ATNP/WG2/
WP/117
05 May 1995

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Washington 15.5.95-19.5.95

Meeting Application Specific Routing Policy Requirements in CNS/ATM-1 Package

Presented By Forrest Colliver

Prepared by Tony Whyman and Forrest Colliver

SUMMARY

The need to support application specific routing policy requirements has recently been required to be part of CNS/ATM-1 Package. This working paper discusses the background to this decision in the context of how work on CNS/ATM-1 Package has progressed, analyses the possible options, and presents the preferred option. Draft SARPs for the preferred option are also provided as an attachment.

TABLE OF CONTENTS

Disk Ref: w2wp117.doc

1. Introduction

1.1 Scope

This document provides a proposed ATN Internet solution for the Application Routing Policy Requirements that were endorsed by WG1 in Toulouse (20-24/3/95), and reviewed by the Paris CISEC Meeting (10-11/4/95). Readers unfamiliar with the recent work in ATNP/WG2 and the WG2 CISEC are recommended to read Appendix B first. This provides background material setting the contribution in context.

1.2 Purpose of Document

The Paris CISEC Meeting did not reach a definitive conclusion as to how to satisfy the Routing Policy requirements raised at the preceding WG1 Toulouse Meeting. However, it was agreed that the approach known to that meeting as “Option #2” was technically the best. This working paper elaborates option #2 and provides a proposed SARPs text.

1.3 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
3	ATNP/WG2-CISEC	Report of the first meeting of the CNS/ATM-1 Internet SARPs Editorial Committee (CISEC)

2. The Routing Policy Requirements

When the routing policy requirements endorsed by WG1 in Toulouse were discussed by the CISEC, 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.

2.1 Conveying Routing Policy Requirements in the CLNP Header

Two options were discussed by CISEC:

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 that had been 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 also 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.

2.2 Distribution of Route Information by IDRP

Provided that it is assumed that an aircraft is always an End Routing Domain, in the air to ground direction, the air-ground subnetworks over which each route is available are explicitly known to an airborne router. An ATN Router may therefore, when forwarding a CLNP packet to a ground router, satisfy the routing policy requirements expressed in the packet header through direct knowledge of available subnetworks. Although the ATN Manual did explicitly limit aircraft to being End Routing Domains, we may wish to enhance the ATN to support air to air communication and hence this assumption does become a restriction on future development. It was, though, accepted in order to proceed with the analysis, as no requirements currently exist for air-air communications.

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 Traffic 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 Traffic 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 seen as having the following deficiencies:

- an explosive growth in the amount of addressing information handled due to large numbers of alias addresses. The large numbers of alias addresses may not permit its use with COTS routers.

- inefficient propagation over air-ground data links as addressing information has only limited compressibility.

- asymmetry, given that it is only valid in the ground to air direction, and hence needs the assumption that the aircraft is an End Routing Domain. It cannot similarly be extended to permit user specified routing policy requirements to apply to any ATN subnetwork, and not just air-ground subnetworks.

Option #3 was seen as having similar deficiencies i.e.

- an explosive growth in the numbers of routes and routing updates that a router would have to handle.

- asymmetry, given that it is only valid in the ground to air direction, and hence needs the assumption that the aircraft is an End Routing Domain. It cannot similarly be extended to permit user specified routing policy requirements to apply to any ATN subnetwork, and not just air-ground subnetworks.

Option #2 was recognised as being the technically best option, albeit in need of validation. This is because:

- 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 symmetric in that it was equally valid in the air to ground direction and hence was extensible and would extend naturally to permit aircraft to be transit routing domains, and to allow routing policy requirements to be expressed for any ATN subnetwork, including those on the ground.

- The security information transferred by IDRP is readily compressible by the local reference compression algorithm.

2.2.1 Detailed Analysis

Option #3 extends the current (ATN Manual) approach for conveying the traffic types supported by a route, to also identify the air-ground subnetwork over which the route may be available. This is by defining a Security Registration identifier for each combination of Traffic Type and air-ground subnetwork. However, this has two clear drawbacks. This first is that the number of routes rapidly multiplies to a level which may well overwhelm the capacity of ATN Routers, both in terms of the number of routes that they can handle, and in the rate of route change. The second is that as this method of "labelling" a route is end-to-end; it can only be used when the origin of a route is in a Routing Domain adjacent to an air-ground subnetwork, as only then will the air-ground subnetworks over which the route is available, be known. Option #3 is therefore asymmetric in that it can only be used for routes advertised in the air to ground direction, but not for ground to air routes. This is because, in general, ground Routing Domains may not be adjacent to the air-ground subnetwork used for communication with a given aircraft. This approach inherently assumes that the aircraft is an End Routing Domain, which imposes a restriction on the future development of the ATN to support air-air routing.

The option #1 approach avoids the proliferation of routes that is characteristic of option #3 by encoding the routing policies satisfied by the route as alias addresses, and the actual air-ground subnetworks over which the route is available, as conventional RDIs in the RD_Path Path Attribute. However, this replaces the large number of routes by a large number of addresses, and is still an end-to-end solution with the same severe drawbacks as option #3. This is similarly because the alias addresses that identify the air-ground subnetworks over which the route is available, have to be generated at the point at which the route is originated, which must consequentially be adjacent to an air-ground subnetwork. Although the security path attribute is readily compressed and effectively removed by the local reference compression algorithm, addressing information is only subject to limited compression by the ICAO Address Compression Algorithm, and hence this option will also significantly increase the communications overhead for air-ground communications.

The option #2 approach avoids these problems by encoding the air-ground subnetwork(s) over which a route is available in the security related information that is defined by ISO 10747 as an optional component of the security path attribute. This security related information may be updated along a route, unlike the security registration identifier, which cannot be modified. Furthermore, different values of the security related information do not result in new route types to be supported, unlike different values of the security registration identifier, which always result in new route types. This approach therefore avoids the end-to-end nature that is a major weakness of the other options, by providing a mechanism to convey information about the air-ground subnetworks over which the route is available, that may be updated at any point on the route, and not just at its origin. Additionally, it does not result in a proliferation of routes, as the field used is not used to distinguish different routes.

However, a recognised problem with option #2, is that changes in the security related information of a route are not immediately notified to adjacent routers to which the route has already been advertised. This is because IDRP deliberately seeks to maintain a stable routing topology at the expense of occasional sub-optimal routing, by the specification of a "Hold Down Timer" that limits the rate of route re-advertisement. Only new routes and withdrawn routes are not subject to this timer. However, while this approach is acceptable for routing based on QoS, where "best efforts" is all that is guaranteed, it is not acceptable for satisfying strong policy requirements. Indeed, a defect appears to exist in the ISO standard with respect to the security related information and the Hold Down Timer. For example, the security related information may also be used to convey information on the protection offered by a route. If this protection is reduced, then the route's users should know about this immediately, so that they may choose an alternative route (if available), that does offer the required protection. Otherwise, data will be discarded at the point at which the protection level falls below that which the user requires. This is not an acceptable consequence of an optimisation.

The resolution to this defect is straightforward: it is to add an additional condition to the existing list in ISO 10747 under which the Hold Down Timer may be ignored i.e. when the security related information on a route changes.

Assuming that this fix is implemented, then option #2 provides a complete solution to the requirement that is both practicable and extensible. It may further be refined by moving the traffic type into the security related information and defining a single ATN Security Registration Identifier. This takes advantage of the IDRP defect resolution to further decrease the number of routes and route updates that ATN Routers have to support.

3. The Realisation of Option #2

3.1 Derived Routing Policy Requirements

Based on the operational requirements statement provided in appendix B, the following derived routing policy 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 required to provide each boundary router with information stating over which air/ground subnetworks a route is available.

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.

Note: 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.

WG2 has already decided that QoS requirements can only be met in the Package 1 timeframe by appropriate network design, and hence that no support for dynamic QoS selection will be provided. Attention is therefore given to meeting the routing policy requirements. These have an impact on the CLNP Header, which must convey such requirements, on IDRP, which needs to distribute the information that ATN Routers need to satisfy these requirements, and on the generation and use of the Forwarding Information Bases (FIBs).

3.2 Impact on the CLNP Header

The ATN Manual already specifies the use of the Security Parameter to convey information about the user data’s traffic type and optionally a Security Classification. This approach has been questioned, as discussed above, but the need now to convey additional information appears to justify the continued use of this parameter, especially as it has now been established that widely used COTS routers can be configured to be transparent to this parameter.

The impact on the CLNP Header of the need to meet the requirements recently endorsed by WG1 is therefore limited to defining an extension to this parameter to convey the additional policy requirements. A proposed extension is provided in Appendix A.

3.3 Impact on IDRP

There are three aspects to the impact on IDRP:

1. Information needs to be conveyed with each route on the traffic types supported by that route (this is an existing requirement and is currently met by defining a distinct Security Registration Identifier for each traffic type and using this to effectively distribute a different route for each traffic type).

2. Information needs to be conveyed with each route that identifies the air-ground subnetwork(s) over which the route is available. This is to enable routes to be chosen on the basis of over which air-ground subnetworks the route is available.

3. Forwarding Information Bases (FIBs) need to be built that enable the next hop to be chosen such that it follows a route that accepts an NPDU's traffic type and is in line with the routing policy requirements, as expressed in the NPDU's Security Parameter. Note that for Mode S and AMSS, the next hop choice will also need to identify a subnetwork connection appropriate to the "ITU Priority" indicated by the NPDU's priority parameter.

3.3.1 Updating the Security Related Information

This section now describes how option #2 is applied to distribute routing information in the ATN Internet in support of application specified routing policy requirements.

The security related information in the IDRP security path attribute can provide information on the traffic types supported by a route and the air-ground subnetworks over which the route is available. This information is not necessarily known at the point of origin of a route (e.g. a Ground Routing Domain) and will be added when the route is advertised over an air-ground subnetwork, or one that has traffic type restrictions. Therefore, when a route is first generated at its point of origin, it will need to have a security path attribute containing an ATN Security Registration Identifier, but the security related information will typically be empty.

Consider then the situation where a route is advertised through the ATN and is then advertised over an adjacency that is supported by a subnetwork connection over at least one air-ground subnetwork. It is proposed that the BIS that receives that route, then updates the security related information in that route's security path attribute to include the traffic types supported over that route, if any restrictions are in place, and an identifier for each air-ground subnetwork that supports this adjacency. The required information is then recorded in the route. This procedure can occur more than once and hence can be extended to record restrictions in the ground ATN Internet, should there be a requirement to do this.

For example, Figure 1 illustrates an example ATN topology. A route advertised by the aircraft (RD M.1) to the Ground Router RD A.2 will initially have an empty security related information field. This will be updated by RD A.2 to include the identifier for AMSS. When this route is then advertised to RD T.1, this Router will be able to determine from the security related information inserted by RD A.2, that the route has no traffic type restrictions and that it passes over AMSS.

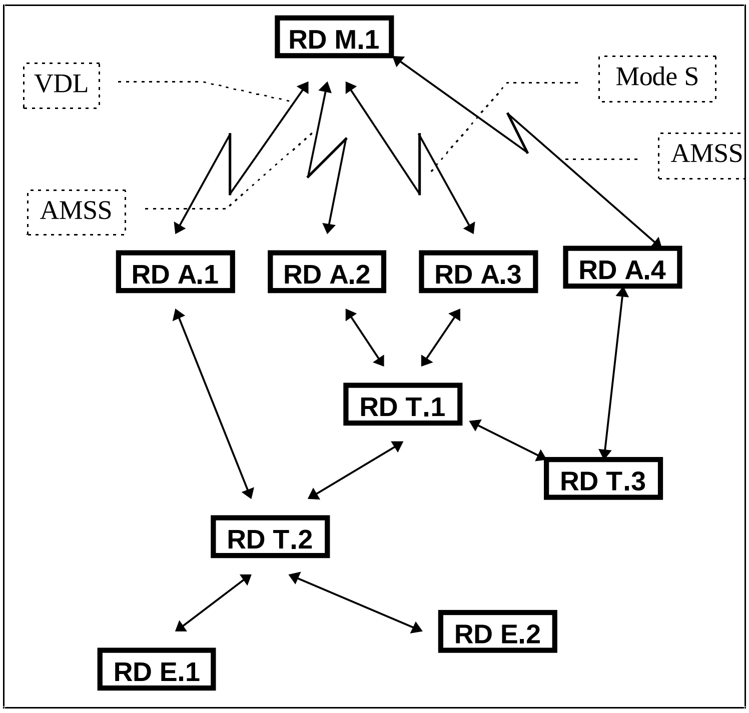

Figure 1 Example ATN Topology

RD T.1 may also receive a route to the same aircraft from RD A.3. This will indicate in the security related information inserted by RD A.3, that the route passes over Mode S and will typically be restricted to Operational Traffic. RD T.1 cannot choose between such routes and hence use only one route when building its FIBs, as each route satisfies a different set of policies and both must be used to build the FIBs. This situation is recognised by ISO 10747, which permits routes to the same destination, but which differ in their security related information, to exist in the same loc-RIB and hence both be used for building FIBs. Note that if two routes have identical security related information then it is correct and proper in this situation for the BIS to choose only one of these as the selected route, and to copy that one alone into the loc-RIB.

However, while RD T.1 may advertise both the routes discussed in the example above, on to RD T.2 and RD T.3, this is undesirable in that two routes now need to be maintained when only one is necessary. Instead, before copying such routes from the loc-RIB to an adj-RIB-out, RD T.1 should aggregate these routes into a single route. In practice this means merging their RD-Path and their security related information. The result would be a single route with security related information that identifies a route available for all traffic types over both AMSS and Mode S.

This approach is symmetric, and works identically in support of air to ground routing and ground to air routing. For example, a route generated by RD E.1 will have an empty security related information field until it is received by RD M.1 when it will be updated to reflect the air-ground subnetwork(s) supporting the adjacency with the ground router. The route then includes the information necessary for the correct building of RD M.1's FIBs.

3.4 Impact of the FIB Structure and Usage

The actual FIB structures that a router uses to forward CLNP NPDUs will always be implementation dependent. However, it possible to define an appropriate FIB model and to use this to show how the FIBs may be built.

The model chosen for this description is that a distinct FIB is created for each combination of Traffic Type and Routing Policy Requests that may occur in the CLNP Security

Parameter. Each FIB then consists of a list of NSAP Address Prefixes, each paired with an identified next hop router described by the subnetwork that is to be used to forward the NPDU, and the address of the next hop router on that subnetwork.

3.4.1 The Forwarding Procedure

The forwarding procedure for each CLNP packet is then as follows:

1. The FIB associated with the traffic type and routing policy requirement in the NPDU's security parameter is chosen.

2. The NSAP Address Prefix that provides the longest match with the NPDU's destination NSAP Address is chosen and the corresponding next hop identified.

3. When the subnetwork is connectionless, the packet is queued for transfer over that subnetwork.

4. When the next hop subnetwork is connection mode, the NPDU will be queued for transmission over an appropriate subnetwork connection with the next hop router. If this is a Mode S or AMSS subnetwork, then a subnetwork connection must be chosen such that it has a connection priority that matches the "ITU Priority" encoded in the NPDU's priority parameter.

Note. This ITU Priority could be just as readily encoded in the CLNP security parameter therefore enabling the NPDU priority parameter to be used for signalling the ATN Internet priority of the NPDU, which is not necessarily the same as the ITU Priority. ITU Priority is really about precedence and pre-emption in air-ground subnetworks, while CLNP priority should be used to ensure a higher service availability to "higher priority" applications. WG2 should consider this possibility i.e. expanding the traffic type information to include ITU Priority as a sub-parameter.

3.4.2 Building the Forwarding Information Bases

This form of FIB structure may be readily built using the routes in the loc-RIB that includes a security path attribute with the ATN Security Registration Identifier in its identifying RIB-Att. The procedure for building each such FIB is:

1. For each distinct NSAP Address Prefix in this loc-RIB, all routes including that NSAP Address Prefix in their NLRI are identified.

2. The route that best meets the Routing Policy Requirement associated with the FIB, whilst supporting the Traffic Type that is associated with the FIB, is chosen.

3. The subnetwork that support the adjacency with the router that had advertised that route are determined and, if more than one, the subnetwork that best meets the Routing Policy Requirement, whilst supporting the Traffic Type that is associated with the FIB, is chosen. This subnetwork and the router's address on that subnetwork are entered into the FIB as the next hop information paired with this NSAP Address Prefix.

Note 1. ATN Routers may also support a loc-RIB that corresponds to routing information distributed under the empty (default) RIB_Att. This will not be used to generate entries for the above FIB structure as such routes do not include the information necessary to satisfy the routing policy requirements. However, they may be used to build a FIB that is used for forwarding CLNP packets that do not have a security parameter in their header.

Note 2. There are also special cases in that a route with an empty security related information in its security path attribute provides equivalent information to a route advertised with the default RIB_Att. Similar, a CLNP packet that identifies a traffic type of General

Communications and no routing policy requirements in its security parameter is equivalent to a CLNP packet with no security parameter.

3.4.3 Conclusion

As may be seen, provided that the identified defect in ISO 10747 is rectified, the "option #2" approach will distribute the information necessary to meet strong policy requirements efficiently, and in a timely manner, whilst enabling the efficient handling of routing policy requests and respecting traffic type restrictions. It is therefore recommended for the CNS/ATM-1 Package SARPs following its successful validation.

It should be noted that this approach does not impact the optional non-use of IDRP for package 1. As the security related information is updated by the receiving router, when a ground or airborne router generates the routes that it assumes would have been advertised to it by the adjacent airborne or ground router, it simply adds the security related information that it would have added anyway.

Proposed draft SARPs incorporating the revised use of IDRP may be found in Appendix A.

Appendix A Proposed Draft SARPs

1. 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 to 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 C5h.

The value component of the CLNP Options Security Parameter shall be encoded 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 2, and defined below.

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

Figure 2 The ATN Security Label

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

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.

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 Authority. 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, ...}.

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.

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 and Routing Policy Requirements, if any, applicable to the transfer of the user data through the ATN.

2. The Security Classification

When no traffic type is identified then General Communications shall be assumed, with a routing policy requirement of “no preference”. When no classification is specified then “unclassified” shall be assumed.

1.4.1 Encoding of the Security Information Field.

The Security Information Field shall comprise zero, one or more 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 3, and defined below:

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

Figure 3 Security Tag Set Format

Note: this format has been chosen to provide for an extensible type-length-value encoding method for security related information placed in the CLNP Header under rules specified by the ATN Security Authority.

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.

1.4.1.2 Security Tag Set Name

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

1.4.1.3 Tag Set Length

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

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.

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

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

Note: This Tag Set is used to identify the traffic type of the data, whether it is for ATC or airline communications, and, for operational communications, any routing policy requirements that apply..

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

Traffic Type	Category	Security Tag Value	Semantics
ATN Operational Communications	Air Traffic Service Communications (ATSC)	000 00001	No Traffic Type Policy Preference
		000 00010	Traffic only follows ATSC route(s).
		000 00011	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)	001 00001	No Traffic Type Policy Preference.
		001 00010	Route Traffic only via Gatelink.
		001 00011	Route Traffic only via VHF Data Link.
		001 00100	Route Traffic only via Satellite Data Link.
		001 00101	Route Traffic only via HF Data Link.
		001 00110	Route Traffic only via Mode S Data Link.
		001 00111	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link.
		001 01000	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then Satellite.
		001 01001	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then HF Data Link, then Satellite Data Link.
ATN Administrative Communications		001 10000	
General Communications		010 00000	
ATN Systems Management Communications		011 00000	

1.4.3 Encoding of the Tag Set for Security Classification

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

Note: the purpose of this field is to permit the later extension of the ATN to handle classified data.

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

2. The IDRP Security Path Attribute and Support Functions

2.1 RIB_ATT Support

A CNS/ATM-1 Package 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 Registration Identifier*. When the router supports classified data then the Security Classification Security Tag shall also be supported.

2.2 Use of the Security Path Attribute

ATN Routers supporting inter-domain routing shall support the IDRP Security Path Attribute with a Security Registration Identifier set to the value defined in 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 1.4.1. The following Security Tag Sets shall be supported:

1. The Security Classification, as defined in 1.4.3, when the router supports classified data.

2. The Air-Ground Subnetwork type, as defined in 2.3.

When a route is available over more than one air-ground subnetwork type, then a separate Security Tag set shall be encoded into this field to identify each air-ground subnetwork that may support the route. When an air-ground subnetwork is restricted to carrying data of only certain traffic types, then the Security Tag set that identifies that air-ground subnetwork shall enumerate the Traffic Types that may pass over that subnetwork.

Note. The Security Tag set format defined for use with CLNP has been adopted here as a convenient method for the extensible encoding of security related information.

2.3 Encoding of the Air/Ground Subnetwork Type

The Tag Set Name shall be set to [0000 0101], and the Security Tag is always two octets in length.

The first (lowest numbered) octet of the Security Tag shall indicate an air-ground subnetwork over which the route may be available according to the following table:

Subnetwork Type	Security Tag (First Octet)
Mode S	0000 0001
VDL	0000 0010
AMSS	0000 0011
Gatelink	0000 0100
HF	0000 0101

The second (highest numbered) octet of the Security Tag shall indicate the Traffic Types allowed to pass over the air-ground subnetwork identified in the first octet. This octet shall comprise a bit map, where each bit corresponds to a different traffic type. A value of FFh shall be used to imply no restrictions. The assignment of bits to traffic type shall be according to the following table, where bit 0 is the low order bit:

Bit Number	Traffic Type
0	ATN Operational Communications (ATC)
1	ATN Operational Communications (AOC)
2	ATN Administrative Communications
3	General Communications
4	ATN Systems Management

The semantics of bits 5 to 7 are reserved for future use and shall always be set to one.

2.4 Update of Security Information

When a Route is:

a) received over an adjacency supported by one or more air-ground subnetworks, and

b) contains a Security Path Attribute and

c) which has the ATN Security Policy Identifier, as the Security Path Attribute's Security Registration Identifier then,

the Security Path Attribute's Security Information shall be updated as follows:

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

2. For each such air-ground subnetwork Security Tag, if ITU requirements or local policies restrict the Traffic Types that may pass over that subnetwork then the second octet of the security tag shall be modified to set to zero the bits corresponding to each traffic type not supported by that air-ground subnetwork.

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.

2.5 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.

2.6 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.

Note: the purpose of this statement is to permit, within the limitations imposed by IDRP, the existance in the loc-RIB of multiple routes to the same aircraft which differ only in the security related information.

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 or equal 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.

2.7 Route Aggregation

The aggregation rules for security path attributes that include the ATN Security Registration identifier shall be:

1. The aggregated security path attribute shall comprise each air-ground subnetwork security tag contained in the security path attribute of the component routes.

2. When an air-ground subnetwork security tag for the same air-ground subnetwork occurs in both component routes, then these shall be combined by a logical “OR” of the second octet of the security tags. Only a single an air-ground subnetwork security tag for each distinct air-ground subnetwork shall be present in the aggregated route.

3. When a security classification security tag set occurs in component routes, then the aggregated route shall include a security classification security tag set identifying the lowest classification of the component routes, otherwise the aggregated route shall not contain a security classification security tag set.

Appendix B - Background

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. Package 1 Application Support Objectives

ATNP/WG1 considered the above decision at its first meeting in San Diego (October 1994) 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.

3. Package 1 Implementation Objectives

3.1 Explicitly-Stated Objectives

The following is a summary of a common set of explicitly-stated goals and associated statements of goal objectives, that evolved from a comparative analysis of the various proposals made within the ATN Panel and its Working Groups during the past year:

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;

Optimisation 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
Minimisation of deviation from particular ATN routing policy solutions, on which procurements

Procurements	in several States and Organisations have been respectively based.

3.2 Implicit Objectives

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

a) Package 1 validation must be completed prior to June 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.

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, while meeting the implementation objectives. 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.

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.

A summary of these "Routing Policy Requirerments" was given in the March 1995 WG1 Flimsy 3, and 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.

5.1 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").

5.2 Traffic Type Policy Requirements

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

I. ATN Operational Communications

A. Air Traffic Service Communications (ATSC)

1. No Traffic Type Policy Preference.

2. Traffic only follows ATSC route(s).

3. 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)

1. No Traffic Type Policy Preference.

2. Route Traffic only via Gatelink.

3. Route Traffic only via VHF Data Link.

4. Route Traffic only via Satellite Data Link.

5. Route Traffic only via HF Data Link.

6. Route Traffic only via Mode S Data Link.

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

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

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

II. ATN Administrative Communications

III. General Communications

IV. 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.