EACI

ATN INTERNET PROJECT (ATNIP)

Disposition of Deleted Requirements in Appendix 6 of the ATN Manual

ATNIP Ref. : DED1/EAS3/STA_ATNP/DCO/34

Author : Tony Whyman

Rev. No. : Issue 1.0

Date : 12-Jun-95

DOCUMENT CONTROL LOG

SECTION	DATE	REV. NO.	REASON FOR CHANGE OR REFERENCE TO CHANGE
	12-Jun-95	Issue 1.0	

TABLE OF CONTENTS

1. Introduction

1.1 Scope

This document is the result of editing work on appendix 6 of the ATN draft SARPs and provides an editor's report listing out all deleted requirements, recommendations and notes.

1.2 Purpose of Document

This document provides traceability of requirements deleted due to decisions made by WG2, the WG2/CISEC and in the course of the editorial process. It is to be used during the review of the revised appendix and as input to the update of the ATN Requirements Database.

2. Deleted Requirements Report

3. Appendix 6 ATN Routing Specification

3.1 A6.1 Provisions for Use of Mobile Subnetworks

Editor's Note: this note seemed to contradict the requrement that preceded it. See note 3 of A6.5.2 for an improved phrasing.

Note. — The alternative mode of operation may also be provided for each subnetwork type..

Editor's Note: Except where indicated, the remaining text has been deleted as it duplicated similar text.

3.1.1 A6.1.1 ISO 8208 Subnetworks that do not Provide Information on Subnetwork Connectivity

Note.— With this subnetwork type, BIS-BIS communication is always air-initiated.

3.1.1.1 A6.1.1.1 Airborne BIS Provisions

3.1.1.1.1 A6.1.1.1.1 Connection Establishment

Whenever an ISO 9542 ISH PDU is received, the Record Configuration function shall be invoked; the routing information necessary for NPDUs to be sent over the subnetwork connection to the indicated NET shall be written into the Forwarding Information Base for use by ISO 8473. A Systems Management Notification shall also be generated to report the arrival of the ISH PDU to local Systems Management.

When the arrival of the ISH PDU is reported to local Systems Management, if a BIS-BIS connection currently exists with the NET given by the ISH PDU, then no further action shall be taken. Otherwise, the NET received shall be appended to the externalBISNeighbor attribute of the BIS's idrpConfig Managed Object, if not already present, and an **adjacentBIS** Managed Object created for the ground BIS identified by this NET, if one does not already exist. An idrp "start event" action shall then be invoked to start the BIS-BIS connection according to ISO/IEC 10747.

Recommendation.— *When a BIS-BIS connection has been established, the periodic transmission of ISH PDUs should be suppressed.*

3.1.1.1.2 A6.1.1.1.3 Call Termination

Whenever a subnetwork connection is terminated, either by the network provider, or by the called DTE, then the back off procedure specified in 6.1.1.1.2 shall be applied. Furthermore, a Systems Management Notification shall be provided to local Systems Management in order to report loss of the subnetwork connection. Forwarding Information associated with the subnetwork connection shall be removed from the Forwarding Information Base.

When local Systems Management terminates a subnetwork connection, or receives a notification reporting loss of the subnetwork connection, if there are no alternative subnetwork connections with the ground BIS associated with that subnetwork connection, then an IDRP "stop event" shall be invoked to terminate the BIS-BIS connection with that ground BIS. If the BIS-BIS connection is not re-established within a period configurable from 1 minute to 300 minutes, or when the resources are required for other use, then the **adjacentBIS** Managed Object associated with the ground BIS shall be deleted, and the ground BIS's NET removed from the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object. When a subnetwork connection is terminated by local systems management, any associated FIB entries shall be removed.

When the subnetwork does not provide a clear indication when the aircraft goes out of range of the mobile subnetwork, or when other communication failure occurs, the airborne BIS shall maintain a "watchdog" timer for each virtual circuit and clear each virtual circuit once activity has ceased for a configurable period (1 - 600 seconds).

Note.— The airborne BIS maintains a "watch-dog" timer for each virtual circuit to detect the event of an aircraft leaving coverage (or other communication failure), if such an event detection is not provided by the subnetwork. This "watch-dog" timer is configurable from 1 to 600 seconds.

3.1.1.2 A6.1.1.2 Ground BIS Provisions

3.1.1.2.1 A6.1.1.2.1 Connection Establishment

A ground BIS shall be available to receive Call Indications on all air-ground subnetworks that do not provide information on subnetwork connectivity to which it has active attachments.

the call is unacceptable then it shall be rejected using a Clear Indication. Otherwise, the call shall be accepted using a Call Accept.

A Ground BIS shall implement the ISO 9542 "Configuration Information". Whenever a Call is accepted, the ISO 9542 Report Configuration Function shall be invoked to send an ISH PDU over this subnetwork connection. The ISH PDU shall include the NET of the Ground BIS’s IDRP Network Entity

Whenever an ISO 9542 ISH PDU is received, the Record Configuration function shall be invoked; the routing information necessary for NPDUs to be sent over the subnetwork connection to the indicated NET shall be written into the Forwarding Information Base for use by ISO 8473. A Systems Management Notification shall also be generated to report the arrival of the ISH PDU to local Systems Management.

When the arrival of the ISH PDU is reported to local Systems Management, then if a BIS-BIS connection currently exists with the NET given by the ISH PDU, then no further action shall be taken.

Note 2.— The acceptability of a BIS-BIS connection with the Airborne BIS is identified by the received NET, and for the traffic type indicated, may be determined using procedures outside of the scope of this specification.

If a BIS-BIS connection is unacceptable, then a Clear Indication shall be generated to terminate the subnetwork connection. Forwarding Information associated with the subnetwork connection shall be removed from the Forwarding Information Base.

If a BIS-BIS connection is acceptable, then the NET received shall be written to the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object, if not already present, and an **adjacentBIS** Managed Object created for the airborne BIS identified by this NET, if one does not already exist. An idrp "start event" action shall then be invoked to start the BIS-BIS connection according to ISO/IEC 10747.

3.1.1.2.2 A6.1.1.2.2 Connection Termination

Whenever a subnetwork connection is terminated, either by the network provider, or by the called DTE, then a Systems Management Notification shall be provided to local Systems Management in order to report loss of the subnetwork connection.

Forwarding Information associated with the subnetwork connection shall be removed from the Forwarding Information Base.

When local Systems Management receives a notification reporting loss of the subnetwork connection, if there are no alternative subnetwork connections with the airborne BIS associated with that subnetwork connection, then an IDRP "stop event" shall be invoked to terminate the BIS-BIS connection with that airborne BIS. If the BIS-BIS connection is not re-established within a period configurable from 1 minute to 300 minutes, or when the resources are required for other use, then the **adjacentBIS** Managed Object associated with the airborne BIS shall be deleted, and the airborne BIS's NET removed from the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object.

3.1.2 A6.1.2 ISO 8208 Subnetworks that Provide Connectivity Information

Note.— With this subnetwork type, BIS-BIS communication may be specified as either ground initiated or air initiated. When the subnetwork is specified as ground-initiated, then the ground BIS is the initiating BIS and the airborne BIS is the responding BIS. When the subnetwork is specified as air-initiated, then the airborne BIS is the initiating BIS and the ground BIS is the responding BIS.

3.1.2.1 A6.1.2.1 Responding BIS Provisions

3.1.2.1.1 A6.1.2.1.1 Connection Establishment

A responding BIS shall be available to receive Call Indications from the subnetwork.

Note 1.— Whenever such a Call Indication is received, the responding BIS may validate the calling DTE and determine the acceptability of the call, using procedures outside of the scope of this specification.

If a call is unacceptable then it shall be rejected using a Clear Request. Otherwise, the call shall be accepted using a Call Accept.

A responding BIS shall implement the ISO 9542 "Configuration Information". Whenever an incoming Call is accepted, the ISO 9542 Report Configuration Function shall be invoked to send an ISH PDU over this subnetwork connection. The ISH PDU shall include the NET of the responding BIS's IDRP Network Entity

Note 2.— The ISH PDU may be conveyed as user data associated with the previously described Call Accept, if the subnetwork supports this capability.

Recommendation.— *When a BIS-BIS connection has been established, the periodic transmission of ISH PDUs should be suppressed.*

Whenever an ISO 9542 ISH PDU is received, the Record Configuration function shall be invoked; the routing information necessary for NPDUs to be sent over the subnetwork connection to the indicated NET shall be written into the Forwarding Information Base for use by ISO 8473. A Systems Management Notification shall also be generated to report the arrival of the ISH PDU to local Systems Management.

When the arrival of the ISH PDU is reported to local Systems Management, if a BIS-BIS connection currently exists with the NET given by the ISH PDU, then the IDRP Decision Process shall be invoked. Otherwise, if the the NET received is not in the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object, then it shall be added and an **adjacentBIS** Managed Object created for the initiating BIS identified by this NET and an idrp "start event" shall be invoked .

Note 3. - When no IDRP BIS-BIS connection exists although the externalBISNeighbor managed object exists, then an IDRP BIS-BIS connection is in progress and no futher action need be taken.

3.1.2.1.2 A6.1.2.1.2 Connection Termination

Whenever a subnetwork connection is terminated, either by the network provider, or by the called DTE, then a Systems Management Notification shall be provided to local Systems Management in order to report loss of the subnetwork connection. Forwarding Information associated with the subnetwork connection shall be removed from the Forwarding Information Base.

3.1.2.2 A6.1.2.2 Initiating BIS Provisions

3.1.2.2.1 A6.1.2.2.1 Connection Establishment

An initiating BIS shall be available to receive "Join Events" from the subnetwork.

If a subnetwork connection is unacceptable then the Join Event shall be ignored. Otherwise, a Call Request shall be issued with the candidate responding BIS's subnetwork address as the called DTE Address.

An initiating BIS shall implement the ISO 9542 "Configuration Information". Whenever a Call to a responding BIS is established, the ISO 9542 Report Configuration Function shall be invoked to send an ISH PDU over this subnetwork connection. The ISH PDU shall include the NET of the initiating BIS's IDRP Network Entity

Note 2.— The ISH PDU may be conveyed as user data associated with the previously described Call Request, if the subnetwork supports this capability.

3.1.2.2.2 A6.1.2.2.2 Connection Termination

Whenever a subnetwork connection is terminated, either by the network provider, or by the called DTE, then a Systems Management Notification shall be provided to local Systems Management in order to report loss of the subnetwork connection.

Forwarding Information associated with the subnetwork connection shall be removed from the Forwarding Information Base.

When local Systems Management receives a notification reporting loss of the subnetwork connection, if there are no alternative subnetwork connections with the responding BIS associated with that subnetwork connection, then an IDRP "stop event" shall be invoked to terminate the BIS-BIS connection with that responding BIS. If the BIS-BIS connection is not re-established within a period configurable from 1 minute to 300 minutes, or when the resources are required for other use, then the **adjacentBIS** Managed Object associated with the responding BIS shall be deleted, and the responding BIS's NET removed from the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object.

If the subnetwork is capable of generating a Leave Event then when a Leave Event is received, all virtual circuits associated with that subnetwork shall be cleared.

3.1.2.2.3 A6.1.2.2.3 Join Events

A join event shall consist of the detection of a newly reachable SNPA (or set of SNPAs) of the responding BIS.

If the router cannot determine implicitly from which subnetwork the join event report is coming, this information shall be conveyed explicitly in the report.

3.1.2.2.4 A6.1.2.2.4 Leave Events

A leave event shall consist of the detection of connectivity break-down identifying the SNPA(s) of the responding BIS(s).

If the router cannot determine implicitly from which subnetwork the leave event report is coming, this information shall be conveyed explicitly in the report.

3.1.2.3 Section A6.2.2.2 The ATN RDC

Editor's Note: Deleted as agreed by WG2

The set of interconnected Routing Domains that together forms the ATN shall operate as a single Routing Domain Confederation (RDC). This shall be known as the ATN RDC. The ATN RDC shall not be nested within any other RDC.

Note 1.— Subordinate RDCs are nested within the ATN RDC.

Note 2.— The purpose of the ATN RDC is to enable routes to be readily restricted in scope to ATN RDs only.

3.1.2.4 Section A6.2.2.2 ATN Island RDCs

Editor's Note: Replaced by revised definition focussing on the role of the default route provider.

Within each ATN Island RDC there shall be at least one RD operating as a Transit Routing Domain and able to provide routes to all ATN RDs within the ATN Island RDC. [a6 t 0970]

All RDs in a single ATN Island shall transfer data under at least one common security policy. [a6 t 0980]

3.2 A6.3 Routing Policy

3.2.1 A6.3.1 General

Editor's Note: Replaced by new A6.5.3, etc.

Through the Routing Decision Process, each BIS in the RD shall apply the route selection algorithm specified by the Routing Policy to information in the Adj-RIB-In to determine a degree of preference for potential routes. A BIS shall select for local use the routes with the highest degree of preference.

Depending on its Routing Policy, the BIS shall select from these selected routes, the routes that it will advertise externally. For those routes, the Routing Policy shall determine how the path attributes may be modified, and any route information reduction and aggregation that may be performed.

3.3 A.6.4 Route Advertisement

Editor's Note: Replaced by new text in support of "option 4 lite".

3.3.1 A6.4.1 Distinguishing Path Attributes

BISs in an ATN Routing Domain supporting Operational and/or Administrative communications shall support the following Distinguishing Path Attribute (DPA):

a. SECURITY

Recommendation. BISs in an ATN Routing Domain supporting Operational and/or Administrative communications should also support the following set of DPAs:

a. SECURITY, TRANSIT DELAY

b. SECURITY, EXPENSE

Recommendation.—BISs in an ATN Routing Domain supporting General Communications should support the following sets of DPAs:

a. SECURITY

b. SECURITY, TRANSIT DELAY

c. SECURITY, EXPENSE

Note 1. - In accordance with ISO/IEC 10747, ATN RDs may also support the empty (default) set of DPAs.

The SECURITY attribute shall identify one of the following Security Types:

a. ATN Operational Communications

Note 2: ATN Operational Communications is an ATN network security type for safety and regularity of flight communications. Example communications may be derived from both Air Traffic Service Communications (ATSC) related to safety and regularity of flight. ATSC is related to flight information services, alerting services, air traffic advisory services, air traffic control services and services related to safety and regularity of flight.

b. ATN Administrative Communications

Note 3: ATN Administrative Communications is an ATN network security type for aircraft communications not associated with safety and regularity of flight. This category does not include public correspondence communications. Examples for this category include private

correspondence of aircraft operators for such items such as flight and ground transportation bookings, deployment of crew and aircraft, organization of supplies and services for ongoing and for return flights or any other logistic purpose which maintains or enhances the efficiency of the over-all flight operation.

c. ATN Systems Management Communications.

Note 4: ATN Systems Management Communications is an ATN network security type for systems management information that is considered critical for support of network operation.

d. General Communications.

Note 5: General Communications is an ATN Network security type which includes all other communications relating to the non-safety and regularity of flight traffic.

ISO 8473 PDUs indicating the ATN Systems Management Communications security type in their Security Label shall be transferred over routes irrespective of the security attribute in the route's DPA. BIS-BIS communications shall be allowed to be transferred over any available subnetwork between two adjacent BISs.

Routes that do not include a security attribute in their DPA shall be implicitly associated with the security type General Communications.

Note 6.— An ATN RD need not support all the above Security Types.

Note 7.— Other DPAs may be supported as a local matter or by bilateral agreement between the operators of interconnected Administrative Domains.

Each ATN BIS shall support at minimum one RIB-Att for each Security Type indicated in a,b, and c it supports. For Operational and Administrative Communications, the RIB-Att shall comprise the SECURITY attribute .

Recommendation.— *For Operational and Administrative Communications an ATN RD should support two additional RIB-Atts for each Security Type it supports: the first RIB-Att comprising the SECURITY attribute identifying the Security Type, and theTRANSIT DELAY attribute only and the second RIB-Att comprising the SECURITY attribute identifying the Security Type, and the EXPENSE attribute only.*

Recommendation. *For General Communications, an ATN RD should support three RIB-Atts: the first RIB-Att comprising the SECURITY attribute identifying the Security Type only; the second RIB-Att comprising the SECURITY attribute identifying the Security Type and the TRANSIT DELAY attribute only; and the third RIB-att comprising the SECURITY attribute identifying the Security Type and the EXPENSE attribute only.*

3.3.2 A.6.4.2 Route Origination

Editor's Note: Replaced by new A6.5.1

When a BIS advertises to a BIS in an adjacent ATN RD, a route to destinations located within its local RD, as required by the applicable Routing Policy specified in 6.3 above, a route to the same set of destinations shall be advertised to the same adjacent BIS for each other RIB-Att in common to the two BISs identified above.

The values assigned to the SECURITY attribute and QOS metrics on routes advertised to another ATN BIS shall depend on the security policies and characteristics of the BIS's local RD, and those of the subnetwork(s) joining the two BISs. When any of those subnetworks are restricted insofar as they are not available for use by traffic under any of the ATN

Security Policies, then the values assigned to the SECURITY attribute and QOS metrics in each individual route shall only depend on the security policies and characteristics of the subnetworks joining the two BISs which are available for traffic which may follow that route. The advertised route information shall enable the receiving BIS to unambiguously identify the joining subnetwork(s) which are associated with the access restrictions and QOS metrics included in the advertised route(s).

3.3.3 A6.4.3 Re-advertisement of Routes

Editor's Note: This has changed for option 4 lite and is now in appendix 11.

When a BIS advertises a route not originated locally and re-advertises it to another ATN BIS according to the applicable routing policy specified in 6.3 above, then it shall update the SECURITY attribute and QOS metrics contained in the route to take into account the security policies and characteristics of the BIS's local RD, and those of the subnetwork(s) joining the two BISs. When any of those subnetworks are restricted insofar as they are not available for use by traffic under any of the ATN Security Policies, then the modification to the values of the SECURITY attribute and QOS metrics in each individual route shall only depend on the security policies and the characteristics of the subnetworks joining the two BISs which are available for traffic that may follow that route.The advertised route information shall enable the receiving BIS to unambiguously identify the joining subnetwork(s) which are associated with the access restrictions and QOS metrics included in the advertised route(s).