic using an ordered preference of Gatelink first, then VHF Data Link.

      viii) Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then Satellite.

      ix) Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then HF Data Link, then Satellite Data Link.

2. ATN Administrative Communications

3. General Communications

4. ATN Systems Management Communications

Note 1: Airlines have a requirement that the mechanism defined for support of ATN policy routing be capable of allowing the inclusion of up to 20 traffic types for AOC traffic.

Note 2: The definition of further traffic types for ATSC is not precluded.

3.1.6.3 Derived Routing Policy Requirements

Based on the operational requirements statement provided above, the following derived operational requirements are believed to exist:

a) To support ATN Internet access control (i.e. traffic type) policy-based routing decisions, it is required to identify a subnetwork use policy by means of a field located in, and conveyed on an end-to-end basis via the CLNP header, based on application supplied information.

b) To maintain an ATN Internet routing information database in each boundary intermediate system router in support of the required policy-based routing decisions, it is necessary to provide each router with information stating via which subnetworks and through which routing domains a given route passes.

c) It is required to enforce access control policies in a “strong” manner, i.e. failure to locate a route satisfying a given policy results in the discard of traffic seeking enforcement of that policy.

d) The lack of specific access control policies (i.e. the “don’t care” traffic type options noted in WG1 Flimsy 3) results in routing decisions based on other aspects, such as connectivity or quality of service. This is regarded as “weak” or best-effort routing.

   It is important to note that any traffic for which delivery is considered to be essential, such as traffic related to the safety and regularity of flight, should be routed on a “weak” basis, to ensure delivery via any existing route.

3.1.7 Message Duplication Prevention Requirement

A message delivered to the communications service shall not be delivered more than once to its peer entity.

3.1.8 QOS Monitoring Requirement

No QOS monitoring is required to be provided in the CNS/ATM-1 package. Inclusion of this capability in future CNS/ATM packages is not precluded.

3.2 Implications of Operational Requirements

3.2.1 Protocol Service Requirements

The noted requirements regarding protocol service pose no particular implications.

3.2.2 General Design Requirements

The noted requirements regarding general network design pose no particular implications.

3.2.3 Message Sequencing Requirements

Working Group 3 discussions have lead to the requirement for connection-mode transport service only, in the CNS/ATM-1 package time frame. However, IATA requirements for per message policy enforcement require functionality best supported by a connectionless transport service.

Note: Implementation of per message policy enforcement in a connection oriented environment will require extensive non-standard modifications to the ISO connection oriented transport protocol.

3.2.4 Communication Service Termination Requirements

Orderly service termination is not provided by the transport layer. This function must be provided as part of the upper layer architecture or application design. There are no transport layer implications of this requirement in CNS/ATM-1 Package.

3.2.5 Priority Requirements

Priority in the transport layer affects transport operations only. Network priority, while related to transport priority for consistency, only affects the operation of the network components (e.g., CLNP routers and end-systems). Further, network and transport priority are semantically independent. Package 1 intermediate systems will be required to forward data consistent with CLNP priority. Every NPDU associated with a given transport connection must have the same priority.

3.2.6 Routing Policy Requirements

Routing policy, as stated above, requires weak QoS and strong traffic type routing.

3.2.6.1 QOS Policy Requirements

End-to-end QoS decisions require that ground IDRP routers exchange route information including QoS. Thus, IDRP route information exchange including QoS poses certain risks to ongoing validation efforts given current validation and operational implementation schedules.

3.2.6.2 Traffic Type Policy Requirements

End-to-end policy enforcement requires that all ground IDRP routers receive route information including traffic type, make routing decisions, and populate local FIBs accordingly. This requires that IDRP update PDUs contain traffic type route information. Without this traffic type information, there is no guarantee of end-to-end policy enforcement and ultimate air/ground subnetwork choice based upon stated traffic type.

If suitable network design provisions are not available, then traffic typing must be conveyed in the CLNP NPDU and acted upon by every router in the communications path to facilitate end-to-end traffic selection and policy enforcement. To communicate traffic type on an end-to-end basis, ground IDRP decisions must be made on this information and knowledge of this information must be conveyed amongst IDRP ground routers. For this reason, guaranteed end-to-end policy decisions may not be feasible in the package 1 time frame.

Note: If traffic type processing is only performed by the “air/ground” routers (routers directly connected to an air/ground subnetwork), there is no guarantee that routers one hop or more removed from a ground based air/ground router will make the correct decision to enable proper subnetwork selection by a ground router directly attached to an air/ground subnetwork. For example, if router A can choose between two forwarding destinations, *router B and router C, and router B supports VHF access only and router C supports satellite access only and both are in contact with the aircraft, router A may choose to forward the packet to router B even if the local policy on router B states satellite preference. Thus, without complete ground knowledge of policy, end to end decisions cannot be made and without end to end decisions packets may be forwarded to routers implementing strong policy (i.e., traffic may be dropped) or packets may be forwarded to routers implementing weak policy but only having access to a less preferred subnetwork. The same scenario applies to the aircraft; however, it is assumed that package 1 aircraft consist of one BIS only which in turn has access to available air/ground subnetworks.*

3.2.7 Message Duplication Prevention Requirement

No implication exists given the use of ISO connection oriented transport protocol.

3.2.8 QOS Monitoring Requirement

QoS “rankings” are only known by the routers on an a priori basis in the CNS/ATM-1 package architecture.

4. Overview of the CNS/ATM-1 ATN Architecture

4.1 Technical Objectives for CNS/ATM-1 Package

In developing the architecture for CNS/ATM-1 Package, certain objectives have been identified by the ICAO ATN Panel Working Groups as being particularly important. These objectives are listed in Table 1, along with comments providing insight into either the rationale behind the objective, or the objective itself.

Table 1: Objectives for Package 1

	Description	Comments
1	Conformance to Key ATN Manual and ATN Draft SARPs Provisions	This objective is essential to support ATN validation. The CNS/ATM-1 Package proposal varies from ATN Manual provisions in only two areas: a) A new requirement is postulated for routing initiation with mobiles not implementing the ISO 10747 Inter-Domain Routing Protocol (IDRP) while maintaining compliance with those that do implement IDRP; and, b) Non-conformance with certain mandatory protocol requirements list elements is proposed when necessary to support the goals of practicality and timeliness while having minimal effect on the utility of validation results.
2	Dynamic Mobile Routing Support	As this is an essential element of the value-added aspect of the ATN, CNS/ATM-1 Package proposes a routing structure which allows dynamic discovery of mobile (i.e. aircraft) routers and routing domains. This is done in a manner which avoids the need for immediate implementation of IDRP in aircraft systems, but retains compatibility with future mobile systems hosting IDRP.
3	Ground Support for Distribution of Mobile Routes	While the loss of detailed knowledge of available ground routes by aircraft systems implied in the previous objective is deemed acceptable, the ground topology is more complex in general, and would benefit from early introduction of IDRP. Thus, this proposal for the CNS/ATM-1 Package includes the implementation of IDRP in ground BISs for distribution of both air/ground and ground-based routes to peer BISs.
4	Practical for Near-Term Implementations in Ground Systems and on-board Aircraft	It is viewed as essential to create a CNS/ATM-1 Package profile which can be implemented in the near-term in both aircraft and ground environments. While this does not necessarily mean that all existing aircraft and ground-based hardware/software systems are capable of hosting the CNS/ATM-1 Package , it is essential to take practical and transition considerations into account to ensure that a significant aircraft and ground equipage can occur.
5	Reasonable Efficiency of use of Mobile Data Links	This CNS/ATM-1 Package architecture includes the use of the ATN mobile SNDCF with local reference capability required, but with other forms of data compression remaining optional. This approach avoids the case where the combination of low air-ground throughput and uncompressed data flows create a situation that cannot realistically be used for ATN validation.
6	Support for Validation Activities	This is an essential goal of the CNS/ATM-1 Package and its successors.
7	Support for Trials Activities	Since it essential to gain practical experience in order to complement certain more formal validation exercises, this approach for CNS/ATM-1 Package is tailored to support near-term trials activities.

4.2 Assumptions and Constraints

Use of the CNS/ATM-1 Package architecture requires an understanding of the underlying assumptions and constraints. The following sub-sections summarise these key assumptions and any associated constraints. It is important to note:

- that the assumptions are necessary in order to satisfy all objectives in Table 1; and,
- that none of the resulting constraints interfere with the attainment of the objectives in Table 1.

4.2.1 Evolutionary Path for the Communication Infrastructure

The primary assumption in CNS/ATM-1 Package is that the first ATN implementations can comprise systems that, while not meeting all requirements originally envisaged in the ATN Manual, are clearly on a evolutionary path to full compliance with ATN Manual regarding the ATN communication infrastructure.

4.2.2 IDRP (ISO 10747)

The use of IDRP in the context of CNS/ATM-1 Package differs in several ways from the provisions of the ATN Manual.

4.2.2.1 Optional Non-Use of IDRP in the Air/Ground Environment

Implementation of IDRP in CNS/ATM-1 Package over air/ground subnetworks is optional. It is recognised that, initially, CNS/ATM-1 Package mobile BISs will not implement IDRP. Consequently mobile BISs shall be required to comply with certain requirements related to the exchange of addressing information between the mobile and ground based Iss.

If a mobile BIS does not support IDRP, then that BIS must then implement a network entity relying upon the ISO 9542 End-System to Intermediate System (ES-IS) protocol Intermediate System Hello (ISH) Protocol Data Unit (PDU) exchange to dynamically manage mobile connectivity to the ATN internet. This is accomplished in a way that ensures compatibility with ground BISs conforming fully to ATN standards and that ensures compatibility when operating in the same environment with other aircraft operating fully-compliant ATN network entities.

4.2.2.2 IDRP Use in the Ground Environment

The protocol requirements for the IDRP implementation (ground-ground) in CNS/ATM-1 Package are equivalent in general to those specified in the ATN Manual. Certain extensions to these originally envisaged requirements are necessary, to support the introduction of routes learned and/or inferred from the air/ground environment into the normal route dissemination process to used by IDRP in the ground environment.

4.2.3 Routing and Addressing

The assumptions and constraints related to routing and addressing may generally be derived from the approach to implementation of IDRP in CNS/ATM-1 Package.

4.2.3.1 Identification of IDRP Operation

The presence or absence of IDRP in an airborne CNS/ATM-1 Package implementation is assumed to be inferred from the Network Selector (N-SEL) component of the Network

Entity Title (NET). The N-SEL value **<0x00>** indicates a network entity containing IDRP, while the N-SEL value **<0xfe>** indicates a network entity that does not contain IDRP.

4.2.3.2 Policy Decision-Making

Since IDRP is not required to be operated over the air/ground path, it may not always be possible to communicate routing information between the aircraft domain and its attached ground domain for support of policy decision making. This, in combination with the reduced capability of the specified IDRP implementation, means that in general, routing information utility is constrained to the knowledge and distribution of connectivity information. Local policies can be applied within each ground BIS based on connectivity and domain identity (derived from NET and address prefix information), however.

4.2.3.3 Aircraft Domain Knowledge of Ground Domain Reachability

Since IDRP is not required to be operated over the air/ground path, it may not always be possible to communicate information to the aircraft domain regarding ground domain reachability. An aircraft CNS/ATM-1 Package BIS thus assumes that upon establishing connectivity to any ground ATN BIS, any ATN destination domain is, in principle, reachable.

4.2.3.4 Identification of Routing Domains

Since IDRP is not required to be operated over the air/ground path, there is no mechanism available to explicitly convey aircraft Routing Domain Identifiers to ground ATN BISs. The identity of the airborne domain is thus inferred from the first 11 octets of the airborne IS NET. For this reason, all CNS/ATM-1 Package aircraft end-systems reachable through a particular aircraft BIS (i.e. through a particular air/ground subnetwork point of attachment) must share this prefix.

4.2.4 COTP (ISO 8073)

In general, operation of the ISO Connection-Mode Transport Protocol (COTP) within CNS/ATM-1 Package conforms to the ATN Manual. Any deviation from the provisions of the ATN Manual are clearly visible in the respective transport layer PRLs.

4.2.5 CLNP (ISO 8473)

In general, operation of the ISO 8473 Connectionless-Mode Network Protocol (CLNP) within CNS/ATM-1 Package Package 1 conforms to the ATN Manual. Any deviation from the provisions of the ATN Manual are clearly visible in the respective network layer PRLs.

It should be noted that in the implementation of the CLNP Forwarding Information Base (FIB) in an air/ground BIS, appropriate means must be provided to link FIB entry management to mobile connectivity information acquisition (i.e. upon receipt of an ISH from the ground BIS).

4.2.6 ES-IS (ISO 9542)

Operation of the ISO 9542 ES-IS Protocol between the airborne BIS and the ground BIS to support routing initiation within CNS/ATM-1 Package conforms to the ATN Manual.

It should be noted that in the absence of IDRP operation over air/ground paths, ES-IS timers must be set in a manner to emulate the IDRP “update” and “keep-alive” functions.

4.2.7 ATN Mobile SNDCF

Operation of the ATN Mobile SNDCF within CNS/ATM-1 Package conforms to requirements established in the ATN Manual.

CNS/ATM-1 Package air/ground BISs:

a) must support the local reference compression mechanism (with or without local reference cancellation) as defined for use in the ATN mobile SNDCF (refer to Section A10.6.4.3.2 of the ATN Manual); and,

b) may optionally support one or more of the stream compression mechanisms defined for use in the ATN mobile SNDCF (refer to Section A10.6.4.3.2 of the ATN Manual), but must, as a minimum, support negotiation of the use or non-use of these compression mechanisms.

4.3 Use of G/G Subnetworks

Use of Ground/Ground Subnetworks by CNS/ATM-1 Package systems conforms to requirements established in the ATN Manual.

4.4 The CNS/ATM-1 Package Ground ATN Internet

In a protocol and service sense, the ground ATN Internet conforms to requirements established in the ATN Manual. The main aspect of interest concening the CNS/ATM-1 Package ground ATN Internet is that, due to the assumption of connectivity required for mobile systems interconnected via air/ground BISs opting not to operate IDRP on the air/ground subnetwork, a relatively higher degree of service availability is required. This can typically be accomplished through means of network design, and through assumptions applied within the application operational environment.

4.5 System Implementation Requirements

The CNS/ATM-1 Package communication architecture is based on the following requirements:

a) Ground ESs must support the ISO 8073 Connection-Mode Transport Protocol (COTP) Class 4, the ISO 8473 Connectionless-Mode Network Protocol (CLNP) and any Subnetwork Dependent Convergence Facilities (SNDCFs) required to access chosen ground subnetworks (e.g. Ethernet LAN, X.25, etc.).

b) Ground BISs must support the ISO 8473 CLNP, the ISO 9542 ES-IS protocol (to support routing initiation over the air-ground link), the ISO 10747 Inter-Domain Routing Protocol (IDRP) (ground-ground) , the ATN Mobile SNDCF, and any SNDCFs required to access chosen ground subnetworks (e.g. Ethernet LAN, X.25, etc.).

c) Airborne ESs must support the ISO 8073 COTP Class 4, the ISO 8473 CLNP and any SNDCFs required to access chosen airborne subnetworks (e.g. ARINC 429 Williamsburg).

d) Airborne BISs must support the ISO 8473 CLNP protocol, a minimal implementation of ISO 9542 ES-IS protocol (to support routing initiation over the air-ground link, a minimal implementation of the ATN mobile SNDCF and any SNDCFs required to access chosen airborne subnetworks (e.g. ARINC 429 Williamsburg).

e) All systems must support the ATN NSAP Addressing Plan (as specified in Appendix 7 of the ATN Manual.

5. System Requirements

5.1 End Systems

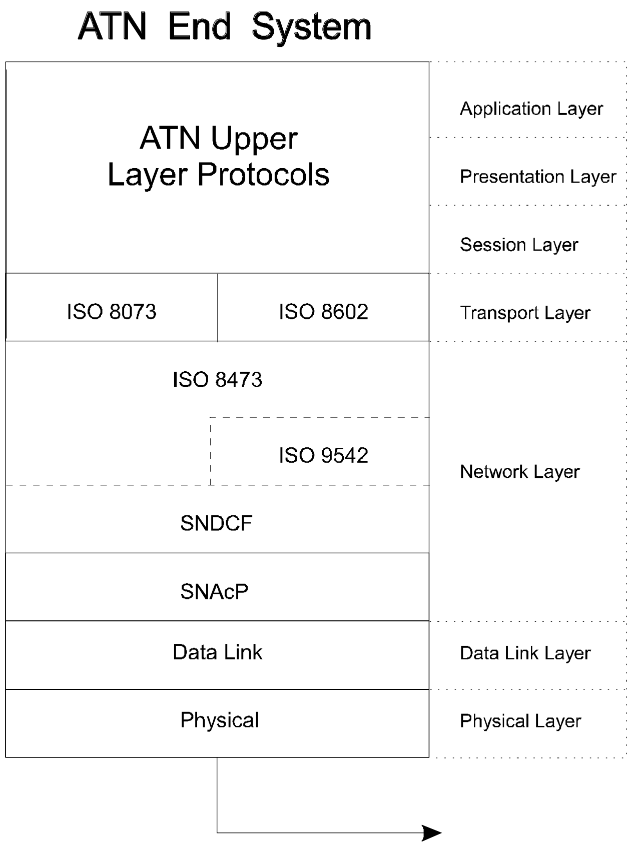

Figure 1 ATN End System Architecture

The architecture of an ATN End System is illustrated in Figure 1. An ATN End System shall include:

1. The Application and Upper Layer protocols specified by the CNS/ATM Application(s) supported by that End System.

2. The Connection Mode Transport Protocol Class 4 specified in ISO/IEC 8073:1992 and profiled in section 6, if the Applications that the ATN End System supports require the Connection Mode Transport Service.

3. The Connectionless Mode Transport Protocol specified in ISO/IEC 8602:1989 and profiled in section 6, if the Applications that the ATN End System supports require the Connectionless Mode Transport Service.

4. The Connectionless Network Protocol specified in ISO/IEC 8473:1993 and profiled for an End System in section 7.1.

Recommendation: An ATN End System should also the End System to Intermediate System Protocol specified in ISO/IEC 9542:1988 and profiled in ISO/IEC ISP 10608.

Note: the SNDCF, subnetwork dependent, data link and physical layer protocols are a local matter dependent upon the subnetwork(s) to which the ATN End System is attached.

5.2 ATN Routers

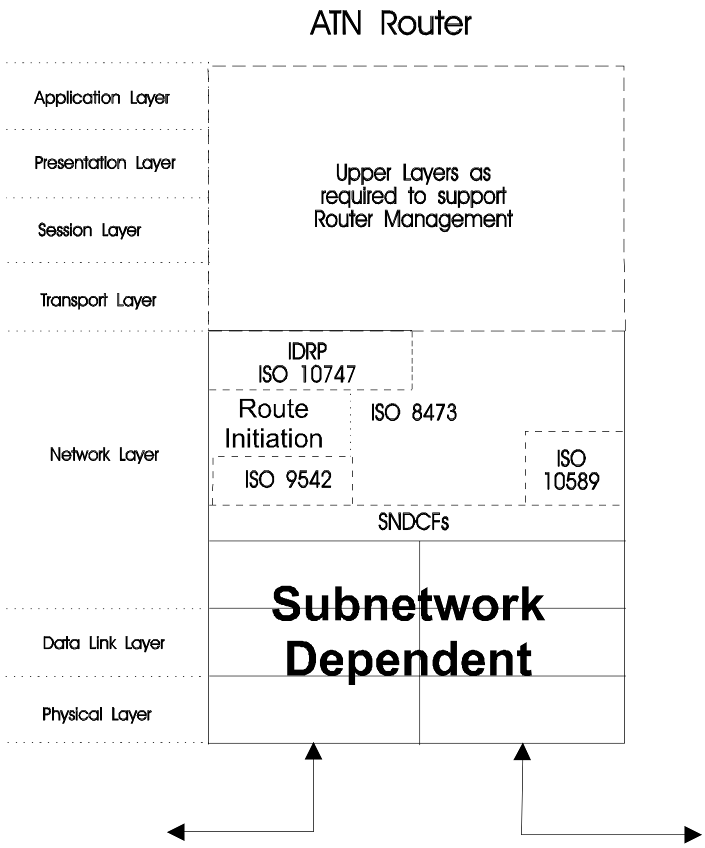

Figure 2 Generic ATN Router Architecture

The generic architecture for an ATN Router is illustrated in Figure 2. The basic components of an ATN Router are:

- ISO/IEC 10747 (Inter Domain Routing Protocol),
- ISO/IEC 8473 (Protocol for Connectionless Network Layer Service),
- ISO/IEC 10589 (IS-IS Routing Protocol),
- ISO 9542 (ES-IS Routing Protocol),
- Route Initiation Procedures in support of Inter-Domain Routing
- Subnetwork Dependent Convergence Facilities (SNDCFs) for attached subnetworks
- subnetwork access functions, data link and physical layer protocols required to support the attached subnetworks.
- Systems Management Functions

Note 1: the choice of subnetworks types supported is, except for routers connected to air-ground data links, a local matter.

Note 2. For CNS/ATM-1 Package Systems Management Functions and upper layer support are also a local matter.

The following classes of ATN Router are recognised by this specification:

	Name	**Routing Protocols Supported**
1.	Static Router	ISO 9542 (optional)
2.	Level 1 Router	ISO 9542 (optional) ISO/IEC 10589 Level 1 only
3.	Level 2 Router	ISO 9542 (optional) ISO/IEC 10589 Level 1 and Level 2
4.	Ground-Ground Router	ISO 9542 (optional) ISO/IEC 10589 (optional) ISO/IEC 10747
5.	Ground-Air Router (ground based)	ISO 9542 ISO/IEC 10589 (optional) ISO/IEC 10747 Route Initiation Procedures
6.	Air-Ground Routers (airborne)	ISO 9542 ISO/IEC 10747 Route Initiation Procedures
7.	Air-Ground Routers (airborne) without IDRP	ISO 9542 Route Initiation Procedures

Note 1. Classes 1, 2 and 3 are only for use within an ATN Routing Domain and are 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 part of Router Class 6 and 7 are concerned with the interconnection of avionics to the airborne router and are the subject of aeronautical industry standards.

All ATN Inter-Domain Routers (i.e. Router Classes 4 to 7 inclusive) shall support the CLNP Options Security Parameter encoded according to 0, 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.

Recommendation: All ATN Routers should implement the CLNP Congestion Notification function.

In support of Systems Management, ATN Routers shall also support the features and facilities of an ATN End System.

5.2.1 Ground/Ground Routers

An ATN Air/Ground Router (Class 4) shall include the following components:

1. The Inter-Domain Routing Protocol specified in ISO/IEC 10747:1993 and profiled in section 7.1.2.3.1 for a Ground Router for information exchange with another Ground Router.

2. The Connectionless Network Protocol specified in ISO/IEC 8473:1993 and profiled in section 7.1 for an Intermediate System.

Note 1. Route initiation procedures for establishing communication with an adjacent Ground Router or Ground-Air Router are a local matter.

Note 2. An ATN Ground Router may also exchange routing information with Class 1, 2 or 3 ATN Routers within its local Routing Domain. This exchange of routing information and the communication of routing information between the intra-domain routing function and the inter-domain routing function are a local matter.

5.2.2 Ground-Air Routers

An ATN Ground-Air Router (Class 5) shall include the following components:

1. The Inter-Domain Routing Protocol specified in ISO/IEC 10747:1993 and profiled in section 7.1.2.3.1 for an Air-Ground Router for information exchange with an Airborne Router.

2. The Inter-Domain Routing Protocol specified in ISO/IEC 10747:1993 and profiled in section 7.1.2.3.1 for a Ground Router for information exchange with another Ground Router.

3. The Connectionless Network Protocol specified in ISO/IEC 8473:1993 and profiled in section 7.1 for an Intermediate System.

4. the End System to Intermediate System Protocol specified in ISO/IEC 9542:1988 and profiled in section 7.2.3 for use in support of route initiation over air-ground data links.

5. The Route Initiation procedures specified in section 8 for use over an air-ground data link when IDRP is to be used to distribute routing information, and also when IDRP is not supported. The procedures used shall depend upon whether the airborne router is of Class 6 or Class 7 and are negotiated as specified in section 8.

Note 1. Route initiation procedures for establishing communication with an adjacent Ground Router or Ground-Air Router are a local matter.

Note 2. An ATN Ground-Air Router may also exchange routing information with Class 1, 2 or 3 ATN Routers within its local Routing Domain. This exchange of routing information and the communication of routing information between the intra-domain routing function and the inter-domain routing function are a local matter.

5.2.3 Air-Ground Routers

An ATN Air-Ground Router (Class 6) shall include the following components:

1. The Inter-Domain Routing Protocol specified in ISO/IEC 10747:1993 and profiled in section 7.1.2.3.1 for an airborne router acting as an End Routing Domain.

2. The Connectionless Network Protocol specified in ISO/IEC 8473:1993 and profiled in section 7.1 for an Intermediate System.

3. the End System to Intermediate System Protocol specified in ISO/IEC 9542:1988 and profiled in section 7.2.3 for use in support of route initiation over air-ground data links.

4. The Route Initiation procedures specified in section 8 for use over an air-ground data link when IDRP is to be used to distribute routing information.

An ATN Airborne Router without IDRP (Class 7) shall include the following components:

1. The Connectionless Network Protocol specified in ISO/IEC 8473:1993 and profiled in section 7.1 for an Intermediate System.

2. the End System to Intermediate System Protocol specified in ISO/IEC 9542:1988 and profiled in section 7.2.3 for use in support of route initiation over air-ground data links.

3. The Route Initiation procedures specified in section 8 for use over an air-ground data link when IDRP is not supported.

6. Transport Layer Protocol Requirements

6.1 Introduction

This section specifies the transport protocol requirements for **CNS/ATM-1 Package** Systems.

6.2 ATN Connection-Mode Transport Protocol

6.2.1 Major Capabilities

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

Index	Class	References	ISO Status	CNS/ATM-1 Package Support
C0	Class 0	14.2	O.1	O
C1	Class 1	14.4	C0:O	O
C2	Class 2	14.2	O.1	O
C3	Class 3	14.3	C2:O	O
C4	Class 4 operation over CONS	14.3	C2:O	O
C4L	Class 4 operation over CLNS	14.3	C2:O	M

6.2.2 Specific ATN Recommendations

Note.- The ATN recommendations for use of optional ISO functionality are presented below. If the recommendation is accepted, the indexed predicate indicates the specific implementation features required to support the recommendation. The index of indices indicates where the features for each recommendation are found.

Does the implementation support the ATN recommendation on:

Index	Recommendation	ATN Status	CNS/ATM-1 Package Support
ATN1	Initiating CR TPDU?	O.2	M
ATN2	Responding to CR TPDU?	O.2	M
ATN3	Extended TPDU Numbering	O	O
ATN4	Acceptance of Non-use of Checksum?	O	MO
ATN5	Use of Concatenation?	O	O
ATN6	Use of Selective Acknowledgement?	O	O
ATN7	Use of Request of Acknowledgment?	O	O
ATN8	Reduction of Credit Window	O	O
ATN9	ER TPDU Transmission?	O	O
ATN10	Use of Called TSAP-ID Parameter in CR TPDU?	M	M
ATN11	Use of Calling TSAP-ID Parameter in CR TPDU?	M	M
ATN12	Use of TPDU Size Parameter in CR TPDU?	O	O
ATN13	Use of the Additional Option Selection Parameter in CR TPDU?	M	M
ATN14	Use of the Priority Parameter in CR TPDU?	O	O
ATN15	Use of the Acknowledgment Timer Parameter in CR TPDU?	O	O
ATN16	Use of Preferred Maximum TPDU Size Parameter in CR TPDU?	O	O
ATN17	Use of Inactivity Time Parameter in CR TPDU?	O	O
ATN18	Use of Called TSAP-ID Parameter in CC TPDU?	M	M
ATN19	Use of Calling TSAP-ID Parameter in CC TPDU?	M	M
ATN20	Use of TPDU Size Parameter in CC TPDU?	O	O

ATN10:: *Note.- This option is recommended to support congestion control.*

Index	Recommendation	ATN Status	CNS/ATM-1 Package Support

ATN21	Use of the Additional Option Selection Parameter in CC TPDU?	O	M
ATN22	Use of the Priority Parameter in CC TPDU?	O	O
ATN23	Use of the Acknowledgment Timer Parameter in CC TPDU?	O	O
ATN24	Use of Preferred Maximum TPDU Size Parameter in CC TPDU?	O	O
ATN25	Use of Inactivity Time Parameter in CC TPDU?	O	O
ATN26	1024 octets as the minimum preferred maximum TPDU size in a CR TPDU?	O	O
ATN27	1024 octets as the minimum preferred maximum TPDU size in a CC TPDU?	O	O
ATN28	1024 octets as the largest value of the maximum TPDU size parameter in a CR TPDU with preferred class 4?	O	O
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?	O	O
ATN30	Congestion Avoidance Measures?	O	O
ATN31	Quality of Service Mapping?	O	O
ATN32	Are existing Timer Settings configurable?	O	O

6.2.3 Initiator/Responder Capability for Protocol Classes 0-4

The ATN transport protocol shall implement at least one of the features marked "O.2" in the table.

Index		References	ISO Status	CNS/ATM-1 Package Support
IR1	Initiating CR TPDU	14.5 a)	O.2	ATN1:M
IR2	Responding to CR TPDU	14.5 a)	O.2	ATN2:M

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

6.2.4 Supported Functions

6.2.4.1 Supported Functions for Class 4 (C4 OR C4L::).

6.2.4.1.1 Mandatory Functions for Class 4.

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

Index	Function	References	ISO Status	CNS/ATM-1 Package Support
T4F1	TPDU transfer	6.2	M	M
T4F2	Segmenting	6.3	M	M
T4F3	Reassembling	6.3	M	M
T4F4	Separation	6.4	M	M
T4F5	Connection establishment	6.5	M	M
T4F6	Connection refusal	6.6	M	M
T4F7	Data TPDU numbering (normal)	6.10	M	M
T4F8	Retention and acknowledgement of TPDUs (AK)	6.13.4.1	M	M
T4F9	Explicit flow control	6.16	M	M
T4F10	Checksum	6.17	M	M
T4F11	Frozen references	6.18	M	M
T4F12	Retransmission on time-out	6.19	M	M
T4F13	Resequencing	6.20	M	M
T4F14	Inactivity control	6.21	M	M

6.2.4.1.2 Mandatory Functions for Operation over Connectionless Network Service.

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

Index	Function	References	ISO Status	CNS/ATM-1 Package Support
T4F23	Transmission over CLNS	6.1.2	M	M
T4F24	Normal release when operating over CLNS (explicit)	6.7.2	M	M
T4F25	Association of TPDUs with transport connections when operating over CLNS	6.9.2	M	M
T4F26	Expedited data transfer when operating over CLNS (Network normal)	6.11.2	M	M
T4F27	Treatment of protocol errors when operating over CLNS	6.22.2	M	M

6.2.4.1.3 ISO 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..

Index	Feature	References	ISO Status	CNS/ATM-1 Package Support
T4F28	Data TPDU numbering (extended)	6.10	O	ATN3:M
T4F29	Non-use of checksum	6.17	O	ATN4:M
T4F30	Concatenation	6.4	O	ATN5:M
T4F31	Retention and acknowledgement of TPDUs Use of selective acknowledgement	6.13.4.3	O	ATN6:M
T4F32	Retention and acknowledgement of TPDUs Use of request acknowledgement	6.13.4.2	O	ATN7:M

note - T4F31 and T4F32:: See T4F8

T4F30:: The transport layer shall not concatenate TPDUs from TCs with different transport priorities.

T4F31:: *Note.- The use of selective acknowledgement is recommended for conservation of bandwidth by preventing retransmission of correctly received out-of-sequence TPDUs.*

T4F32:: *Note.- The use of request of acknowledgement is recommended to reduce AK traffic.*

6.2.5 Supported TPDUs

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

Index	TPDUs		References	ISO Status	CNS/ATM-1 Package Support
ST1	CR	supported on transmission	13.1	IR1:M	ATN1:M
ST2	CR	supported on receipt	13.1	IR2:M	ATN2:M
ST3	CC	supported on transmission	13.1	IR2:M	ATN2:M
ST4	CC	supported on receipt	13.1	IR1:M	ATN1:M
ST5	DR	supported on transmission	13.1	IR2:M	ATN2:M
ST6	DR	supported on receipt	13.1	IR1:M	ATN1: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

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

Index	Class	References	ISO Status	CNS/ATN/1 Support
SER4L	Class 4 over CLNS	6.22.2	O	ATN9:M

6.2.6 Supported Parameters of Issued TPDUs

6.2.6.1 Parameter Values for CR TPDU (C4L::).

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

Index		Reference
ICR1	Bits 8 to 7 shall be set to zero	13.3.4 g)

If the preferred class in the CR is 2,3 or 4

Index		Reference	ISO Status	CNS/ATM-1 Package Support
ICR2	Is class 0 always offered as an alternative class?	14.4	O	X

6.2.6.2 Supported Parameters for Class 4 TPDUs (C4L::).

6.2.6.2.1 Optional Parameters for a Connection Request TPDU.

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

Index	Supported parameters	References	ISO Status	CNS/ATM-1 Package Support
I4CR7	Called TSAP-ID	13.3.4 a)	O	ATN10:M
I4CR8	Calling TSAP-ID	13.3.4 a)	O	ATN11:M
I4CR9	TPDU size	13.3.4 b)	O	ATN12:M
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	ATN13: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	ATN14:M
I4CR16	Transit delay	13.3.4 p)	O	O
I4CR17	Acknowledgement time	13.3.4 j)	O	ATN15:M
I4CR18	Preferred maximum TPDU size	13.3.4 c)	O	ATN16:M
I4CR19	Inactivity timer	13.3.4 r)	O	ATN17:M

I4CR9:: **Recommendation.-** *The transport layer should propose a TPDU size of 1024 octets or more.*

The transport layer should use the TPDU size parameter rather than the preferred maximum TPDU size parameter.

6.2.6.2.2 Optional Parameters for a Connection Confirm TPDU.

ISO Note. - The following parameters are optional if a CC TPDU is issued in class 4:

Index	Supported parameters	References	ISO Status	CNS/ATM-1 Package Support
I4CC6	Called TSAP-ID	13.4.4	O	ATN18:M
I4CC7	Calling TSAP-ID	13.4.4	O	ATN19:M
I4CC8	TPDU size	13.4.4	O	ATN20:M
I4CC9	Protection parameters	13.4.4	O	O
I4CC10	Additional option selection	13.4.4	O	ATN21: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	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.*

6.2.6.2.3 Optional Parameter for a Disconnect Request TPDU.

Index	Supported parameter	References	ISO Status	CNS/ATM-1 Package Support
I4DR4	Additional information	13.5.4 a)	O	O

6.2.6.2.4 Mandatory Parameter for a Data TPDU.

ISO Note.- The following parameter is mandatory in a DT TPDU if request of acknowledgement has been selected.

Index	Supported parameter	References	ISO Status	CNS/ATM-1 Package Support
I4DT4	ROA	13.7.3 b)	T4F32:M	T4F32:M

6.2.6.2.5 Optional Parameter for an Acknowledgement TPDU.

ISO Note.- An AK TPDU containing flow control information will be transmitted if an AK TPDU is received under the conditions specified in ISO 8073 12.2.3.9. The following parameter is mandatory if an AK TPDU is issued in Class 4.

Index	Supported parameter	References	ISO Status	CNS/ATM-1 Package Support
I4AK4	Flow control confirmation	13.9.4 c)	O	O

6.2.6.2.6 Use of the Subsequence Number Parameter in the Acknowledgement TPDU.

ISO Note.- If an implementation can reduce credit and does so in the manner outlined in ISO 8073 12.2.3.8.2 then subsequence number in AK is mandatory.

Index	Supported parameters	References	ISO Status	CNS/ATM-1 Package Support
I4AK5	Subsequence number	13.9.4. b)	O	ATN8:M

6.2.6.2.7 Use of the Selective Acknowledgement Parameter in the Acknowledgement TPDU.

ISO Note.- The following parameter is optional in an AK TPDU if selective acknowledgement has been negotiated.

Index	Supported parameter	References	ISO Status	CNS/ATM-1 Package Support
I4AK6	Selective acknowledgement parameters	13.9.4. d)	T4F31:O	T4F31:O

6.2.6.2.8 Optional Parameters for an Error TPDU.

Index	Supported parameter	References	ISO Status	CNS/ATM-1 Package Support
I4ER3	Invalid TPDU	13.12.4 a)	O	O

6.2.7 Supported Parameters for Received TPDUs

Note.- ISO 8073 requires implementations to be capable of receiving and processing all possible parameters for all possible TPDUs, depending upon the class and optional functions implemented.

TPDUs in Class 4 (C4L::).

ISO Note.- If use of checksum has been selected then it is mandatory to process a checksum parameter in the following TPDUs:

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

Index	TPDU	References	ISO Status	CNS/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

6.2.8 User Data in Issued TPDUs

Class 4 (C4 or C4L::).

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

Index	User Data	References	ISO Status	CNS/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

6.2.9 User Data in Received TPDUs

The transport layer shall be able to receive the following:

Index	User Data	References	ISO Status	CNS/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

6.2.10 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 8073 transport protocol.

6.2.10.1 Class Negotiation - Initiator

Index	Feature	References	CNS/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	References	ISO Allowed values	ATN Supported values	CNS/ATM-1 Package Supported Values
NAC5	Class 4 over CLNS	6.5.5 j)	None	None	None

NAC5:: *Note.- The class cannot be negotiated since Class 4 is the only class allowed over CLNS.*

6.2.10.2 Class Negotiation - Responder

Index	Preferred class	References	ISO Allowed responses	CNS/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.

6.2.10.3 TPDU Size Negotiation.

Index	TPDU size	References	ISO Status	CNS/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	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
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.*

TS3, TS4:: **Recommendation.-** *1024 octets is the recommended minimum maximum-TPDU size.*

Index	TPDU size	References	Allowed Values	CNS/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	One of 128, 256, 512, 1024, 2048, 4096, 8192

TS3, TS4, T4S1, T4S2:: **Recommendation.-** *The supported TPDU size of 1024 octets is recommended to support efficient transmission of anticipated application data exchanges.*

TS3, TS4, T4S1, T4S2:: *Note.- A given transport implementation may support a smaller TPDU size.*

6.2.10.4 Use of Extended Format.

Index	Extended format	References	ISO Allowed Values	CNS/ATM-1 Package Supported Values
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:: **Recommendation.-** *Implementations of the ATN transport layer should propose use of normal format in the CR TPDU.*

NEF3:: *Note.- Because the increased TPDU size resulting from use of extended data TPDU numbering may be more inefficient, this option should be used on a TC only when absolutely required.*

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

6.2.10.5 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	References	ISO Status	CNS/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 TPDUs.*

6.2.10.6 Non-use of Checksum (C4L and T4F29::).

Index	Non-use of checksum	References	ISO Allowed Values	CNS/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.- A transport layer is able to propose either use or non-use of checksum in a CR TPDU.*

NUC2:: *Note.- 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.*

NUC2:: **Recommendation.--** *The transport layer should accept non-use of checksum when proposed in a CR TPDU.*

6.2.10.7 Use of Selective Acknowledgement

Index	Selective Acknowledgement	References	ISO Status	CNS/ATM-1 Package Support
USA1	Is use of selective acknowledgement proposed in CR TPDUs ?	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

6.2.10.8 Use of Request Acknowledgement

Index	Request of Acknowledgement	References	ISO Status	CNS/ATM-1 Package Support
ROA1	Is use of request of acknowledgement proposed in CR TPDUs ?	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

6.2.11 Error Handling

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

6.2.11.1 Action on Receipt of a Protocol Error.

Index	Item	References	Values	
			ISO Allowed	CNS/ATM-1 Package Supported
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.*

6.2.11.2 Actions on receipt of an invalid or undefined parameter in a CR TPDU.

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

Index	Event	References	ISO Status	CNS/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	Reference	Value	
			ISO Allowed	CNS/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 Errors

RR7:: *Note.- The choice of action (Ignore, Protocol error) is an implementation choice and may depend on the type of error encountered.*

6.2.11.3 Actions on receipt of an invalid or undefined parameter in a TPDU other than a CR TPDU.

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

Index	Event	References	ISO Status	CNS/ATM-1 Package Support
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

6.2.12 Class 4 Timers and Protocol Parameters

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

Index		References	ISO Status	CNS/ATM-1 Package Support
TA1	T1 (Local Retransmission)	12.2.1.1.4	M	M
TA2	N (Maximum Transmission)	12.2.1	M	M
TA3	I_L (Inactivity Time)	12.2.1.1.7	M	M
TA4	W (Window Update)	12.2.1	M	M
TA5	L (Frozen Reference Time)	12.2.1.1.6	M	M

Index	**Timer/Protocol Parameter**	**References**	**ISO Status**	**CNS/ATM-1 Package Support**
ATN-TA1	R (Persistence)	12.2.1.1.5	O	O
ATN-TA2	M_{LR} (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA3	M_{RL} (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA4	E_{LR} (Maximum Transmission Delay)	12.2.1.1.2	O	O

ATN-TA5	E_{RL} (Maximum Transmission Delay)	12.2.1.1.2	O	O
Index	**Timer/Protocol Parameter**	**References**	**ISO Status**	**CNS/ATM-1 Package Support**
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

ISO Note.- The following applies to an implementation under test:

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

6.3 ATN Connectionless Transport Protocol

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

Item	**Protocol Function Support**	**Clause**	**ISO Status**	**CNS/ATM-1 Package Support**
NS	Network service selection	5.3.2.2	M	M
AM	Address mapping	5.3.2.3	M	M
	PDU Support			
UD1	Unitdata PDU supported on transmission	6.1.3	M	M
UD2	Unitdata PDU supported on reception	6.1.3	M	M
	Parameters of the Unitdata PDU on Transmission			
TpTc	<t> TPDU UD Checksum	6.2.4.1	O	O
TpTs	<t> TPDU UD Source TSAP-ID	6.2.4.1	M	M
TpTd	<t> TPDU UD Destination TSAP-ID	6.2.4.1	M	M
TpTu	<t> TPDU UD User Data	6.2.4.1	O	M
	Parameters of the Unitdata PDU on Reception			
TpRc	<r> TPDU UD Checksum	6.2.4.2	M	M
TpRs	<r> TPDU UD Source TSAP-ID	6.2.4.2	M	M

TpRd	<r> TPDU UD Destination TSAP-ID	6.2.4.2	M	M
TpRu	<r> TPDU UD User Data	6.2.4.2	M	M
	Service Support			
CL	Connectionless Mode Network Service	6.2	M	M

7. Network Layer Protocol Requirements

7.1 CLNP Requirements

The Connectionless Network Protocol (CLNP) is specified in ISO 8473:1993. In the ATN, CLNP shall be used in accordance with the ISO specification and, for ATN End Systems, in accordance with the profile specified in 7.1.2.1 below, and for ATN Routers, in accordance with the profile specified in 7.1.2.2.1 below.

All ATN End Systems supporting air/ground applications and all ATN Routers shall support the CLNP Security Parameter and the encoding of the CLNP Options field Security Parameter shall be as specified in 0 below.

Recommendation.— *ATN Routers should support the CONGESTION NOTIFICATION function.*

Recommendation.- *Mechanisms should be adopted to signal subnetwork congestion to the transport entity.*

7.1.1 Encoding of the CLNP Security Parameter

Note 1. The CLNP Options Security Parameter is used in the ATN to convey information about the Traffic Type and Routing Policy Requirements pertaining the ot the user data of the NPDU. It may also be used to convey a security classification.

Note 2. CLNP options field parameters are encoded using a type-length-value encoding. For the Security Parameter, the value of the "type" is specified in ISO 8473 as C9h.

The value component of the CLNP Options Security Parameter shall be encoded as follows:

The first octet of the parameter value shall be the security type code, defined as follows:

1. The first octet shall always be encoded as [**1100 0000]** to indicate the Globally Unique Security Format

2. The remaining octets shall contains the ATN Security Label encoded as the four fields illustrated in Figure 3, and defined below.

	Security Registration ID Length	Security Registration ID (variable)	Security Information Length	Security Information (optional)
Octet	0	1	n	n+1

Figure 3 The ATN Security Label

Note.— The Security Registration ID identifies the associated security policy.

7.1.1.1 Security Registration ID Length

This field shall be one octet long and contain the length in octets of the Security Authority's Security Registration Identifier.

7.1.1.2 Security Registration ID

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

Note.— The ATN Security Registration Identifier identifies the ATN Security Policy. ICAO has been assigned an International Code Designator (ICD) decimal value [00027] by the BSI in accordance with the dictates of ISO 6523. According to ISO 6523 and ISO 8824 this value identifies an arc off 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, ...}.

7.1.1.3 Security Information Length

This field shall be one octet in length and shall indicate the length in octets of the Security Information. If there is no security information, this field shall indicate a zero length.

7.1.1.4 Security Information

The Security Information field of the ATN Security Label shall be used to convey, as separate Tag Sets:

1. The Traffic Type.
2. The Routing Policy Requirements, if any, applicable to the transfer of the user data through the ATN.
3. The Security Classification

When no traffic type is identified then General Communications shall be assumed. When no routing policy requirements are specified then “no preference” shall be assumed. When no classification is specified then “unclassified” shall be assumed.

7.1.1.4.1 Encoding of the Security Information Field.

The Security Information Field shall comprise zero, one or two Security Tag sets, with no Security Tag with the same Tag Set Name occurring more than once.

Each Security Tag set shall consist of four fields, as illustrated in Figure 4, and defined below:

	Tag Set Name Length	Tag Set Name	Tag Set Length	Security Tag
Octet	0	1	n	n+1

Figure 4 Security Tag Set Format

7.1.1.4.1.1 Security Classification Registered Field Set

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

7.1.1.4.1.2 Security Tag Set Name

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

7.1.1.4.1.3 Tag Set Length

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

7.1.1.4.1.4 Security Tag

The Security Tag field shall be used to convey security related information for which the syntax and semantics are identified by the preceding Tag Set Name.

7.1.1.4.2 Encoding of the Tag Set for Traffic Type

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

The Security Tag shall indicate the Traffic Type of the user data contained in the NPDU according to the following table:

Security Tag Value	Semantics
0000 0001	ATN Administrative Communications
0000 0010	ATN Operational Communications
0000 0011	General Communications
0000 0100	ATN Systems Management Communications

7.1.1.4.3 Encoding of the Tag Set for Routing Policy Requirements

This Tag Set shall only be used when a tag set indicating a Traffic Type of ATN Operational Communications is also included in the same Security Information Field.

The Tag Set Name shall be set to [0000 0100].

The Security Tag shall indicate the Routing Policy Requirements for the data contained in the same NPDU, according to the following table:

Category	Security Tag Value	Semantics
Air Traffic Service Communications (ATSC)	0000 0001	No Traffic Type Policy Preference
	0000 0010	Traffic only follows ATSC route(s).
	0000 0011	Route Traffic using an ordered preference of Mode S first, then VHF Data Link, then Satellite Data Link, then HF Data Link.
Aeronautical Operational Control (AOC)	0001 0001	No Traffic Type Policy Preference.

Category	Security Tag Value	Semantics
	0001 0010	Route Traffic only via Gatelink.
	0001 0011	Route Traffic only via VHF Data Link.
	0001 0100	Route Traffic only via Satellite Data Link.
	0001 0101	Route Traffic only via HF Data Link.
	0001 0110	Route Traffic only via Mode S Data Link.
	0001 0111	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link.
	0001 1000	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then Satellite.
	0001 1001	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then HF Data Link, then Satellite Data Link.

7.1.1.4.4 Encoding of the Tag Set for Security Classification

The Tag Set Name shall be set to [0000 0011].The Security Tag shall indicate the security classification of the NPDU. according to the following table:

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

7.1.2 APRLs for the Connectionless Network Protocol

7.1.2.1 ATN specific support

Index	Item	CNS/ATM-1 Package Support

Index	Item	CNS/ATM-1 Package Support
ATNCLNP5	Implementation includes the Congestion Notification Function?	O
ATNCLNP6	Implementation includes the <r> PDU Lifetime Control function ?	O
ATNCLNP8	Implementation supports the ATN Security Policy	M

Table 2 ISO/IEC 8473 ATN specific support

Note : Recommendation ATNCLNP6 only applies to the End System part of the CNS/ATM-1 Package Router. In the Intermediate System part, the PDU Lifetime Control function is mandatory.

7.1.2.2 CLNP End System Profile

Note. In the following tables, the columns "ATN Manual Support" refers to the support requirement specified by the 2nd edition of the ATN Manual.

7.1.2.2.1 Major Capabilities - End System Implementation

Item	Capability	Ref.	ISO Status	ATN Manual Support	CNS/ATM-1 Package Support
ES	End System		O.1	O.1	M
IS	Intermediate System		O.1	O.1	–
FL-r	<r> Full protocol	6	M	M	M
FL-s	<s> Full protocol	6	M	M	M
NSS-r	<r> Non-segmenting subset	5.2	M	M	M
NSS-s	<s> Non segmenting subset	5.2	IS:M ^IS:O	IS:M ^IS:X	OX
IAS-r	<r> Inactive subset	5.2	ES:O	ES:O	O
IAS-s	<s> Inactive subset	5.2	IAS-r:M ^IAS-r:X	IAS-r:M ^IAS-r:X	IAS-r:M ^IAS-r:X
S802	SNDCF for ISO 8802	8.4.2	O.2	O	O.2
SCLL	SNDCF for CL Link Service	8.4.4.1	O.2	O	O.2
SCOL	SNDCF for CO Link Service	8.4.4.2	O.2	O	O.2
SX25	SNDCF for ISO 8208	8.4.3	O.2	O	O.2
ATN SNDCF	SNDCF for Mobile Subnetworks Draft ATN Internet SARPs Ref: Chapter 10		N/A	ISMOB:M ISGRD:O ^IS:O	O.2

Table 3 – ISO/IEC 8473 Major Capabilities - End System implementation

7.1.2.2.2 End Systems - Supported Functions

Item	Function	Ref.	ISO Status	ATN Manual Support	CNS/ATM-1 Package Support
ePDUC	PDU Composition	6.1	M	M	M
ePDUD	PDU Decomposition	6.2	M	M	M
eHFA	Header Format Analysis	6.3	M	M	M
ePDUL-s	<s> PDU Lifetime Control	6.4	M	M	M
ePDUL-r	<r> PDU Lifetime Control	6.4	O	ATNCLNP6:M	ATNCLNP6:M
eRout	Route PDU	6.5	M	M	M
eForw	Forward PDU	6.6	M	M	M
eSegm	Segment PDU	6.7	M	M	M
eReas	Reassemble PDU	6.8	M	M	M
eDisc	Discard PDU	6.9	M	M	M
eErep	Error Reporting	6.10	M	M	M
eEdec-s	<s> Header Error Detection	6.11	M	M	M
eEdec-r	<r> Header Error Detection	6.11	M	M	M
eSecu-s	<s> Security Draft ATN Internet SARPs Ref: A9.5.4	6.13	O	ATNCLNP1:M ATNCLNP2:M ATNCLNP3:O ATNCLNP7:M	ATNCLNP8:M O
eSecu-r	<r> Security Draft ATN Internet SARPs Ref: A9.5.4	6.13	O	ATNCLNP1:M ATNCLNP2:M ATNCLNP3:O ATNCLNP7:M	ATNCLNP8:M
eCRR-s	<s> Complete Route Recording	6.15	O	OX	OX
eCRR-r	<r> Complete Route Recording	6.15	O	O	OX
ePRR-s	<s> Partial Route Recording	6.15	O	M	M
ePRR-r	<r> Partial Route Recording	6.15	O	M	M
eCSR	Complete Source Routing	6.14	O	OX	OX
ePSR	Partial Source Routing	6.14	O	OX	OX
ePRI-s	<s> Priority	6.17	O	M	MO
ePRI-r	<r> Priority	6.17	O	M	MO
eQOSM-s	<s> QOS Maintenance	6.16	O	M	MO
eQOSM-r	<r> QOS Maintenance	6.16	O	M	MO
eCong-s	<s> Congestion Notification	6.18	eQOSM-s:M	eQOSM-s:M	ATNCLNP5:M O
eCong-r	<r> Congestion Notification	6.18	O	O	ATNCLPN5:M
ePadd-s	<s> Padding	6.12	O	OX	OX
ePadd-r	<r> Padding	6.12	M	M	M
eEreq	Echo Request	6.19	O	O	M
eErsp	Echo Response	6.20	O	O	M
eSegS	Create segments smaller than necessary	6.8 Note 2 b)	O	O	O

Table 4 – ISO/IEC 8473 End Systems Supported Functions

7.1.2.2.3 Supported Security Parameters

Item	Function	Ref.	ISO Status	ATN Manual Support	CNS/ATM -1 Package Support
iSADSSEC	Source Address Specific Security	7.5.3.1	iSecu:O.5	iSecu:O	OX
iDADSSEC	Destination Address Specific Security	7.5.3.2	iSecu:O.5	iSecu:O	OX
iGUNSEC	Globally Unique Security	7.5.3.3	iSecu:O.5	iSecu:M	ATNCLNP8: M

Table 5 – ISO/IEC 8473 supported security parameters

7.1.2.2.4 Quality of Service Maintenance Function

Item	Function	Ref.	ISO Status	ATN Manual Support	CNS/ATM-1 Package Support
iQOSNAVAIL	If requested QOS not available, deliver at different QOS	6.16	iQOSM:M	iQOSM:M	M
iQOSNOT	Notification of failure to meet requested QOS	6.16	iQOSM:O	iQOSM:M	M
	Which of the following formats of QOS are implemented ?				
iSADDQoS	Source Address Specific QoS	7.5.6.1	iQoSM:O.3	iQOSM:O	OX
iDADDQoS	Destination Address Specific QoS	7.5.6.2	iQoSM:O.3	iQOSM:O	OX
iGUNQoS	Globally Unique QoS	7.5.6.3	iQoSM:O.3	iQOSM:M	M
iSvTD	Sequencing V's Transit Delay	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4
iCongE	Congestion Experienced	7.5.6.3	iGUNQoS:O.4	ATNCLNP5:M	M
iTDvCst	Transit Delay versus Cost	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4
iREPvTD	Residual Error Probability versus Transit Delay	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4
iREPvCst	Residual Error Probality versus Cost	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4

Table 6 – ISO/IEC 8473 Quality of Service Maintenance Function

7.1.2.2.5 End Systems - Timers

Item	Timer	Ref.	ISO Status	ISO Range	ATN Manual Support	CNS/ATM -1 Package Support
eReasTim	Reassembly Timer	6.8	M	500ms to 127.5s	M	500ms to 127.5s

Table 7 – ISO/IEC 8473 End Systems Timers

7.1.2.3 CLNP Intermediate System Profile

7.1.2.3.1 Major Capabilities

Item	Capability	Ref.	ISO Status	ATN Manual Support	CNS/ATM-1 Package Support
ES	End System		O.1	O.1	-
IS	Intermediate System		O.1	O.1	M
FL-r	<r> Full protocol	6	M	M	M
FL-s	<s> Full protocol	6	M	M	M
NSS-r	<r> Non-segmenting subset	5.2	M	M	M
NSS-s	<s> Non segmenting subset	5.2	IS:M ^IS:O	IS:M ^IS:X	M
IAS-r	<r> Inactive subset	5.2	ES:O	ES:O	-
IAS-s	<s> Inactive subset	5.2	IAS-r:M ^IAS-r:X	IAS-r:M ^IAS-r:X	-
S802	SNDCF for ISO 8802	8.4.2	O.2	O	M
SCLL	SNDCF for CL Link Service	8.4.4.1	O.2	O	O
SCOL	SNDCF for CO Link Service	8.4.4.2	O.2	O	O
SX25	SNDCF for ISO 8208	8.4.3	O.2	O	O
ATN SNDCF	SNDCF for Mobile Subnetworks Draft ATN Internet SARPs Ref: Chapter 10		N/A	ISMOB:M ISGRD:O ^IS:O	ISMOB:M ISGRD:O ^IS:O

Table 8 – ISO/IEC 8473 major capabilities

ISMOB: If ISO 8473 is used over mobile subnetworks, then ISMOB is true, else ISMOB is false.

ISGRD: If ISO 8473 is used over ground subnetworks, then ISGRD is true, else ISGRD is false.

7.1.2.3.2 Intermediate Systems - Supported Functions

Item	Function	Ref.	ISO Status	ATN Manual Support	CNS/ATM -1 Package Support
iPDUC	PDU Composition	6.1	M	M	M
iPDUD	PDU Decomposition	6.2	M	M	M
iHFA	Header Format Analysis	6.3	M	M	M
iPDUL	PDU Lifetime Control	6.4	M	M	M
iRout	Route PDU	6.5	M	M	M
iForw	Forward PDU	6.6	M	M	M
iSegm	Segment PDU	6.7	iDSNS:M	iDSNS:M	M
iReas	Reassemble PDU	6.8	O	O	O
iDisc	Discard PDU	6.9	M	M	M
iErep	Error Reporting	6.10	M	M	M
iEdec	Header Error Detection	6.11	M	M	M
iSecu-	Security Draft ATN Internet SARPs Ref: A9.4.2, A9.5.4	6.13	O	ATNCLNP1:M ATNCLNP2:M ATNCLNP3:O ATNCLNP7:M	ATNCLNP8: M
iCRR-	Complete Route Recording	6.15	O	OX	OX
iPRR-	Partial Route Recording Draft ATN Internet SARPs Ref:A9.4.4	6.15	O	M	M
iCSR	Complete Source Routing Draft ATN Internet SARPs Ref: A9.4.3	6.14	O	OX	OX
iPSR	Partial Source Routing Draft ATN Internet SARPs Ref: A9.4.3	6.14	O	OX	OX
iPRI-	Priority Draft ATN Internet SARPs Ref: A9.4.4	6.17	O	M	M
iQOSM-	QOS Maintenance Draft ATN Internet SARPs Ref: A9.4.5, A9.5.4.4	6.16	O	M	M
iCong-	Congestion Notification Draft ATN Internet SARPs Ref: 9.4.7	6.18	O	ATNCLNP5:M	ATNCLNP5: M
iPadd-r	<r> Padding	6.12	M	M	M
eEreq	Echo Request	6.19	O	O	M
eErsp	Echo Response	6.20	O	O	M
iSegS	Create segments smaller than necessary	6.8	O	O	O
iDSNS	Simultaneous support of subnetworks with different SN-User data sizes Draft ATN Internet SARPs Ref: A10.3.7		O	O	O

Table 9 – ISO/IEC 8473 Intermediate Systems supported functions

7.1.2.3.3 Supported Security Parameters

Item	Function	Ref.	ISO Status	ATN Manual Support	CNS/ATM -1 Package Support
iSADSSEC	Source Address Specific Security	7.5.3.1	iSecu:O.5	iSecu:O	OX
iDADSSEC	Destination Address Specific Security	7.5.3.2	iSecu:O.5	iSecu:O	OX
iGUNSEC	Globally Unique Security	7.5.3.3	iSecu:O.5	iSecu:M	ATNCLNP8: M

Table 10 – ISO/IEC 8473 supported security parameters

7.1.2.3.4 Quality of Service Maintenance Function

Item	Function	Ref.	ISO Status	ATN Manual Support	CNS/ATM-1 Package Support
iQOSNAVAIL	If requested QOS not available, deliver at different QOS	6.16	iQOSM:M	iQOSM:M	M
iQOSNOT	Notification of failure to meet requested QOS	6.16	iQOSM:O	iQOSM:M	M
	Which of the following formats of QOS are implemented ?				
iSADDQoS	Source Address Specific QoS	7.5.6.1	iQoSM:O.3	iQOSM:O	OX
iDADDQoS	Destination Address Specific QoS	7.5.6.2	iQoSM:O.3	iQOSM:O	OX
iGUNQoS	Globally Unique QoS	7.5.6.3	iQoSM:O.3	iQOSM:M	M
iSvTD	Sequencing V's Transit Delay	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4
iCongE	Congestion Experienced	7.5.6.3	iGUNQoS:O.4	ATNCLNP5:M	M
iTDvCst	Transit Delay versus Cost	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4
iREPvTD	Residual Error Probability versus Transit Delay	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4
iREPvCst	Residual Error Probality versus Cost	7.5.6.3	iGUNQoS:O.4	iQOSM:M	iGUNQoS:O.4

Table 11 – ISO/IEC 8473 Quality of Service Maintenance Function

7.1.2.3.5 Intermediate Systems - Timer and Parameter Values

Item	Timer	Ref.	ISO Status	ATN Manual Support	CNS/ATM -1 Package Support
iReasTim	Reassembly Timer	6.8	iReas:M	M	500ms to 127.5s

Table 12 – ISO/IEC 8473 Intermediate Systems Timer and Parameter Values

7.2 IDRP Requirements

7.2.1 Protocol Extensions

7.2.1.1 Use of the Security Path Attribute

ATN Routers supporting inter-domain routing (i.e. Router Classes 4 to 7 inclusive) shall support the IDRP Security Path Attribute with a Security Registration Identifier set to the value defined in 7.1.1.2 for the ATN Security Registration Identifier. 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 7.1.1.4.1. The following Security Tag Sets shall be supported:

1. The Traffic Type, as defined in 7.1.1.4.2.

2. The Security Classification, as defined in 7.1.1.4.4, when the router supports classified data.

3. The Air-Ground Subnetwork type, as defined in 7.2.1.2.

When a route is available for more than one traffic type, then a Security Tag set shall be encoded into this field for each Traffic Type for which the route is available. If no Traffic Type Security Tag sets are present then this shall imply that all Traffic Types are supported.

When a route may pass over more than one air-ground subnetwork type, then a Security Tag set shall be encoded into this field for each air-ground subnetwork that the route may pass over.

7.2.1.2 Encoding of the Air/Ground Subnetwork Type

The Tag Set Name shall be set to [0000 0101].

The Security Tag shall indicate the air-ground subnetwork that the route may pass over according to the following table:

Subnetwork Type	Security Tag
Mode S	0000 0001
VDL	0000 0010
AMSS	0000 0011
Gatelink	0000 0100

7.2.1.3 Update of Security Information

When a Route is received over an adjacency supported by one or more air-ground subnetworks and the route contains a Security Path Attribute and 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. If ITU requirements or local policy restricts the Traffic Types that may pass over the subnetworks supporting the adjacency then:

a) If no Traffic Type Security Tags are already present then a Security Tag shall be added for each Traffic Type permitted to pass over the subnetworks, otherwise

b) Any Traffic Type Security Tags that identify Traffic types which ITU or local policy does not permit over these subnetworks, shall be removed.

2. A Security Tag shall be added for each air-ground subnetwork supporting the adjacency and which is not already contained in the Security Information.

3. When the router supports classified data, and 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.

7.2.1.4 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.*

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. 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.

7.2.2 CLNP Forwarding

Note 1. For the purposes of specifying the rules for CLNP forwarding using information learnt by IDRP, this specification assumes an implementation model whereby each distinct combination of Security Tag Sets in the CLNP Options Security Parameter uniquely identifies a Forwarding Information Base (FIB). Forwarding then takes place by forwarding on the longest matching address prefix, if any, present in that FIB only. This implementation model is not mandatory, and any implementation that externally exhibits identical behaviour, will comply with this specification.

Note 2. ISO/IEC 10747 clause 7.16.2 requires that a loc-RIB that is identified by a RIB_ATT containing the Security Path Attribute can contain more than one route to the same NLRI, provided that those routes provide the same level of protection.

When the Security Registration Identifier in an IDRP Security Path Attribute indicates the ATN Security Policy, then only a Security Classification Tag set, if present, shall indicate a difference in the level of protection offered by the route.

When the IDRP Phase 2 Routing Decision Process generates the entries for a FIB identified by a combination of Security Tag Set values, then only those routes in the loc-RIB identified by the RIB_Att that contains the ATN Security Policy Security Path Attribute shall be used to generate the FIB entries, and only those routes shall be chosen which:

1. Are available for the Traffic Type contained in the set of Security Tag set values that identifies the FIB.

2. May pass over air-ground subnetwork(s) compatible with the Routing Policy Requirements contained in the set of Security Tag set values that identifies the FIB.

3. Provide sufficient protection i.e. have a superior classification to that given in the Security Tag Set for the Security Classification contained in the set of Security Tag set values that identifies the FIB.

When more than one route is contained in the Loc-RIB that meets the above rules, then the route shall be selected which best meets the Routing Policy Requirements. Local Policy rules shall apply if two or more routes best meet the Routing Policy Requirements.

When more than one subnetwork supports the selected route (i.e. the adjacency with the next hop BIS), then the FIB shall identify as the next hop subnetwork, the subnetwork that supports the adjacency that:

1. Is available for the Traffic Type contained in the set of Security Tag set values.

2. Best meets the Routing Policy Requirements, if the subnetwork is an air-ground subnetwork.

3. Provides sufficient protection.

7.2.3 Compliance Statement

7.2.3.1 Air-Ground Router

Note. Only Class 6 ATN Air-Ground Routers implement IDRP. This compliance statement does not apply to Class 7 ATN Air-Ground Routers.

An Air-Ground Router shall implement the ISO 10747 Routing Information Protocol in compliance with the APRL specified in 7.2.3.3, and the requirements contained in the remainder of this section.

7.2.3.1.1 RIB_ATT Support

A CNS/ATM-1 Package Air-Ground Router incorporating IDRP shall support the following RIB_Att sets, and shall attempt to negotiate the use of all those RIB_Atts it supports when opening a BIS-BIS connection:

a. The empty RIB-Att

b. SECURITY

An Instance of the Security Path Attribute shall be supported for the *ATN Security Policy* (See 0). The Traffic Type and Air-Ground Subnetwork Type Security Tags shall be supported for use with the ATN Security Policy Security Path Attribute. When the router supports classified data then the Security Classification Security Tag shall also be supported.

7.2.3.1.2 Routing Policy Rules

7.2.3.1.2.1 Route Origination and Selection

An Air-Ground Router shall provide to each adjacent ATN Ground-Air Router to which it is currently connected, one or more routes to the NSAPs and NETs contained within its local RD; a route to the same set of NSAP Address Prefixes shall be advertised to a Ground-Air Router for the SECURITY RIB_Att only.

Note: rules to select the routes that the router will use, out of those offered by Ground-Air Routers, are at the discretion of the aircraft operator.

7.2.3.1.2.2 Network Later Reachability Information

An Air-Ground Router shall not originate a route containing an NSAP Address Prefix in any of its path attributes or Network Layer Reachability Information, that is not octet aligned.

7.2.3.1.2.3 Multiple Subnetwork Paths

Note. Support for QoS Metrics is optional in CNS/ATM-1 Package.

The values of QoS metrics in routes advertised to a Ground-Air Router, if any, shall reflect the “best” subnetwork to use for that metric. e.g. the value of the Transit Delay metric shall reflect the subnetwork joining the Air-Ground and Ground-Air Router which is both available for use and has the lowest transit delay.

Note: CNS/ATM-1 Package Routers implementing IDRP may be linked by more than one subnetwork path. This situation is viewed by IDRP as still a single adjacency. However, the available QoS may be different. These differences need to be reflected dynamically whenever the communications paths between an Air-Ground and a Ground-Air Router change.

Whenever a new subnetwork connection becomes available between an Air-Ground Router and a Ground-Air Router that have an existing adjacency, or when a subnetwork connection is lost without losing the adjacency (i.e. another subnetwork connection is still available for use), then the routes to be advertised shall be re-computed according to the above requirements.

7.2.3.2 Ground-Air Router

A Ground-Air Router (Class 5) shall implement the ISO 10747 Routing Information Protocol in compliance with the APRL specified in 7.2.3.3, and the requirements contained in the remainder of this section for exchanging routing information with an Air-Ground Router (Class 6).

7.2.3.2.1 RIB_ATT Support

A CNS/ATM-1 Package Ground-Air Router incorporating IDRP shall support the following RIB_Att sets, and shall attempt to negotiate the use of all those RIB_Atts it supports when opening a BIS-BIS connection:

a. The empty RIB-Att

b. SECURITY.

An Instance of the Security Path Attribute shall be supported for the *ATN Security Policy* (See 0). The Traffic Type and Air-Ground Subnetwork Type Security Tags shall be supported for use with the ATN Security Policy Security Path Attribute. When the router supports classified data then the Security Classification Security Tag shall be supported.

7.2.3.2.2 Routing Policy Rules

7.2.3.2.2.1 Route Origination and Selection

An ATN Ground-Air Router shall provide the following routes to each adjacent Air-Ground RD, and for the SECURITY RIB_Att only:

1. A route to NSAPs and NETs contained within the Ground-Air Router's local RD; the route's destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD.

2. An aggregated route to NSAPs and NETs contained within the local ATN Island RDC;

3. An aggregated route to NSAPs and NETs contained within all other ATN Islands for which a route is available.

Note: rules to select the routes that the router will use, out of those offered by Air-Ground Routers, are at the discretion of the ground network operator.

7.2.3.2.2.2 Network Later Reachability Information

A Ground-Air Router shall not originate a route containing an NSAP Address Prefix in any of its path attributes or Network Layer Reachability Information, that is not octet aligned.

7.2.3.2.2.3 Multiple Subnetwork Paths

The values of QoS metrics in routes advertised to an *Air-Ground* Router, if any, shall reflect the "best" subnetwork to use for that metric. e.g. the value of the Transit Delay metric shall reflect the subnetwork joining the *Air-Ground* and Ground-Air Router which is both available for use and has the lowest transit delay.

Note: CNS/ATM-1 Package Routers implementing IDRP may be linked by more than one subnetwork path. This situation is viewed by IDRP as still a single adjacency. However, the available QoS may also be different. These differences need to be reflected dynamically whenever the communications paths between an Air-Ground and a Ground-Air Router change.

Whenever a new subnetwork connection becomes available between an Air-Ground Router and a Ground-Air Router that have an existing adjacency, or when a subnetwork connection is lost without losing the adjacency (i.e. another subnetwork connection is still available for use), then the routes to be advertised shall be re-computed according to the above requirements. Any routes for which the QoS metrics have changed, shall be re-advertised to the Air-Ground Router upon expiry of the **minRouteOrigination** timer, or the **minRouteAdvertisement** time, as appropriate.

7.2.3.2.3 Routing Domain Confederations

A Ground-Air Router shall be a member of the Fixed ATN RDC and the RDC of the ATN Island(s) of which it is a member. If the local RD is also a Backbone RD, the Ground-Air Router shall also be a member of the appropriate Backbone RDC.

7.2.3.3 APRLs

7.2.3.3.1 ATN Specific Protocol Requirements

Index	Item	Ground-Air Router	Air-Ground Router
ATNIDRP10	Does the implementation support the ATN Security Policy?	M	M
ATNIDRP11	Does the implemenation support classified data communications	O	O

7.2.3.3.1.1 IDRP General

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
BASIC	Are all basic BIS functions implemented?	12.1	M	M	M
MGT	Is this system capable of being managed[1] by the specified management information?	11	M	O	O
VER	Does this BIS support Version Negotiation?	7.8	M	M	M
RTSEP	Does this BIS support ROUTE_SEPARATOR attribute?	7.12.1	M	M	M
HOPS	Does this BIS support the RD_HOP_COUNT attribute?	7.12.13	M	M	M
PATH	Does this BIS support the RD_PATH attribute?	7.12.3	M	M	M
CAPY	Does this BIS support the Capacity Attribute?	7.12.15	M	M	M
FSM	Does this BIS manage BIS-BIS connections according to the BIS FSM description?	7.6.1	M	M	M
FCTL	Does this BIS provide flow control?	7.7.5	M	M	M
SEQNO	Does this BIS provide sequence number support?	7.7.4	M	M	M
INTG1	Does this BIS provide Data integrity using authentication type 1?	7.7.1	O.1	M	M
INTG2	Does this BIS provide Data integrity using authentication type 2?	7.7.2	O.1	O	O
INTG3	Does this BIS provide Data integrity using authentication type 3?	7.7.3	O.1	O	O
ERROR	Does this BIS handle error handling for IDRP?	7.20	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

7.2.3.3.1.2 IDRP Update Send Process

	Item	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
INT	Does the BIS provide the internal update procedures?	7.17.1	M	M	O
RTSEL	Does this BIS support the **MinRouteAdvertisementInterval** Timer?	7.17.3.1	M	M	O

1 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 CNS/ATM-1 Package and hence it is not reasonable to require mandatory support for this requirement.

RTORG	Does this BIS support the **MinRDOriginationInterval** Timer?	7.17.3.2	M	M	M
JITTER	Does this BIS provide jitter on its timers?	7.17.3.3	M	M	M

7.2.3.3.1.3 IDRP Update Receive Process

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
INPDU	Does the BIS handle inbound BISPDUs correctly?	7.14	M	M	M
INCONS	Does this BIS detect inconsistent routing information?	7.15.1	M	M	M

7.2.3.3.1.4 IDRP Decision Process

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
TIES	Does this BIS break ties between candidate routes correctly?	7.16.2.1	M	M	M
RIBUPD	Does this BIS update the Loc-RIBs correctly?	7.16.2	M	M	M
AGGRT	Does this BIS support route aggregations?	7.18.2.1, 7.18.2.2, 7.18.2.3	O	M	O
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
FIBUPD	Does this BIS create FIB entries reflecting subnetwork access restrictions correctly ?	7.16.2	-	M	M

7.2.3.3.1.5 IDRP Receive Process

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
RCV	Does the BIS process incoming BISPDUs and respond correctly to error conditions?	7.14, 7.20	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

MXPDU	Does the BIS accept incoming UPDATE, IDRP ERROR and RIB REFRESH PDUs whose size in octets is between **minBISPDULength** and **maxBISPDULength**?	6.2,7.20	M	M	M

7.2.3.3.1.6 IDRP Optional Transitive Attributes

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
MEXIT	Does this BIS support use of the MULTI-EXIT DISC attribute?	7.12.7	O	O	O

7.2.3.3.1.7 Peer Entity Authentication

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
AUTH	Does this BIS correctly authenticate the source of a BISPDU?	7.7.2	O	M	M

7.2.3.3.1.8 Generating Well-Known Discretionary Attributes

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
EXTG	Does the BIS support generation of the EXT_INFO attribute?	7.12.2	O	O	O
NHRS	Does the BIS support generation of the NEXT_HOP attribute in support of route servers?	7.12.4	O	OX	O
NHSN	Does the BIS support generation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	OX	O
DLI	Does the BIS support generation of the DIST_LIST_INCL attribute?	7.12.5	O	MO	MO
DLE	Does the BIS support generation of the DIST_LIST_EXCL attribute?	7.12.6	O	OX	O
TDLY	Does the BIS support generation of the TRANSIT DELAY attribute?	7.12.8	O	O	O
RERR	Does the BIS support generation of the RESIDUAL ERROR attribute?	7.12.9	O	O	O
EXP	Does the BIS support generation of the EXPENSE attribute?	7.12.10	O	O	O
LQOSG	Does the BIS support generation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	OX	OX
HREC	Does the BIS support generation of the HIERARCHICAL RECORDING attribute?	7.12.12	O	OX	OX
SECG	Does the BIS support generation of the SECURITY attribute?	7.12.14	O	M	M
PRTY	Does the BIS support generation of the PRIORITY attribute?	7.12.16	O	O	O

7.2.3.3.1.9 Propagating Well-Known Discretionary Attributes

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
EXTGP	Does the BIS support propagation of the EXT_INFO attribute?	7.12.2	M	M	-
NHRSP	Does the BIS support propagation of the NEXT_HOP attribute in support of route servers?	7.12.4	O	OX	-
NHSNP	Does the BIS support propagation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	OX	-
DLIP	Does the BIS support propagation of the DIST_LIST_INCL attribute?	7.12.5	O	M	-
DLEP	Does the BIS support propagation of the DIST_LIST_EXCL attribute?	7.12.6	O	M	-
TDLYP	Does the BIS support propagation of the TRANSIT DELAY attribute?	7.12.8	O	O	-
RERRP	Does the BIS support propagation of the RESIDUAL ERROR attribute?	7.12.9	O	O	-
EXPP	Does the BIS support propagation of the EXPENSE attribute?	7.12.10	O	O	-
LQOSP	Does the BIS support propagation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	O	-
HRECP	Does the BIS support propagation of the HIERARCHICAL RECORDING attribute?	7.12.12	O	OX	-
SECP	Does the BIS support propagation of the SECURITY attribute?	7.12.14	O	M	-
PRTYP	Does the BIS support propagation of the PRIORITY attribute?	7.12.16	O	O	-

7.2.3.3.1.10 Receiving Well-Known Discretionary Attributes

Item	Description	Ref.	ISO Status	Ground-Air Router	Air-Ground Router
EXTR	Does the BIS recognise upon receipt the EXT_INFO attribute?	7.12.2	M	M	M
NHRSR	Does the BIS recognise upon receipt the NEXT_HOP attribute ?	7.12.4	M	M	O
DLIR	Does the BIS recognise upon receipt the DIST_LIST_INCL attribute?	7.12.5	M	M	M
DLER	Does the BIS recognise upon receipt the DIST_LIST_EXCL attribute?	7.12.6	M	M	M
TDLYR	Does the BIS recognise upon receipt the TRANSIT DELAY attribute?	7.12.8	M	M	O
RERRR	Does the BIS recognise upon receipt the RESIDUAL ERROR attribute?	7.12.9	M	M	O
EXPR	Does the BIS recognise upon receipt the EXPENSE attribute?	7.12.10	M	M	O
LQOSR	Does the BIS recognise upon receipt the LOCALLY DEFINED QOS attribute?	7.12.11	O	O	O
HRECR	Does the BIS recognise upon receipt the HIERARCHICAL RECORDING attribute?	7.12.12	M	M	O
SECR	Does the BIS recognise upon receipt the SECURITY attribute?	7.12.14	M	M	M
PRTYR	Does the BIS recognise upon receipt the PRIORITY attribute?	7.12.16	M	M	O

7.2.3.4 ES-IS Requirements

In support of the Route Initiation procedures over air-ground subnetworks, the ISO 9452 ES-IS Configuration Information function shall be supported in compliance with the APRL given below.

Note. The ES-IS protocol may also be used within a Routing Domain to support routing information exchange between End Systems and Routers and between Routers in support of ISO/IEC 10589. However, the profile for this use is outside of the scope of this specification.

Item	Protocol Function	Ref.	ISO Status	ATN Support	CNS/ATM -1 Package Support
CI	Is configuration information supported ?		O	M	M
RI	Is redirection information supported ?		O	O	-
	Are the following functions supported ?				
ErrP	Protocol Error Processing	6.13	M	M	M
HCsV	PDU Header Checksum Validation	6.12	M	M	M
HCsG	PDU Header Checksum Generation	6.12	O	O	MO
RpCf	Report Configuration	6.2,6.2.2	CI:M	CI:M	M
RcCf	Record Configuration	6.3,6.3.1	CI:M	CI:M	M
FlCf	Flush Old Configuration	6.4	CI:M	CI:M	M
RqRd	Request Redirect	6.8	RI:M	RI:M	-
CfNt	Configuration Notification	6.7	CI:O	CI:M	-
CTGn	ESCT Generation	6.3.2	CI:O	CI:O	-
AMGn	Address Mask (only) generation	6.8	RI:O	RI:O	-
SMGn	Address mask and SNPA Mask generation	6.8	RI:O	RI:O	-
	Are the following PDUs Supported ?				
ESH-r	<r> End System Hello	7.1,7.5	CI:M	CI:M	-
ISH-<r>	<r> Intermediate System Hello	7.1,7.6	CI:O	CI:O	M
ISH-<s>	<s> Intermediate System Hello	7.1,7.6	CI:M	CI:M	M
RD-s	<s> Redirect	7.1,7.7	RI:M	RI:M	-
RD-r	<r> (ignore) Redirect	6.9,7.1,7.7	M	M	-
	Are the following PDU fields supported ?				
FxPt	<s> Fixed Part <r> Fixed Part	7.2.1-7 7.2.1-7	M M	M M	M M
SA-r	<r> Source Address, one or more NSAPs	7.3.1/2/3	CI:M	CI:M	-
NET-s	<s> Network Entity Title	7.3.1/2/4	M	M	M
NET-r	<r> Network Entity Title	7.3.1/2/4	ISH-r:M	ISH-r:M	M
DA-s	<s> Destination Address	7.3.1/2/5	RI:M	RI:M	-
BSNPA-s	<s> Subnetwork Address	7.3.1/2/6	RI:M	RI:M	-
Scty-s	<s> Security	7.4.2	O	O	OX
Scty-r	<r> Security	7.4.2	O	O	OX
Pty-s	<s> Priority	7.4.3	O	O	OX
Pty-r	<r> Priority	7.4.3	O	O	OX
QoSM-s	<s> QOS Maintenance	7.4.4	RI:O	RI:O	-
AdMk-s	<s> Address Mask	7.4.5	RI:O	RI:O	-
SNMk-s	<s> SNPA Mask	7.4.6	RI:O	RI:O	-
ESCT-s	<s> Suggested ES Configuration Timer	7.4.7	CI:O	CI:O	O
ESCT-r	<r> (ignore) Suggested ES Configuration Timer	7.4.7	ISH-r:M	ISH-r:M	M

Item	Protocol Function	Ref.	ISO Status	ATN Support	CNS/ATM-1 Package Support
OOpt-r	<r> (ignore) unsupported or unknown options	7.4.1	M	M	M
OOpt-s	<s> Other options		P	P	X
	Parameter Ranges				
HTv	What range of values can be set for the Holding Time Field in transmitted PDUs ?		M	M	1 to 30s, with 1s resolution
CTv	If configuration information is supported, what range of values can be set for the Configuration Timer ?		CI:M	CI:M	1 to 30s, with 1s resolution

Table 13 – ISO 9542 Intermediate Systems

7.2.3.5 Mobile SNDCF Requirements

In both **Air-Ground** and **Ground-Air Router**s, implementations of the ICAO Mobile SNDCF shall be compliant with the following APRL.

7.2.3.5.1 Major Capabilities

Item	Capability	Mobile SNDCF PICS Reference	Status	CNS/ATM-1 Package Support
mcSetup	Call Setup and Clearing Procedures	2.1	M	M
*mcNego	Negotiation of Compression Algorithm	2.2.1	O	M
*mcLocRef	Local Reference Header Compression	2.2.2	O.1	M
*mcCan	Local Reference Cancellation	2.2.3	mcLocRef:O ^mcLocRef:X	O
*mcACA	ICAO Address Compression Algorithm	2.2.4	O.1[2]	O
mcV42	V.42bis Compression	2.2.5	O.1[2]	O

[2] Dynamically, if both V.42bis compression and the ICAO ACA are implemented, only one of these options may be accepted if Negotiation Of Compression Algorithm is implemented. Alternatively, if Negotiation Of Compression Algorithm is not implemented, or Fast Select is not available, then only one of these options may be offered.

7.2.3.5.2 Call Setup and Clearing Procedures

Item	Function	ATN Manual Reference	Status	CNS/ATM-1 Package Support
csDynam	Dynamic Call Setup	A10.6.4.3.2	O.2	O
csSys	Call Setup by Systems Management	A10.6.4.3.2	O.2	M
csPri	Mapping onto subnetwork priority[3]	A10.6.4.3.2	M	M
csDef	Use of non-standard Default packet size	A10.6.4.3.2	M	M
csFast	Use of Fast Select[4]	A10.6.4.3.2	M	M
csOther	Use of other optional User Facilities and CCITT-specified DTE facilities	A10.6.4.3.2	O[5]	O
csAdd	Use of additional call user data in call request	A10.6.4.3.2	O	O
csReq	Required use of additional user data in incoming call request	A10.6.4.3.2	X	X
csCol	Call Collision Resolution	A10.6.4.3.2	M	M
csNeg	Call Acceptance/Rejection Procedures	A10.6.4.3.2	M	M
csDiag	Use of call rejection diagnostic codes	A10.6.4.3.2	O	O
csReset	Call Reset procedures	A10.6.4.11	M	M
csSMClear	Call Clearing by Systems Management	A10.6.4.10	O.3	M
csTimeClear	Call Clearing on an inactivity timeout	A10.6.4.10	O.3	O

[3] The supplier shall explain how the mapping between the SN-Unitdata priority and subnetwork priority is performed.

[4] Only required if supported by subnetwork

[5] If answered “yes”, suppliers shall describe each optional User Facilities and CCITT-specified DTE facilities supported and the use made of it.

csResClear	Call Clearing when resources required by a higher priority VC	A10.6.4.10	O.3	O

8. Mobile Routing Requirements

8.1 Requirements for Airborne Air/Ground BISs

Specific requirements are placed on airborne systems, in order to simplify their implementation while allowing for future growth to full ATN Manual functionality. These requirements are described in the following sub-sections.

8.1.1 Requirements related to General Routing Functionality

Airborne Air/Ground BISs:

a) may optionally support quality of service (QOS) based routing decisions, but must not reject CLNP Network Protocol Data Units (NPDUs) with QOS maintenance parameters set;

b) must support security-based (i.e. traffic type) routing decisions, and thus must not reject CLNP NPDUs with security parameters set;

c) may optionally support ISO 10747 (IDRP) over the air/ground subnetworks, but must indicate their level of routing service to ground peers as described in this paper: and,

d) if not supporting IDRP shall accept NPDUs addressed to the airborne NSAP with an N-SEL set to **<0x00>** (i.e. addressed to a network entity containing IDRP), but shall ignore their content (i.e. an airborne router opting not to implement IDRP shall gracefully ignore any NPDUs containing IDRP PDUs that may be sent to the aircraft).

8.1.2 Requirements related to Air/Ground Routing Initiation

Air/Ground BISs operating over an ISO 8208 subnetwork that provides connectivity information (refer to Section 6.1.2 of the ATN Manual) may optionally not support the full ISO 9542 (ES-IS) protocol, but must support as a minimum the capabilities described in the following sub-sections, based on the airborne IS operating role.

8.1.2.1 Airborne Air/Ground BIS Operation in the “Initiator Role”

The following procedures and requirements apply to an airborne BIS operating in the “initiator role” while connected to an ISO 8208 subnetwork that provides connectivity information (e.g. the aeronautical satellite subnetwork), as specified in Section A6.1.2 of the ATN Manual or otherwise.

Airborne BISs must provide the following capabilities:

i) Accept any incoming Intermediate System Hello (ISH) PDU from the ES-IS protocol and update the local router Forwarding Information Base (FIB) accordingly (i.e. with NET/DTE/SNPA address mapping information).

ii) Upon reception of a join-event notification from the local subnetwork interface unit (e.g. the notification of successful GES logon from a Data-3 SDU), generate an ISH (as per ISO 9542, and the ATN Manual, Section

A6.1.2.2.1) containing the NET of the local airborne router to all appropriate remote ground routers, as qualified below:

a) The routers with which an ISO 9542 dialogue takes place (i.e. the "appropriate routers") must be locally known, based on static, dynamic, or configurable procedures.

Note: In the case of the satellite subnetwork, the routers reachable via the connected GES may be known by means of a table containing a list of reachable router Data Circuit-Terminating Equipment (DTE) and Subnetwork Point of Attachment (SNPA) addresses associated with a particular Satellite, Satellite Beam and GES ID. The ID of the connected GES (including the satellite ID and beam ID) provides an index into that table, and the receipt of a join-event allows the tagging of the associated entries in that table as "reachable".

b) The local NET value reported to the remote (i.e. ground) BIS must have an N-SEL field set to **<0x00>** when the airborne router supports ISO 10747 (IDRP) and an N-SEL value set to **<0xfe>** when the airborne router does not support IDRP. The ground router is expected to adapt to the mode of operation offered by the airborne router.

c) The holding time in the ISH PDU should be set to an infinite value in the case where IDRP is operated over the air/ground path, as recommended in the ATN Manual. If the airborne router does not support IDRP, the holding time must be set to a value of **<3>** minutes.

iii) If the airborne router does not support IDRP over the air/ground path, these ISH PDUs must be sent periodically, with the format and content described above, at a rate compatible with the holding time specified in the initial ISH PDU. Note that this is counter to the recommendation in the ATN Manual, Section A6.1.2.2.1, but is required in the absence of the air/ground operation of IDRP. In this situation, the periodic ISH PDUs function in the manner of the IDRP keep-alive functionality.

8.1.2.2 Airborne Air/Ground BIS Operation in the "Responder Role"

The following procedures and requirements apply to an airborne BIS operating in the "responder role" while connected to an ISO 8208 subnetwork that provides connectivity information (e.g. the Mode S subnetwork), as specified in Section A6.1.2 of the ATN Manual.

Airborne BISs must provide the following capabilities:

i) Accept any incoming Intermediate System Hello (ISH) PDU from the ES-IS protocol and update the local router Forwarding Information Base (FIB) accordingly (i.e. with NET/DTE/SNPA address mapping information).

ii) Upon reception of an incoming ISH PDU from the BIS acting as the "initiator" (i.e. in this case, the ground BIS), generate an ISH (as per ISO 9542, and the ATN Manual, Section A6.1.2.1.1) containing the NET of the local airborne router to that ground router, as qualified below:

a) The local NET value reported to the remote (i.e. ground) BIS must have an N-SEL field set to **<0x00>** when the airborne router supports ISO 10747 (IDRP) and an N-SEL value set to **<0xfe>** when the airborne router does not support IDRP. The ground router is expected to adapt to the mode of operation offered by the airborne router.

b) The holding time in the ISH PDU must be set to an infinite value in the case where IDRP is operated over the air/ground path. If the airborne router does not support IDRP, the holding time must be set to a value of **<3>** minutes.

iii) If the airborne router does not support IDRP over the air/ground path, these ISH PDUs must be sent periodically, with the format and content described above, at a rate compatible with the holding time specified in the initial ISH PDU. Note that this is counter to the recommendation in the ATN Manual, Section A6.1.2.1.1, but is required in the absence of the air/ground operation of IDRP. In this situation, the periodic ISH PDUs function in the manner of the IDRP keep-alive functionality.

8.2 Requirements for Ground-Based Air/Ground BISs

Ground-based Air/Ground BISs are required to provide functionality complementing that described for the respective peer airborne BIS types in the preceding section.

Additionally, ground-based Air/Ground BISs are required to introduce routes into the ground-based ATN Internet based on information derived from the air/ground routing information exchange (i.e. the exchange of connectivity and domain identity information). These routes are required to be distributed among ground-based BISs by means of IDRP routing information exchanges.