Analysis of Proposed Modifications to the ATN Routing Architecture to meet ATNP/WG1 Routing Policy Requirements

1. Background

When the routing policy requirements endorsed by ATNP/WG1 in Toulouse were discussed by the CISEC prior to the first meeting in April 1995, it was agreed that there were two issues that needed to be discussed and agreed before these requirements could be met:

- First, how are policy requirements expressed in the CLNP Header.
- Second, how is routing information supporting the meeting of these requirements distributed by IDRP.

During the April 1995 CISEC meeting, a number of options for resolution of these two issues were discussed, and it was agreed that the participants in the CISEC process should consider these options, and develop more detailed proposals for evaluation by the May 1995 CISEC meeting. This flimsy presents an overview of the three proposals (denoted Options 1, 4 and 5) ultimately analyzed by the May 1995 CISEC meeting, and presents an overview of the key differences among these options.

Note: Options 2 and 3 as discussed at the April 1995 CISEC meeting have not been further progressed, since the new Options 4 and 5 were derived directly from Options 2 and 3, respectively, and are viewed to replace them. These new derived options were the result of the analysis performed by the proposing States/Organizations (i.e. EUROCONTROL, France and SITA), who concluded that the CLNP header mechanism initially proposed in Options 2 and 3 (i.e. the NSAP address convention) should be replaced by an approach using the CLNP security option to convey application user policy preference. Elements of Options 4 and 5 are further clarified in the annex to this flimsy.

2. References

	Reference	Title
1	ATNP/WG1/Toulouse-Flimsy 3	Requirements placed on the ATN Communication Service by Air/Ground Applications
2	ATNP/WG2-WP/CISEC/10	Analysis of Alternatives for CNS/ATM-1
3	ATNP/WG2-WP/117 (ATNP/WG2-AP/CISEC/12)	Meeting Application Specific Routing Policy Requirements in CNS/ATM-1 Package

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

3. Routing Policy Information Exchange

3.1 Conveying Routing Policy Requirements in the CLNP Header

Two techniques for conveyance of routing policy requirements were discussed during the April 1995 CISEC meeting:

1) Expression of the user’s requirements in the CLNP Security Parameter (essentially expanding upon the specification in the ATN Manual)

2) Expression of the user’s requirements through NSAP 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).

3.2 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.

Given this assumption, three techniques emerged as candidates in support of ground-to-air routing:

a) An Addressing convention can be used in conjunction with 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.

b) The IDRP Security Path Attribute can be used 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 synthesized from this information e.g. to construct a separate FIB for each user policy request.

c) The IDRP Security Path Attribute can be used 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 synthesized from this information e.g. to construct a separate FIB for each user policy request. This is an extension of the ATN Manual approach.

4. Description of Options

4.1 Characterization of the Options

Given the elements of routing policy information expression and exchange described in Section 3 above, the three options considered by the CISEC can be characterized as in the table that follows. Note that the "Reference" column refers to the designators used in the two lists in Section 3 above.

Option	Policy Mechanism Reference from Section 3	CLNP Header Application Policy Expression Approach	IDRP Route Information Processing Approach
Option 1	2(a)	Expresses application policy using Addressing Convention in NSAP Address.	Conveys route policy support information using Addressing Convention for IDRP RD_Path NLRI exchange.
Option 4	1(b)	Expresses application policy using Security Option in CLNP NPDU. *Note: Uses "Type/Value" semantic with single registration identifier.*	Conveys route policy support information using security related information in the IDRP security path attribute. *Note: Due to "Type/Value semantic, particular benefits accrue from route aggregation.*
Option 5	1(c)	Expresses application policy using Security Option in CLNP NPDU. *Note: Uses "Type-Only" semantic with multiple registration identifiers.*	Conveys route policy support information using security related information in the IDRP security path attribute.

4.2 Description of System/Functional Attributes

During the May 1995 CISEC meeting, an extensive discussion of the relative system and functional attributes of Options 1, 4 and 5 took place. These tables present a comparison of the three options in order to highlight the key technical differences among those options. The CISEC agreed that these attributes do not in general constitute decision criteria for choice among the options, but felt that understanding of these attributes contributes to the decision making process.

4.2.1 End-System Attributes

Deviation from Binary COTS Products	Option 1	Option 5	Option 4
1. Method required for Conveyance of Policy	Alias Addresses	CLNP Security Option	CLNP Security Option

Preferences			
2. Software Modification Implications	Mechanism required for embedding of Application Policy Information in NSAP Address	Mechanism required for embedding of Application Policy Information in CLNP Security Option	Mechanism required for embedding of Application Policy Information in CLNP Security Option

4.2.2 BIS Attributes

Characteristics differing among the Options	Option 1	Option 5	Option 4
1. FIB & RIB Processing	Use of RD_Path to populate FIB(s) and RIB(s) Single FIB	Multiple FIBs	Multiple FIBs
2. One to One Matching between LocRIB and FIBs	Yes	Yes	No
3. Forwarding Process	NSAP Pre-processing before route look-up	One FIB per subnetwork type	One FIB per policy preference
4. Support for IDRP Security	Not Required	Required (Type)	Required (Type/Value)
5. Hold Down Timer Mechanism	As per standard	As per standard	Requires additional condition

4.2.3 IS Attributes

Characteristics differing among the Options	Option 1	Option 5	Option 4
1. Requires transparent transfer of CLNP Security Option	No	Yes	Yes

5. Analysis of Architectural Attributes

The table in this section presents the architectural attributes of the three proposals which were viewed to be related to the decision as to which of the three options should be adopted to meet the requirements in ATNP WG1 Flimsy 3 from Toulouse.

Attribute	Option 1	Option 5	Option 4
1. Air/Ground Subnetwork Selection based on Application Policy	Yes	Yes	Yes

Preference			
2. Selection of routes across multiple RDs based on Application Policy Preferences expressed as Traffic Types	Yes	Yes	Yes
3. Requirement for use of one octet in NSAP address System ID field for conveyance of policy preference	Yes	No	No
4. Constraints on Scalability of routing architecture	Policy selection is limited to 256 choices, unless more address space is devoted to this purpose.	No intrinsic limitation	No intrinsic limitation
5. Relative benefits derived from Aggregation	None	None	Aggregation of routes based on security attributes possible.

6. Validation Considerations

Note: Entries in the table below are provided only for informational purposes, and do not constitute a commitment from any of the States or Organizations named. Further, the entries for the UK and for EUROCONTROL were constructed using information known by other CISEC members, and are subject to verification and modification by representatives of the UK and EUROCONTROL. Finally, information supplied for the France (EURATN/Merit) entry assumes the retention of the current Merit IDRP in the validation testbed; discussions are currently in progress regarding replacement of this IDRP with a more capable product available to the EURATN Consortium. If this approach is taken, the entry for the validation testbed for France would be the one denoted “France (EURATN/IDRP)”.

Implementations	Option 1	Option 5	Option 4
US (ACET/Merit)	Introduce virtual RDIs. Decision process to populate FIB.	Introduce multiple FIBs. Introduce IDRP Security.	Introduce multiple FIBs. Introduce IDRP Security. Modify Hold-Down Timer conditional.
US (DLP/2)	Introduce virtual RDIs. Decision process to populate FIB. Modify forwarding process. Modify policy support.	Introduce multiple FIBs. Modify Phase 2 routing decision process. Introduce route aggregation.	Introduce multiple FIBs. Modify Phase 2 routing decision process. Introduce route aggregation.

Implementations	Option 1	Option 5	Option 4
	Introduce optional non-use of air/ground IDRP.	Introduce CLNP security. Introduce IDRP security. Modify forwarding process. Introduce optional non-use of air/ground IDRP.	Introduce CLNP security. Introduce IDRP security. Modify forwarding process. Modify Hold-Down Timer conditional. Introduce optional non-use of air/ground IDRP.
UK (Retix TAR)	TBD	TBD	Modify multiple FIB implementation, to process security preference as defined in this option. Modify IDRP security processing to handle security preference as defined in this option. Modify Hold-Down Timer conditional. Introduce route aggregation. Without route aggregation, available approximately August 1995.
France (EURATN/Merit)	Introduce virtual RDIs. Decision process to populate FIB.	Introduce multiple FIB implementation, to process security preference as defined in this option. Introduce IDRP security processing to handle security preference as defined in this option.	Introduce multiple FIB implementation, to process security preference as defined in this option. Introduce IDRP security processing to handle security preference as defined in this option. Modify Hold-Down Timer conditional.
France (EURATN/IDRP)	TBD	Integrate IDRP within EURATN platform. Introduce multiple FIB implementation, to process security preference as defined in	Integrate IDRP within EURATN platform. Introduce multiple FIB implementation, to process security preference as defined in

Implementations	Option 1	Option 5	Option 4
		this option. Modify IDRP security processing to handle security preference as defined in this option.	this option. Modify IDRP security processing to handle security preference as defined in this option. Modify Hold-Down Timer conditional. Introduce route aggregation.
SITA	TBD	Integrate Retix IDRP. Modify multiple FIB implementation, to process security preference as defined in this option. Modify IDRP security processing to handle security preference as defined in this option. (Available approx. September 1995)	TBD
EUROCONTROL (Retix TAR)	TBD	TBD	Modify multiple FIB implementation, to process security preference as defined in this option. Modify IDRP security processing to handle security preference as defined in this option. Modify Hold-Down Timer conditional. Introduce route aggregation. Without route aggregation, available approximately August 1995.

7. Conclusion and Recommendation

With this flimsy, the ATNP CISEC provides to ATNP Working Groups 1, 2 and 3 an annex (Annex A) containing descriptive material derived from the input papers on each respective option. This annex has been agreed by the CISEC to contain reasonable and objective descriptions of those options, to support Working Group deliberations leading to the selection of one of these three options for inclusion in CNS/ATM-1 package SARPs and Guidance Material.

In addition to this annex, the authors of the respective input papers on Options 1, 4 and 5 have agreed to provide the Working Groups with one page “decision case papers”, supporting the views represented by the proponents of these options. These case papers are also intended to support Working Group deliberations leading to the selection of one of these three options for inclusion in CNS/ATM-1 package SARPs and Guidance Material.

RECOMMENDATION: Following the presentation of this flimsy, the presentation of the three decision case papers, and the resulting deliberations, the it is recommended that the Working Groups select one of these three options for inclusion in CNS/ATM-1 package SARPs and Guidance Material, with the decision being reached no later than the conclusion of the 15 - 19 May 1995 Working Group meeting sessions.

It was the unanimous opinion of the CISEC members that this decision **must** be reached during this ATNP Working Group meeting session, i.e. no later than 19 May 1995. The CISEC also agreed to abide by the decision of the Working Groups, and to begin immediate development of appropriate SARPs and Guidance Material according to that decision.

Annex A

Description of Options

1. Option 1: CLNP Addressing Convention, Route Distribution via NLRI

This option uses information added to the ATN NSAP format to carry routing policy information in CLNP packets, and in the NLRI information propagated as part of IDRP Update PDUs. End Systems identify the ordered preference of air/ground subnetworks over which an individual NPDU will be sent by encoding this information in a field in the NSAP. This routing policy information is encoded according to Table 1.

Table 1: Policy Preference Encoding for Option 1

Routing Policy Value	
0000 0001	No Traffic Type Policy Preference
0000 0010	Traffic only follows ATSC route(s).
0000 0011	Route Traffic using an ordered preference of Mode S first, then VHF Data Link, then Satellite Data Link, then HF Data Link.
0010 0001	No Traffic Type Policy Preference.
0010 0010	Route Traffic only via Gatelink.
0010 0011	Route Traffic only via VHF Data Link.
0010 0100	Route Traffic only via Satellite Data Link.
0010 0101	Route Traffic only via HF Data Link.
0010 0110	Route Traffic only via Mode S Data Link.
0010 0111	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link.
0010 1000	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then Satellite.
0010 1001	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then HF Data Link, then Satellite Data Link.

Using this same NSAP encoding convention, the IDRP NLRI field is used to enumerate all prefixes that correspond to the routing policies permitted by the path being advertised. Additionally, this option introduces the concept of a Virtual Routing Domain Identifier (VRDI) to denote which air/ground subnetwork is in the path being advertised. Each subnetwork type will be assigned a VRDI which will allow routers “downstream” to determine which a/g subnetwork is included in the path being advertised in an IDRP Update PDU. Subnetwork types defined for VRDI RD_Path values are defined by Table 2.

Table 2: VRDI RD_Path Encoding for Option 1

Subnetwork Type	VRDI Value
Mode S	0000 0001
VDL	0000 0010
AMSS	0000 0011
Gatelink	0000 0100
HF	0000 0101

The ground router after receiving the ISH from the aircraft will construct an update PDU containing the VRDI information for the a/g subnetwork in the RD_PATH attribute and all its associated prefixes in the NLRI field.

Ground routers receiving information from other BISs will examine the RD_PATH attribute and the NLRI information along with the known policies to determine which routes to insert into the FIB and which routes to propagate to other systems. This option will result in only one FIB which constrains all the enumerated NLRI prefixes.

2. Option 4: CLNP Security Parameter, Route Distribution via IDRP Security with Single Security Registration Identifier

2.1 Overview

This option uses the security field in CLNP packets to indicate the desired routing policy for the NPDU. This option encodes the air/ground subnetwork in the path being advertised within the security related information field of the security attribute as defined by IDRP. The security attribute is also used to identify traffic types supported by the path being advertised. To use this option as proposed, changes in the IDRP standard are required regarding the use of the “hold down” timer.

Ground routers will, after receiving the ISH from the aircraft, construct an update PDU containing the air-ground subnetwork type and traffic types supported in the security related information field and put the aircraft prefix in the NLRI field.

Ground routers receiving information from other BISs will examine the security related information field and the NLRI information along with the policy to determine which routes to insert into the FIB and which routers to propagate to other systems. This option will result in multiple FIBs, with one per air/ground policy preference.

2.2 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. 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.

2.3 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.

2.3.1 Updating the Security Related Information

This section now describes how this option 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.

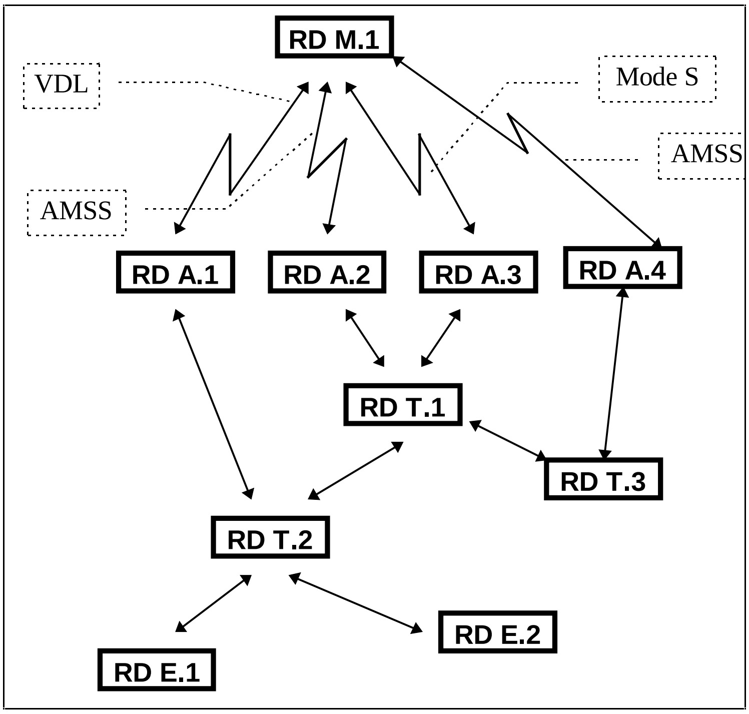

Figure 1 Example ATN Topology

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 recognized 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.

2.4 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.

2.4.1 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.

2.4.2 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. Option 5: CLNP Addressing Convention, Route Distribution via IDRP Security with Multiple Security Registration Identifiers

This option tries to adapt as much as possible the mechanisms defined in the ATN manual regarding the use of the security parameter in CLNP PDUs and the IDRP security attribute. The proposal is to define additional security attributes, basically a security type per type of ATN air/ground subnetworks , and to carry the ATN user routing preference in the information field of the security parameter of 8473 NPDUs.

3.1 Additional security types :

Currently the manual mandates the use four different types of security :

1) ATN Administrative Communications

2) ATN Operational Communications

3) General Communications

4) System Management Communications.

In order to accommodate the requirements defined in the WG1 Flimsy 3 (attached to the Toulouse WG2 report), which are based on air/ground subnetworks preferences and AOC/ATC domains, Option 5 simply requires to define the following additional security types:

5) VHF Data Link

6) Satellite Data Link

7) HF Data Link

8) Mode S Data Link

9) Gatelink

10) ATSC

The mechanisms to handle these new security types are exactly the same as the one defined in the manual for the four types of communications. These mechanisms are conformant to the current version of CLNP and IDRP standard.

For future evolution, in order to allow migration to an enhanced IDRP such as the one proposed in Option 4, a new security type could be defined:

11) ATN

In Option 5 , this additional security "ATN" would be passed transparently and would not lead to any specific processing but would allow in the future interoperability with systems which process not only the type of security but also the value of the security, as proposed in Option 4.

3.2 Possible simplification of the list of the security types :

At this stage no specific preferences policies have been expressed in terms of the Administrative, Operational, General, System Management traffic categories. So the package 1 implementation could only consider the new security types listed above and may not need yet to implement the 4 types already listed in the manual. This would allow a reduction of the number of security types which must be handled. This is a proposed optimization but is not mandatory to implement Option 5.

3.3 Routing policy conveyed by the ISO 8473 NPDUs

The policy is conveyed in the information field of the security parameter of the CLNP PDUs .

There will be as many possible values for this field as users' routing preference policies such as the ones expressed in the flimsy 3 of the Toulouse WG report, each value characterizing one policy.

3.4 FIB handling by CLNP

1) First envisaged FIB architecture :

For each security type a separate inter-domain FIB shall be maintained by each ATN BIS. Each of the above FIBs is updated by IDRP. For each NPDU the CLNP route function shall select a set of FIBs according to the security type conveyed in the NPDU and according to the routing preference conveyed in the information field of the security parameter.

This is the architecture recommended by the IDRP standards, where there is a one to one matching of the locRibs organization to the FIBs , however the drawback is that more than one FIB look -up may occur in the case of complex policies.

2) Second envisaged FIB architecture

For each routing preference policies a separate inter-domain FIB shall be maintained. In this case only one FIB look-up occurs , because the CLNP can directly access the appropriate FIB using the security parameter, type and information, conveyed in the NPDU header.

However the drawback is that the IDRP procedure to add LOCRIB's route to the FIB is more complex and must analyze routing preference policies to select the FIBs into which the information must be added.

Conclusion

The choice between the FIB architecture 1 and 2 is a local implementation matter. Both solution allow to accommodate the IDRP security types and the 8473 NPDU security value as proposed in Option 5.

3.5 Security handling in IDRP

Each ATN BIS shall support a RIB-ATT per security type. Once an air/ground subnetwork becomes available a new route is propagated, which RIB_ATT contains the corresponding security. Once a subnetwork is no longer available, the corresponding route is withdrawn.

This solution is the standard use of the security type as defined in the current version of the IDRP Standard.

4. Option 3: (Original Concept) CLNP Addressing Convention, Route Distribution via IDRP Security with Multiple Security Registration Identifiers

This option was already presented in the report of the APRIL CISEC meeting but without all the details which allow to compare it with the other options.

For the reader's understanding, Option 5 is a revisited version of Option 3 , which needed to be updated to reflect new views regarding the mechanism to convey the routing preference in CLNP PDUs.

At the April CISEC meeting, it was almost agreed that the preference policy would be carried in the address part of the 8473 NPDUs. In this context , Option 3 (which relates more to IDRP than to the conveyance of routing policy in CLNP) was then defined as below. Since then, CISCO reported that their OSI routers can not accept more than 3 NSAP aliases which in the case where the initial solution to convey preferences in NSAP addresses is maintained, would prevent ATN end users to use CISCO routers. As some ATN users strongly requested to be able to be able to use CISCO or current off-the-shelf OSI routers in End routing domains, certain CISEC members are now proposing to carry the preference policy in the security parameter of the CLNP NPDU.

4.1 Additional security types :

Currently the ATN manual mandates the use four different types of security:

1) ATN Administrative Communications

2) ATN Operational Communications

3) General Communications

4) System Management Communications.

In order to accommodate the requirements defined in the WG1 Flimsy 3 attached to the Toulouse WG report, which are based on air/ground subnetworks preferences and AOC/ATC domains, Option 3 simply requires to define the following additional security types:

5) VHF Data Link

6) Satellite Data Link

7) HF Data Link

8) Mode S Data Link

9) Gatelink

10) ATSC

The mechanisms to handle these new security types are exactly the same as the one defined in the manual for the four types of communications. These mechanisms are conformant to the current version of CLNP and IDRP standard.

4.2 Possible simplification of the list of the security types :

At this stage no specific preferences policies have been expressed in terms of the Administrative, Operational, General, System Management traffic categories. So the package 1 implementation could only consider the new security types listed above and may not need yet to implement the 4 types already listed in the manual. This would allow a reduction of the number of security types which must be handled . This is a proposed optimization but is not mandatory to implement option 3.

4.3 Routing policy conveyed by the ISO 8473 NPDUs

The routing preference policy shall be conveyed within the address part of the CLNP NPDU. The required policy shall be encoded as a Tag, which for a given traffic type represents the preferences in terms of air/ground subnetwork.

Moreover the above tag should not be included in the NSAP address prefix in order to allow COTS products using the IS-IS protocol to carry ATN traffic.

4.4 FIB handling by CLNP

1) First envisaged FIB architecture :

For each IDRP security type a separate inter-domain FIB shall be maintained by each ATN BIS. Each of the above FIBs is updated by IDRP. For each NPDU the CLNP route function shall select a set of FIBs according to the routing preference "tag" conveyed in the destination NSAP address of the CLNP NPDU to be forwarded..

This is the architecture recommended by the IDRP standards, where there is a one to one matching of the locRibs organization to the FIBs , however the drawback is that more than one FIB look -up may occur in the case of complex policies.

2) Second envisaged FIB architecture

For each routing preference policies a separate inter-domain FIB shall be maintained. In this case only one FIB look-up occurs , because the CLNP can directly access the appropriate FIB using the routing preference "tag" conveyed in the destination NSAP address of the CLNP PDU to be forwarded.

However the drawback is that the IDRP procedure to add LOCRIB’s route to the FIB is more complex and must analyze routing preference policies to select the FIBs into which the information must be added.

Conclusion

The choice between the FIB architecture 1 and 2 is a local implementation matter. Both solution allow to accommodate the IDRP security types and the 8473 NPDU security value as proposed in option 3.

4.5 Security handling in IDRP

Each ATN BIS shall support a RIB-ATT per security type. Once an air/ground subnetwork becomes available a new route is propagated, which RIB_ATT contains the corresponding security. Once a subnetwork is no longer available, the corresponding route is withdrawn.

This solution is the standard use of the security type as defined in the current version of the IDRP Standard.

Annex B: Option 1 Point of View

1. Introduction

This annex documents support for the "Option 1" proposal, traffic typing via NSAP, discussed at the first and second CISEC meetings. Development risk, validation, risk, technical maturity, and support by commercial off-the-shelf products are assessed in supporting this option as the ATM/CNS Package 1 ATN design

2. Technical Maturity

Routing based on the security attribute is a new concept introduced by the OSI routing protocols. Consequently, it is also not widely implemented nor well understood. Routing based purely on address is a concept that is at the heart of the Internet and has been implemented, sold as a product and been widely tested and used. While available in certain IDRP implementations, large scale routing based on the security attribute has not been demonstrated. As a result, the technical maturity of this section of IDRP has not been demonstrated.

Traffic typing via NSAP values has been implemented in OSI protocols as part of the US validation effort for over two years. This work has been reported to ICAO (most recently in the form of the Routing Initiation Protocol [RIP] discussed in Melbourne) and is considered to be stable and feasible by the US.

Option 1 introduces the concept of a virtual RDI, and the use of this RDI is consistent with the intended use of RDIs in IDRP. While the virtual RDI is new, RD_PATH and its expression of RDIs has been implemented in available IDRP implementations and has been tested and demonstrated on a wide basis as a result (e.g., the US validation effort has demonstrated RD_PATH support in the MERIT IDRP implementation in September 1994.

3. Validation Risk

Ten months remain to validate the ATN to the original March 1995 schedule. In this time frame, package 1 implementations must undergo development and experimentation. A "one of" implementation of an ATN router supporting the required package 1 features is not sufficient for validation; independently implemented ATN components interoperating in a test network large enough to demonstrate system performance are required. States and organizations have previously developed ATN validation systems and have targeted package 1 implementations. The security features of options 4 and 5 are not available as COTS and will require development. This development could likely comprise the bulk of the validation schedule and impact the experimentation necessary for a proper validation program.

It is estimated that option 1 development could be completed one month in the US validation program, leaving 9 months for package 1 flight trials and experimentation

4. Support for COTS

COTS Level 1 and 2 IS-IS routers do not widely support the CLNP security attribute. In fact, tests performed in the US using a Cisco router show that the device actually drops packets when the security attribute is set. Additionally, COTS end-systems (e.g., Sun and Retix) do not support setting or handling of the security attribute. End-system impact extends to TP4, CLNP, and ES-IS. Options 4 and 5 require end-system and IS-IS support for security while option 1 does not. option 1 could be more widely supported COTS that either options 4 or 5

5. Conclusion

Based on the above considerations, option one provides the least risk alternative to providing ample time for validation and allowing for the most cost effective implementation of ATN through its support of COTS components.

Annex C: Option 4 Point of View

1. Introduction

This annex contrasts the two main architectural elements of the solutions discussed in the body of this paper, and concludes that the Option 4 proposal best serves the needs of CNS/ATM-1 Package.

2. Routing Policy Requests in the CLNP Header

There was initially strong support within the CISEC for the use of an addressing convention to perform this function, as is proposed in Option 1, based on the desire to use commercially available L1 and L2 Routers within ATN Ground Routing Domains. It was understood based on States' inputs to the CISEC that no such router currently supports the security parameter, and that commercial routers will discard packets that contain such a parameter. It was also recognized that End Systems may not support this parameter. However, the meeting also recognized 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. 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 ISO 10747 (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.

Following these discussions, 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. Given this configuration possiblity, given the other problems noted above regarding "address aliasing", and considering the likely impact of the "addressing convention" on end-systems and application architecture, conveyance of policy request information using the CLNP security option therefore appears to be a workable approach and is thus proposed in Option 4.

3. IDRP Route Information Dissemination

Option 5 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. However, Option 5 has this has two clear drawbacks. The first is that the number of routes multiplies to a level which may well overwhelm the capacity of ATN Routers in the long run, 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 "labeling" 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 5 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.

Option 1 avoids the proliferation of routes that is characteristic of Option 5 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 drawbacks as Option 5. This is 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 be adjacent to an air-ground subnetwork.

Option 4 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 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 recognized problem with Option 4 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. 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. This is believed to be a defect in the ISO 10747 standard, and is thus a candidate for changes in the standard. Assuming that this fix is implemented, then Option 4 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.

4. Conclusion

For the architectural and transitional reasons discussed in this paper, Option 4 is viewed to be the best option for CNS/ATM-1 Package implementation. This is supported in the context of validation considerations as well, since this option is viewed by several States and Organizations to be implementable in the necessary time frame for Package 1 validation, i.e. this option can be supported by validation test bed implementations prior to the end of 1995.

Annex D: Option 5 Point of View

1. Introduction

This annex presents a comparison of the three options under consideration, from the point of view of the proponents of Option 5.

2. Option 1

Option 1 is a temporary solution which would allow the fast production of a system for immediate validation activity but does not offer good prospect in terms of future integration of new policies requirements.

It is reasonable to envisage that as soon as the ATN will start to be deployed , more and more complex routing policies requirements will emerge , and this within package 1 timeframe. With the option 1 solution this will lead to a more and more complex ATN addressing plan and may soon reach the limitation of 256 possible policies identified in the CISEC evaluation of options.

3. Option 5

Option 5 is the closest to the security procedures solution presented in the current ATN manual. Thre are some validation implementation which have implemented the manual recommendation in term of security and which with some minor updates can accomodate very soon this solution. It is evolutive in terms of policies , as there is no limitations in the length of the field which carries the routing preference information. Its evolution is only limited if new air/ground subnetworks are identified, as in this case it requires the definition of a new security type, which will be rejected by old systems in the case of a migration.

4. Option 4

Option 4 is not radically different from option 5, but requires an IDRP which is able to process the value of the security an a non standard holding timer procedure. The advantage of this option is that it offers the best capabilities in terms of evolution, and can provide solutions if new air/ground subnetworks are defined, which is not the case of option 5.

The problem is that such implementation of IDRP does not exist yet . The changes to be performed from currently available implementation can be dealt with but are not minor, they require a non trivial testing process and there is a reasonable chance that , if this option is adopted , a stable implementation will not exist before early 1996 . Another drawback is that the ATN will not be conformant anymore to the ISO 10747 implementation .

5. Conclusion

From the 3 options under discussion, option 1, option 4, option 5 ,   option 5 is the preferred option because it satisfies the WG2 ATN validation timeframe as well as allowing , within the ATM/CNS Package 1 timeframe , the integration of   new policies without the restrictions related to option 1.

It can also allow the migration in the future to enhancement such as option 4, (see option 5 presentation) when this option 4 definition and implementation will be stabilized and when the IDRP updates that this option 4 requires will have been analyzed and approved by ISO .