ATNP/WG2-WP/327

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

Working Group 2

Munich, Germany 24 - 28 June 1996

The AOC Traffic Type and Strong QoS

Presented by HENK J. HOF

Prepared by Tony Whyman

SUMMARY

This Working Paper provides proposals on how to handle the requirement expressed by WG3 on support of strong separation between AOC and ATSC Traffic.

DOCUMENT CONTROL LOG

SECTION	DATE	REV. NO.	REASON FOR CHANGE OR REFERENCE TO CHANGE
	24-May-96	Issue 1.0	

TABLE OF CONTENTS

1. Introduction

1.1 Background

In Flimsy #8 generated from the WG3 Brussels meeting, the requirement was stated that:

Strong QOS shall be applied in support of Operational Traffic Type and ATSC Traffic Category. That is, an NPDU marked ATSC Traffic Type without an ATSC route shall be discarded. No AOC Traffic shall traverse an ATC route unless that route is marked for both Categories.

The flimsy further went on to say that "WG3 believes Sub-Volume 5, 3.2.1.2.3 currently supports this requirement." However, the requirement as stated above is not currently supported by the draft ATN Internet SARPs.

1.2 Scope

This paper discusses the implications of the above requirement and how it may be realised in the draft ATN Internet SARPs.

2. Summary

WG3 is wrong in its assumption that AOC is currently recognised as a distinct category of traffic as regards routing in the ground ATN, for either air/ground or ground/ground communications. Change is therefore necessary if this requirement is to be met.

To support such a requirement, it appears appropriate to extend the current set of security tags recognised by IDRP, to include a tag that identifies a route as being approved for AOC use, and a tag that identifies a route as being approved for ATN Administrative Communications. This second tag is necessary if all Traffic Types are to be properly distinguished. Appropriate policy rules also need to be formulated making use of the new security tags.

An alternative and possibily simpler approach has been suggested and this was investigated. This would be to simply change the policy rules without adding additional information to routes. However, it does not appear to be viable. Whilst it is possible to define a policy that recognises a route as being ATSC approved or approved for all other Traffic Types (except for ATSC), this effectively results in a partitioned ATN which loses the benefits of a single network, supporting all types of traffic.

The proposed changes are given below in section 5. These are a relatively straightforward extension of the current routing strategy and represent a minimum change approach. If WG3 believes that its requirement has to be met, then the proposed changes are recommended.

3. Requirement Analysis

3.1 Route Categories

The WG3 requirement is about marking routes with the Traffic Types that they support. The ATN Internet SARPs currently specify that the Security Information contained within an IDRP Security Path Attribute is used to convey information about the type of traffic that a route can carry and the Air/Ground Subnetworks that the route may pass over, and this is done through two Security Tags:

- The Air/Ground Subnetwork Security Tag

- The ATSC Class Security Tag.

3.1.1 The Air/Ground Subnetwork Security Tag

This tag is added to a route's security path information, whenever a route passes over an Air/Ground Data Link. The tag records the type of air/ground data link (e.g. Mode S, AMSS, etc.) and the traffic types of data that can pass over the data link (e.g. ATSC, AOC, etc.). If more than one type of Air/Ground Data Link concurrently supports access to the same aircraft, then a tag is added for each such data link.

This Security Tag is used:

a) to support the AOC user routing policy requests. These allow an application to specify which Air/Ground subnetwork type, out of those available, is used to convey the data, between air and ground. Such requests are also handled in a "strong" manner. That is, if the requested Air/Ground subnetwork type is not available, then the data is discarded.

b) to avoid data of a given traffic type and address to an airborne system, being routed to an Air/Ground Data Link that does not support the uplink of data of that type.

This Security Tag will only be found in routes to aircraft. It is never present in routes to ground destinations except in an Airborne Router. This includes routes that will be used by data that originated in an aircraft, has been downlinked to an Air/Ground Router, and is now in the ground portion of its journey. It cannot therefore be used as a general mechanism for determining the traffic types of data that may pass over a given route.

3.1.2 The ATSC Class Security Tag

This tag is added to a route, when that route has been approved for ATSC data, and, additionally, identifies the ATSC Class supported. The tag is added when a route is created. It can be removed, or the ATSC Class reduced, but it can never be added to an existing route, nor can the ATSC Class be increased. The actual encoding of the ATSC Class is a bit-map, so that when routes to the same destination are aggregated, all supported ATSC Classes can be identified in the aggregated route.

This tag is used to support ATSC User specified routing policy requests. When data has a traffic type of ATSC it can only be routed over an ATSC approved route, and this requirement is met by only forwarding such data over a route with an ATSC Class Security Tag present. Furthermore, when more than one possible route is available, the route is chosen that either:

a) Supports the same ATSC Class as indicated in the data's security label; or, if no such route can be found

b) Supports a higher ATSC Class ; or, if no such route can be found

c) Supports a lower ATSC Class.

3.2 Strong QoS and ATSC Data

The requirement in 1.1 and in respect of ATSC Data, is met through the implementation of the ATSC Class Security Tag. This enables a route to be marked for ATSC data, and the forwarding rules are specified such that ATSC data is only forwarded over such a route.

3.3 Strong QoS and AOC Data

Strong QoS routing principles are applied for AOC data in respect of Air/Ground routing in that AOC data will only use the Air/Ground Data Links that are available for AOC data and when permitted by the originator. However, this does not extend into the ground environment, where AOC data may follow any available route to a ground destination, including those with an ATSC Class Security Tag.

4. Meeting the Requirement

4.1 Strategy #1: Revised Routing Policy

A simple strategy for meeting the requirement that "No AOC Traffic shall traverse an ATC route unless that route is marked for both Categories", would appear to be to specify a routing policy that the presence of an ATSC Security Tag in a route implies that the route is not available to AOC data, and vice versa i.e. the non-presence of an ATSC Class Security Tag implies that the route is available for AOC data.

However, the ATSC Class Security Tag is not, in IDRP terms, a distinguishing path attribute, and an IDRP route with an ATSC Class Security Tag belongs to the same RIB_Att as a route with a Security Path Attribute but no ATSC Class Security Tag. This is significant, because IDRP does not permit two routes to the same destination, to be advertised between the same pair of BISs unless those routes belong to different RIB_Atts. Hence, if the above strategy is undertaken, it implies the constraint that a router can never simultaneously advertise to an adjacent BIS, both an ATSC and an AOC route to the same destination.

This would be a serious constraint on the design of the ground ATN, but, for air/ground routing, would demand that Air/Ground Routers support either ATSC or AOC but never both. These are significant and potentially expensive constraints, and appear to go against one of the basic objectives of the ATN, that it would be concurrently useable by more than one type of traffic. Indeed, if such constraints were accepted, then there would seem little point in having typed traffic as there would be separate ATNs for each supported Traffic Type.

4.2 Strategy #2: A New Security Tag

The problem with the above approach is that it is trying to gain implicit information from the presence/non-presence of the ATSC Class Security Tag. A better strategy would therefore appear to be to add explicit information on whether a route is approved for AOC traffic, into the route's security information. This may be achieved by defining a new Security Tag for AOC Traffic.

If an AOC Security Tag was introduced, then this can be given the semantics that, when it is present, the route is available for AOC data, and when it is not present, the route is not available for AOC data. When both the AOC and ATSC Class Security Tags are present in a route, then it is available for both types of traffic.

It is then possible to define policies such that AOC Traffic is only forwarded over routes that contain the AOC Security Tag. The WG3 requirement is thus met, without the constraints inherent in the first approach. It is a simple extension to the current approach and is therefore to be recommended.

However, traffic types of ATN Administrative Communications and ATN Systems Management Communications are also defined. It is intended that the latter type of traffic should be able to pass over any route. However, the former is a distinct type of traffic that may sometime share routes with ATSC and AOC, and sometimes may have its own routes. A similar mechanism is therefore also needed for identifying routes available for ATN Administrative Communications.

5. Proposed SARPs Changes

The following changes to the draft ATN SARPs are necessary to support strategy #2:

- Specification of the AOC Security Tag
- Rules for Updating/Aggregating the AOC Security Tag
- Forwarding rules referencing the AOC Security Tag.

5.1 Specification of the New Security Tags

5.1.1 Changes to 8.3.1.2

Add new list item (c): “The AOC Security Tag”.

Add new list item (d): “The ATN Administrative Communications Security Tag”.

Add new paragraphs at end of section:

“At most one AOC Security Tag Set shall be present in a route’s Security Path Attribute.

At most one ATN Administrative Communications Security Tag shall be present in a route’s Security Path Attribute.”

5.1.2 New Section 8.3.1.3.3 “Encoding of the AOC Security Tag

The Tag Set Name shall be set to [0000 0111] and the Security Tag always has a length of zero. i.e. there are no parameters to this Security Tag.

Note: When this security tag is present, it implies that the route is available for AOC Traffic. When this security tag is not present, it implies that the route is not available for AOC Traffic.

Data with a Traffic Type of ATN Operational Communications - Aeronautical Operational Control (AOC) shall only be forwarded over a route which contains an AOC Security Tag in its Security Information.

5.2 Rules for Updating the New Security Tags

5.2.1 New Section 8.3.1.3.4 “Encoding of the ATN Administrative Communications Security Tag

The Tag Set Name shall be set to **[0000 1000]** and the Security Tag always has a length of zero. i.e. there are no parameters to this Security Tag.

Note: When this security tag is present, it implies that the route is available for ATN Administrative Traffic. When this security tag is not present, it implies that the route is not available for ATN Administrative Traffic.

Data with a Traffic Type of ATN Administrative Communications shall only be forwarded over a route which contains an ATN Administrative Communications Security Tag in its Security Information.

5.2.2 New Section 8.3.1.4.4 The AOC Security Tag

When a route is advertised to an adjacent BIS, then:

a) If the route has been originated by an Air/Ground Router according to the procedures for the optional non-use of IDRP (as specified in 3.5.2.11), and the adjacency with the Airborne Router is over an air/ground data link approved for AOC use, then an AOC Security Tag shall be added to the route.

b) If the route had been received from an Airborne Router by an Air/Ground Router, over an air/ground data link approved for AOC use, then an AOC Security Tag shall be added, if one is not already present.

c) If the route has been originated locally (i.e. within the same Routing Domain), by a Router other than an Airborne router, and

- if the route is to be advertised to an adjacent BIS over an adjacency supported by one or more subnetworks approved for AOC traffic, then

- an AOC security tag shall be added to the route.

Note. - In the case of an Airborne Router, the AOC Security Tag is inserted by the Air/Ground Router (see case (b) above), and this avoids an Airborne Router having to know which air/ground data links are approved for AOC use.

d) if the route has been received from another BIS and

- the route is to be advertised to an adjacent BIS over an adjacency supported by subnetworks that are not approved for AOC Traffic, then

- the AOC security tag shall be removed from the route before it is advertised to the adjacent BIS.

An AOC Security Tag shall not be present in a route's security information, if an Air/Ground Subnetwork Security Tag is also present indicating that the Air/Ground Subnetwork does not support AOC Traffic.

5.2.3 New Section 8.3.1.4.4 The ATN Administrative Communications Security Tag

When a route is advertised to an adjacent BIS, then:

a) If the route has been originated by an Air/Ground Router according to the procedures for the optional non-use of IDRP (as specified in 3.5.2.11), and the adjacency with the Airborne Router is over an air/ground data link approved for ATN Administrative Communications use, then an ATN Administrative Communications Security Tag shall be added to the route.

b) If the route had been received from an Airborne Router by an Air/Ground Router, over an air/ground data link approved for ATN Administrative Communications use, then an ATN Administrative Communications Security Tag shall be added, if one is not already present.

c) If the route has been originated locally (i.e. within the same Routing Domain), by a Router other than an Airborne router, and

- if the route is to be advertised to an adjacent BIS over an adjacency supported by one or more subnetworks approved for ATN Administrative Communications traffic, then

- an ATN Administrative Communications security tag shall be added to the route.

Note. - In the case of an Airborne Router, the ATN Administrative Communications Security Tag is inserted by the Air/Ground Router (see case (b) above), and this avoids an Airborne Router having to know which air/ground data links are approved for ATN Administrative Communications use.

d) if the route has been received from another BIS and

- the route is to be advertised to an adjacent BIS over an adjacency supported by subnetworks that are not approved for ATN Administrative Communications Traffic, then

- the ATN Administrative Communications security tag shall be removed from the route before it is advertised to the adjacent BIS.

An ATN Administrative Communications Security Tag shall not be present in a route's security information, if an Air/Ground Subnetwork Security Tag is also present indicating that the Air/Ground Subnetwork does not support ATN Administrative Communications Traffic.

5.3 Aggregation Rule for the New Security Tags

Add new list items (e) and (f) to 8.3.1.6.3, as follows:

e) If the NLRI of the component routes is not identical, then when an AOC security tag occurs in all component routes, the aggregated route shall contain an AOC security tag. If an AOC security tag is not present in at least one component route then the aggregated route shall not contain an AOC security tag. Otherwise, if the NLRI is identiical then when an AOC security tag occurs in any of the component routes, the aggregated route shall contain an AOC security tag.

f) If the NLRI of the component routes is not identical, then when an ATN Administrative Communications security tag occurs in all component routes, the aggregated route shall contain an ATN Administrative Communications security tag. If an ATN Administrative Communications security tag is not present in at least one component route then the aggregated route shall not contain an ATN Administrative Communications security tag. Otherwise, if the NLRI is identiical then when an ATN Administrative Communications security tag occurs in any of the component routes, the aggregated route shall contain an ATN Administrative Communications security tag.

5.4 Updated Forwarding Rules for AOC and ATN Administrative Communications

3.2.1.2.3 ATN Operational Communications - AOC Traffic Type

3.2.1.2.3.1 No Routing Policy Specified

Note 1.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 001 00001.

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

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Operational Communications - Aeronautical Operational Control, and

c) no Routing Policy Specified,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises an AOC Security Tag, and :

i. an Air/Ground Subnetwork Security Tag that has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, or

ii. no Air/Ground Subnetwork Security Tag.

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

3.2.1.2.3.2 Air/Ground Subnetwork Type Specified

Note 1.— This case corresponds to Traffic Type and Associated Routing Policy Security Tag values 001 00010 through to 001 00110, inclusive.

Note 2.— The Air/Ground Subnetworks that may be so specified are: Gatelink, VDL, AMSS, HF and Mode S.

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

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Operational Communications - Aeronautical Operational Control, and

c) a requirement to route traffic only via a specific Air/Ground Subnetwork only,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises an AOC Security Tag and either

i. an Air/Ground Subnetwork Security Tag that indicates that the route passes over that Air/Ground Subnetwork and has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, or,

ii. no Air/Ground Subnetwork Security Tag.

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

3.2.1.2.3.3 Air/Ground Subnetwork Order of Preference Specified

Note 1.— This case corresponds to Traffic Type and Associated Routing Policy Security Tag values 001 00111 through to 001 01001, inclusive.

Note 2.— The Air/Ground Subnetworks for which an order of preference may be so specified are: Gatelink, VDL, AMSS, HF and Mode S.

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

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Operational Communications - Aeronautical Operational Control, and

c) a requirement to route traffic only via certain Air/Ground Subnetworks and with a specified order of preference,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises an AOC Security Tag, and:

i) an Air/Ground Subnetwork Security Tag that indicates that the route passes over the first preference Air/Ground Subnetwork and has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, if present, or

ii) an Air/Ground Subnetwork Security Tag that indicates that the route passes over the second preference Air/Ground Subnetwork and has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, if present, and so on until a suitable route is found or no further preferences are specified, or

iii) no Air/Ground Subnetwork Security Tag.

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

If after applying the above procedures, a more specific route is available to the NPDU's destination, but

1) the route has an Air/Ground Subnetwork Security Tag that indicates that the route passes over a lower preference Air/Ground Subnetwork while

2) having "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, then

3) the more specific route shall be selected in preference to the less specific route.

Note 3.— The purpose of this requirement is to ensure that the NPDU is not forced to visit a default route provider only to find that a higher preference route does not actually exist to the NPDU's destination.

3.2.1.2.4 ATN Administrative Communications Traffic Type

Note 1.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 001 10000.

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

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Administrative Communications,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises an ATN Administrative Communications Security Tag, and:

i) either an Air/Ground Subnetwork Security Tag that has "ATN Administrative Communications" in its set of permissible Traffic Types, or

ii) no Air/Ground Subnetwork Security Tag.

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