ATNP/WG2/
WP/235
02 February 1996

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Brisbane 5.2.96-9.2.96

Proposed Guidance Material for Section Four of the ATN Internet SARPs Guidance Material (Part 2 - Network Layer)

Presented By Henk Hof

Prepared by Tony Whyman

SUMMARY

Action 6/32 required the author to edit the proposed section four guidance material and to present the result to the next meeting. This paper completes the remainder of that action, and provides the guidance material specific to the network layer. This has been based upon the ATN Manual, and includes new material to bring it up-to-date with recent changes to the SARPs. It should be noted that IDRP is only described in overview and that further work is needed to describe it fully.

DOCUMENT CONTROL LOG

SECTION	DATE	REV. NO.	REASON FOR CHANGE OR REFERENCE TO CHANGE
	2/2/96	Issue 1.0	

TABLE OF CONTENTS

4.3 CLNP Implementation Considerations

ISO 8473 describes a protocol for providing the connectionless mode network service. The ISO 8473 protocol is a SNICP capable of operating over many different sorts of subnetwork including X.25, ISDN and LANs. It is an internetworking protocol and may be used to create a connectionless internetwork integrating many different underlying subnetworks.

4.3.1 The Connectionless Mode Network Service

The OSI connectionless network service is the service provided to a network service user when the ISO 8473 connectionless network protocol is used as a SNICP. The operation of the connectionless network service is illustrated in Figure 4-1. It consists of a single end to end primitive - the N-UNITDATA service.

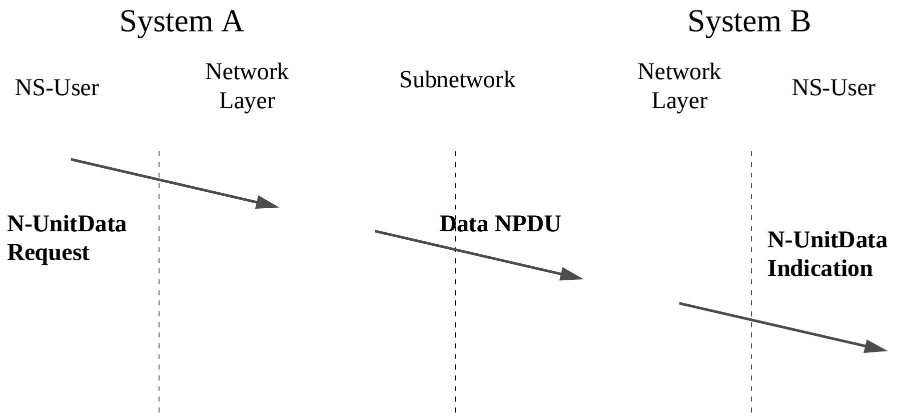

Figure 4-1 Connectionless Network Service

The service is requested by the sender who passes, as the service parameters, the user data (up to 64Kbytes), the network address of the destination, the sender's own source address, and an indication of the quality of service required, and, in the ATN, this includes the Network Priority of the data and the associated ATN Security Label.

The unitdata item is then passed through the network independently of any other data passed between the same source and destination and is finally delivered to the addressed destination. Delivery is not guaranteed and neither is the order of submission of successive unitdata items necessarily preserved. The network may discard a packet if the network is congested, and different packets may take different routes and hence have different transit times. It is the responsibility of a transport layer protocol to provide reliability, in the form of data and data sequence integrity management, if this is required.

4.3.2 The Connectionless Network Protocol

The protocol specified by ISO 8473 is the Connectionless Network Protocol (CLNP). The operation of the CLNP is straightforward and is as described below.

4.3.2.1 Satisfying the N-UNITDATA.Request

Once an NS-User has submitted an N-UNITDATA Request, the information passed with the request is formatted as a single packet, known as a Data Protocol Data Unit (Data PDU). As well as the user data, the PDU contains the source and destination addresses and the quality of service requests, priority and ATN Security Label.

Information controlling the maximum lifetime of the PDU in the network is also provided, in order to prevent PDUs existing forever in erroneous loops, and local management may also add information to specify all or part of the route that the PDU takes. As large Data PDUs may also need to be segmented en route to cope with subnetworks that support only a small packet size, there is thus information present to enable the unambiguous reassembly of segments when and if they arrive at the destination.

Once the PDU has been created, the ES or IS to receive the PDU is then chosen (the next hop) as well as the subnetwork over which the PDU to be sent. This is typically performed by consulting a local routing table. This may have been configured by a System Manager but, more likely, it is maintained by the ISO 9542 ES-IS Routing Information Exchange Protocol (see 4.4.1).

The NPDU is then sent to the chosen “next hop” ES or IS. Note that if the PDU is larger than the maximum packet size supported by the subnetwork then it is segmented prior to being sent.

The procedures for the transfer of an NPDU over a given subnetwork are specific to that subnetwork and are specified in a Subnetwork Dependent Convergence Function (SNDCF) appropriate to the subnetwork type. SNDCFs for the common subnetwork types are specified in ISO 8473. A special SNDCF has, however, been specified for ATN Mobile Subnetworks (see 4.4.4.1).

4.3.2.2 NPDU Forwarding

At each Intermediate System that receives the Data PDU, a similar decision to that made in the originating ES, is made as to which system is the next hop and over which subnetwork, out of those attached to the IS, the PDU will be sent. Segmentation may occur if necessary. Note that once a PDU has been segmented, its component parts are treated as if there were separate Data PDUs and may even be further fragmented.

An Intermediate System may discard a whole Data PDU or a segment. It may do this because of congestion, a security problem, because the PDU's lifetime has expired, or just because it cannot determine a suitable next hop for the PDU's destination.

The Routing Tables kept by an Intermediate System are typically much more complex than an End System’s, and are maintained by a dynamic routing information exchange protocol. These include ISO 9542 ES-IS (see 4.4.1), the ISO 10589 IS-IS Intra-Domain Routing Information Exchange Protocol (see 0), and the ISO 10747 Inter-Domain Routing Protocol (see 0).

4.3.2.3 At the Destination End System

When a Data PDU arrives at the End System that contains its destination, the PDU must first be re-assembled if it was previously segmented - assuming that all the constituent segments arrive within the PDU's lifetime - otherwise, the PDU will be discarded without being presented to the destination user.

Otherwise, once a whole PDU has arrived, it will be passed to the destination NS User, with the service primitive's parameters derived from the PDU contents, including the NPDU priority and Security Label. In the ATN, it is essential that these latter two parameters are made available to the NS-User, as they are required by the Transport Layer.

4.3.3 Addressing Consideration

The Source Address and Destination Address parameters used by the CLNP are OSI NSAP Addresses. These are variable length octet aligned addresses allocated from a global addressing plan that is ultimately administered by ISO, as specified in ISO 8348. The ATN Addressing Plan specified in the ATN SARPs is compliant with this addressing plan, and specifies a twenty octet NSAP Address syntax, together with the allocation procedures. As far as the CLNP is concerned, the actual syntax of the address is immaterial; the forwarding algorithm operates by comparing octet strings and through address prefix matching rules.

The encoding used by the ISO 8473 protocol to convey NSAP Addresses is the preferred binary encoding specified in ISO 8348.

4.3.3.1 Network Entity Titles

NSAP Addresses are used to identify NS-Users by way of the NSAP through which they access the Network Service. However, it is also sometimes necessary to address an NPDU to the Network Entity itself. This is necessary both for network management purposes and for certain routing techniques. Network Entities are identified and addressed by their Network Entity Title (NET).

A *NET* identifies a Network Entity in an end-system or intermediate-system. A NET has exactly the same format as an NSAP address, and is indistinguishable from an NSAP Address. NPDUs addressed to a Network Entity have its NET as their destination address.

NETs are also used widely by CLNP. For example, the entries in the *Source Routing* and *Recording of Route* parameters are NETs. The *Source Address* parameter in the Error Report (ER) NPDU is also a NET.

4.3.4 Other NS User Services

Although the service provided to the NS User is strictly speaking a unitdata service only, other information is typically available and useful for NS Users in making efficient use of the Network. Specifically, information on service characteristics may be accessed and indications on PDUs discarded while in transit.

The service characteristics information that may be made available includes:

- Quality of Service information i.e. an indication of the likely transit delay, protection from unauthorised access, cost and the residual error probability.

- Probability of sequence preservation

- Maximum PDU lifetime.

However, in the ATN, it is expected that such information will be known *a priori* by the Transport Layer and need not be available on a dynamic basis. Indeed, there is standard mechanism available to support the dynamic distribution of such Quality of Service Information.

4.3.5 Error Reports

Error reports may also be provided if PDUs are discarded while in transit. These are supported by a second PDU format - the Error PDU.

An Error PDU may be generated to report every Data PDU that is discarded. However, neither its generation nor its receipt are guaranteed.

In the ATN, Error PDUs received by an End System need to be made available to the NS-User as additional reports. This may be as an extension to the service interface or through a local management mechanism.

4.3.6 Quality of Service Maintenance

CLNP permits an NS-User to make specific QoS Requests in the form of relative preferences as to which QoS metrics to route a packet on. The use of such requests has been considered at length during the development of the ATN SARPs, and, due to practical difficulties in maintaining the necessary routing information, there are no near to medium term plans to make use of these facilities in the ATN.

4.3.7 Priority

Priority is an essential feature in the ATN Internet for ensuring that the performance targets for safety related data are met, whilst permitting the network also to be used by routine communications. Safety related data is always sent with a higher priority than routine data and is given preferential access to resources.

In the ATN Internet Layer itself, an NPDU of a higher priority is given preferred access to network resources. During periods of higher network utilisation, higher priority NPDUs may therefore be expected to be more likely to reach their destination (i.e. are less likely to be discarded by a congested router) and to have a lower transit delay (i.e. be more likely to be selected for transmission from an outgoing queue) than are lower priority packets.

ATN Internet Entities maintain their queues of outgoing NPDUs in strict priority order, such that a higher priority NPDU in an outgoing queue will always be selected for transmission in preference to a lower priority NPDU. Higher priority PDUs may thus overtake a lower priority PDU, and this effect will be especially noticeable during periods of network congestion; the network may appear congested to low priority data, whilst still appearing uncongested to higher priority data.

Furthermore, during periods of congestion, or when any other need arises to discard NPDUs currently held by an ATN Internet Entity, lower priority NPDUs are always discarded before higher priority NPDUs.

4.3.8 ATN Security

In CNS/ATM-1 Package security mechanisms are largely the responsibility of each application. However, in order to meet several Routing Control requirements, security related mechanisms are implemented in the ATN Internet. These take the form of routing decisions that are made with respect to a Security Label encoded in each NPDU header, and according to a set of routing policy rules specified in the ATN Internet SARPs.

The ATN Security Label conveys the following information:

I. A **Traffic Type**: this identifies the type or class of data and is used both to place other information in the security label in context, and as an input to access control rules. In the latter case, certain air-ground networks may limit their users to certain traffic types only. The Routing Control mechanisms will not route data of an unacceptable traffic type over such networks and will attempt to route such data around these subnetworks, if possible.

   A. ATN Operational Communications -ATSC
   B. ATN Operational Communications - AOC
   C. ATN Administrative Communications
   D. General Communications
   E. ATN Systems Management

II. An **ATSC Class**: this is valid for ATSC Traffic Types and identifies the class of subnetwork over which the data should be forwarded. Data may not be forwarded over a subnetwork with a higher ATSC Class than that indicated by its Security Label, and the ATN Internet aims to send data with a declared ATSC Class over a subnetwork supporting that ATSC Class. If no such subnetwork is available, then the next lowest available class subnetwork is chosen.

III. An **Air/Ground Subnetwork Preference**: this is valid for AINSC Traffic Types are identifies the Air/Ground subnetworks over the data may be forwarded and the relative preference of such subnetworks.

The ATN Internet Routing Control mechanisms are supported only by the Inter-Domain Routing Protocol. When routes are advertised between ATN Routers, they include a Security Information field that provides information on:

a) The Traffic Types permitted to use the route;

b) The Air/Ground Subnetwork(s) over which the route passes, if any; and

c) The ATSC Class of the route.

Using this information, ATN Routers are able to forward each NPDU in line with its Security Label and the routing control rules.

4.3.9 ISO 8473 Mandatory Internetwork Protocol Functions

This section describes the functions which are performed as part of the ATN Internetwork Protocol within all Network entities conforming to ISO 8473. These are listed in Table 4-1, which also classifies these functions according their conformance requirement and by protocol subset. ATN Systems have to be able to support both the full and the non-segmenting subset.

The conformance requirements of each function are identified as a numeric type, as follows:

Type 1: These functions are supported in all implementations of the protocol.

Type 2: These functions are not required to be supported. If an implementation does not support a **Type 2** function and the function is selected within an NPDU, then the NPDU is discarded. If the ER flag is set within the NPDU header, then an error report is generated.

Type 3: These functions are not required to be supported. If an implementation does not support a **Type 3** function and the function is selected within an NPDU, then the NPDU is processed exactly as though the function had not been selected.

4.3.9.1 PDU Composition Function

The PDU COMPOSITION function is responsible for the construction of a Network protocol data unit according to the rules governing the encoding of NPDUs. PCI required for delivering the data unit to its destination is determined from current state and local information and from the parameters associated with the **N-UNITDATA** Request.

Network Protocol Address Information (NPAI) for the Source Address and Destination Address fields of the NPDU header is derived from the **NS-Source-Address** and **NS-Destination-Address** parameters. The **NS-Destination-Address** and **NS-Quality-of-Service** parameters, together with current state and local information, are used to determine which optional functions are to be selected. ATN **NS-Userdata** comprises the Data field of the protocol data unit.

Protocol Function Name	Classification of Protocol Function		
	Full Protocol	Non-Segmenting Subset	Inactive Subset
PDU Composition	1	1	1
PDU Decomposition	1	1	1
Header Format Analysis	1	1	1
PDU Lifetime Control	1	1	N/A
Route PDU	1	1	N/A
Forward PDU	1	1	N/A
Segment PDU	1	N/A	N/A
Reassemble PDU	1	N/A	N/A
Discard PDU	1	1	N/A
Error Reporting	1	1	N/A
Header Error Correction	1	1	N/A
Security	2	2	N/A
Complete Source Routing	2	2	N/A
Complete Route Recording	2	2	N/A
Echo Request	2	2	N/A
Echo Response	2	2	N/A
Partial Source Routing	3	3	N/A
Partial Route Recording	3	3	N/A
Priority	3	3	N/A
QOS Maintenance	3	3	N/A
Congestion Notification	3	3	N/A
Padding	3	3	N/A

Table 4-1 ISO 8473 Protocol Functions

During the composition of the protocol data unit, a Data Unit Identifier is assigned to distinguish this request to transmit **NS-Userdata** to a particular destination ATN NS user from other such requests. The originator of the NPDU chooses the Data Unit Identifier so that it remains unique (for this Source and Destination address pair) for the maximum lifetime of the Initial NPDU in the Network; this rule applies for any NPDUs derived from the Initial NPDU as a result of the application of the SEGMENTATION function. Derived NPDUs correspond to the same Initial NPDU, and hence the same **N-UNITDATA** Request, if they have the same Source Address, Destination Address, and Data Unit Identifier. The total length of the NPDU in octets is determined by the originator and placed in the Total Length field of the NPDU header. This field is not changed in any Derived NPDU for the lifetime of the protocol data unit.

When the non-segmenting protocol subset is employed, neither the Total Length field nor the Data Unit Identifier field is present. The rules governing the NPDU composition function are modified in this case, and are as follows:

1. The total length of the NPDU in octets is determined by the originator and placed in the Segment Length field of the NPDU header.

2. The segmentation field is not changed for the lifetime of the NPDU.

3. No Data Unit Identification is provided.

The Data Unit Identifier is also used for functions such as error reporting.

4.3.9.2 PDU Decomposition Function

The PDU DECOMPOSITION function is responsible for removing the PCI from the NPDU, in preparation for processing of that information.

Information pertinent to the generation of the **N-UNITDATA** Indication is determined as follows:

1. The **NS-Source-Address** and **NS-Destination-Address** parameters of the **N-UNITDATA** Indication are recovered from the NPAI in the Source and Destination Address fields of the NPDU header.

2. The data field of a received NPDU is retained until all segments of the original service data unit have been received; collectively, these form the **NS-Userdata** parameter of the **N-UNITDATA** Indication.

3. Information relating to the QOS provided during the transmission of the NPDU is determined from the QOS and other information contained in the Options Part of the NPDU header. This information constitutes the **NS-Quality-of-Service** parameter of the **N-UNITDATA** Indication.

4.3.9.3 Header Format Analysis Function

The HEADER FORMAT ANALYSIS function determines whether the full protocol described in this chapter is employed, or one of the defined subsets thereof. If the Network protocol data unit has a Network Layer Protocol Identifier indicating that this is a standard version of the ATN CLNP, this function determines whether a received NPDU has reached its destination, using the Destination Address provided in the NPDU. If the Destination Address provided in the NPDU identifies an NSAP served by this Network entity, then the NPDU has reached its destination; if not, it must be forwarded.

If the Network protocol data unit has a Network Layer Protocol Identifier indicating that the Inactive Network Layer Protocol subset is in use, then no further analysis of the NPDU header is required and the NPDU is discarded.

4.3.9.4 PDU Lifetime Control Function

The PDU LIFETIME CONTROL function is used to enforce the maximum NPDU lifetime. This function is closely associated with the HEADER FORMAT ANALYSIS function. This function determines whether an NPDU received may be forwarded or whether its assigned lifetime has expired, in which case it is discarded.

The operation of the PDU LIFETIME CONTROL function evaluates and takes action based on the contents of the PDU Lifetime field in the NPDU header. This field contains, at any time, the remaining lifetime of the NPDU (represented in units of 500 milliseconds). The lifetime of the Initial NPDU is at least three (3) times the ATN Internet span or three (3) times the maximum expected transit delay (in units of 500 milliseconds), whichever is greater. This value is set by the originating Network entity, and placed in the PDU Lifetime field of the NPDU. When the SEGMENTATION function is applied to an NPDU, the value of the PDU Lifetime field of the Initial NPDU is copied into all of the Derived NPDUs.

The lifetime of the NPDU is decremented by every Network entity which processes the NPDU. When a Network entity processes an NPDU, it decrements the PDU Lifetime field by at least one count. The value of the PDU Lifetime field is decremented by more than one count if the sum of:

1. the transit delay in the underlying service from which the NPDU was received; and

2. the delay within the system processing the NPDU

exceeds or is estimated to exceed 500 milliseconds. In this case, the PDU Lifetime field is decremented by one for each additional 500 milliseconds of delay. The determination of delay is not required to be precise, but where a precise value cannot be ascertained, the value used is an overestimate, not an underestimate.

If the PDU Lifetime field reaches a value of zero before the NPDU is delivered to the destination, the NPDU is discarded. The ERROR REPORTING function is invoked, and results in the generation of any required ER NPDUs.

4.3.9.5 Route PDU Function

The ROUTE PDU function determines the Network entity to which a protocol data unit must be forwarded and the underlying service that must be used to reach that Network entity. The ROUTE PDU function is closely associated with the routing functions of the ES-IS and IS-IS routing information exchange protocols.

The ROUTE PDU function uses the Destination Address, the total length of the NPDU, and connectivity/topology information contained in the Routing Information Base in order to select a destination Network entity and underlying subnetwork service for forwarding an NPDU. Where segmentation is required, the ROUTE PDU function further determines over which underlying service the Derived NPDU segments must be sent in order to reach that Network entity. The results of the ROUTE PDU function are passed to the FORWARD PDU function (along with the NPDU itself) for further processing. Selection of the underlying service that must be used to reach the "next" system in the route is initially influenced by the **NS-Quality-of-Service** parameter of the **N-UNITDATA** Request, which specifies the QOS requested by the sending ATN NS user. The ROUTE PDU function determines whether this QOS is to be provided directly by the ATN CLNP (through the selection of the Quality of Service Maintenance parameter and other optional parameters) or through the QOS facilities offered by each of the underlying services, prior to invocation of the FORWARD PDU function. Route selection also takes into consideration the value of the Quality of Service Maintenance parameter, and other optional parameters provided in the NPDU.

4.3.9.6 Forward PDU Function

The FORWARD PDU function provides access to and control of local interfaces to supporting subnetworks and/or convergence protocols. The FORWARD PDU function issues an **subnetwork-UNITDATA** Request primitive, supplying the subnetwork or SNDCF identified by the ROUTE PDU function with the protocol data unit as user data to be transmitted, the address information required by that subnetwork or SNDCF to identify the adjacent system within the subnetwork-specific addressing domain (this may be an intermediate-system or the destination end-system), and QOS constraints (if any) to be considered in the processing of the user data. When the NPDU to be forwarded is longer than the maximum service data user size provided by the underlying service, the SEGMENTATION function is applied.

4.3.9.7 Segmentation Function

For an ATN Network Entity implementing the full protocol, segmentation is performed when the size of the PDU is greater than the maximum service data unit size supported by the underlying service to be used to transmit the NPDU. The underlying service may be provided indirectly by the Subnetwork Dependent Convergence Facility, or directly by the Subnetwork Access Protocol. Segmentation comprises the composing of two or more new NPDUs (Derived NPDUs) from the NPDU received. The NPDU received may be the Initial NPDU, or it may be a Derived NPDU.

All of the header information from the NPDU to be segmented, with the exception of the segment length and checksum fields of the fixed part, and the segment offset of the segmentation part, is duplicated in each Derived NPDU, including all of the address part, the data unit identifier and total length of the segmentation part, and the options part (if present). The rules for forwarding and segmentation guarantee that the header length is the same for all segments (Derived NPDUs) of the

Initial NPDU, and is the same as the header length of the Initial NPDU. The size of an NPDU header will not change due to operation of any protocol function. The user data encapsulated within the NPDU received is divided such that the Derived NPDUs satisfy the size requirements of the user data parameter field of the primitive used to access the underlying service.

Derived NPDUs are identified as being from the same Initial NPDU by means of

1. the source address,

2. the destination address, and

3. the data unit identifier.

The following fields of the NPDU header are used in conjunction with the Segmentation function:

Segment Offset: Identifies the octet at which the segment begins, with respect to the start of the Initial NPDU.

Segment Length: Specifies the number of octets in the Derived NPDU, including both header and data.

More Segments Flag: Set to **[1]** if this Derived NPDU does not contain, as its final octet of user data, the final octet of the Initial NPDU.

Total Length Specifies the entire length of the Initial NPDU, including both header and data.

Derived NPDUs may be further segmented without constraining the routing of the individual Derived NPDUs.

The Segmentation Permitted flag is set to **[1]** to indicate that segmentation is permitted. If the Initial NPDU is not to be segmented at any point during its lifetime in the Network, the flag is set to **[0]** by the source Network entity. The setting of the Segmentation Permitted flag cannot be changed by any other Network entity for the lifetime of the Initial NPDU and any Derived NPDUs.

4.3.9.8 Reassembly Function

The Reassembly function reconstructs the Initial NPDU from the Derived NPDUs generated by the operation of the Segmentation Function on the Initial NPDU (and, recursively, on subsequent Derived NPDUs).

A bound on the time during which segments (Derived NPDUs) of an Initial NPDU must be held at a reassembly point before being discarded is provided, so that reassembly resources may be released when it is no longer expected that any outstanding segments of the Initial NPDU will arrive at the reassembly point. Upon reception of a Derived NPDU, a reassembly timer is initiated with a value which indicates the amount of time which must elapse before any outstanding segments of the Initial NPDU are assumed to be lost. When this timer expires, all segments (Derived NPDUs) of the Initial NPDU held at the reassembly point are discarded, the resources allocated for those segments are freed, and if requested, an ER is generated. While the exact relationship between reassembly lifetime and NPDU lifetime is a local matter, the Reassembly Function should preserve the intent of the NPDU lifetime. Consequently, the reassembly function should discard NPDUs whose lifetime would otherwise have expired had they not been under the control of the reassembly function.

The Segmentation and Reassembly functions are intended to be used in such a way that the fewest possible segments are generated at each segmentation point and reassembly takes place at the final destination of an NPDU. However, other schemes which:

1. interact with the routing algorithm to favour paths on which fewer segments are generated;

2. generate more segments than absolutely required in order to avoid additional segmentation at some subsequent point; or

3. allow partial or full reassembly at some intermediate point along the route;

are not precluded. The information necessary to enable the use of one of these alternative strategies may be made available through the operation of a Network Layer Management function or by other means.

The originator of the Initial NPDU determines the value of the Segmentation Permitted flag in the Initial NPDU and all Derived NPDUs (if any). Partial or full reassembly in an ATN Intermediate-system cannot change this value in the Initial NPDU or any NPDU derived from it, and cannot therefore add or remove the segmentation part of the header.

4.3.9.9 Discard PDU Function

The DISCARD PDU function performs all of the actions necessary to free the resources reserved by the Network entity when an error condition prevents further processing of the NPDU. The DISCARD PDU function is executed when any of the following error conditions is encountered:

1. A violation of protocol procedure has occurred.

2. An NPDU is received whose checksum is inconsistent with its contents.

3. An NPDU is received, but due to local congestion, it cannot be processed.

4. An NPDU is received with a correct header checksum, but whose header contents are invalid.

5. An NPDU is received which cannot be segmented and cannot be forwarded because its length exceeds the maximum service data unit size supported by any underlying service available for transmission of the NPDU to the next Network entity on the chosen route.

6. An NPDU is received whose destination address is unreachable or unknown.

7. Incorrect or invalid source routing was specified. This may include a syntax error in the source routing field, an unknown or unreachable address in the source routing field, or a path which is not acceptable for other reasons.

8. An NPDU is received whose NPDU lifetime has expired or a segmented NPDU is received whose lifetime expires during reassembly.

9. An NPDU is received which contains an unsupported Type 2 option.

4.3.9.10 Error Reporting Function

The ERROR REPORTING function initiates the return of an ER NPDU to the source Network entity when a protocol data unit is discarded. The ER NPDU identifies a discarded NPDU, specifies the type of error detected, and identifies the discarding Network entity. Error Report procedures are not used to convey information regarding success or failure of delivery of an NPDU issued by a source Network entity.

The originator of a DT NPDU controls the generation of ER NPDUs. An ER flag in the original NPDU is set by the source Network entity to indicate that an ER NPDU is to be returned if the Initial NPDU or any NPDUs derived from it are discarded; if the flag is not set, Error Reports are suppressed. The suppression of ER NPDUs is controlled by the originating Network entity and not by the ATN NS user.

The ERROR REPORTING function performs as follows:

1. An ER NPDU is not generated to report the discard of an ER NPDU.

2. An ER NPDU is not generated to report the discard of a DT NPDU unless that NPDU has the ER flag set to allow Error Reports.

3. The entire header of the Discarded NPDU is placed in the data field of the ER NPDU. The data field of the Discarded NPDU is not included in the data field of the ER NPDU.

4. If a DT NPDU is discarded for one of the reasons in Paragraph 4.3.9.9, and the ER flag has been set to allow Error Reports, an ER NPDU is generated.

If a DT NPDU with the E/R flag set to allow Error Reports is discarded for any other reason, an ER NPDU may be generated (as an implementation option).

4.3.9.10.1 Initiation of Error Reports

An ER NPDU is composed from information contained in the header of the discarded *Data* (DT) NPDU to which the Error Report refers. The content of the Source Address field of the discarded DT NPDU is used as the Destination Address of the ER NPDU. This value (which in the context of the DT NPDU was used as an NSAP Address) is used in the context of the ER NPDU as the NET of the Network entity that originated the DT NPDU. The NET of the originator of the ER NPDU is conveyed in the Source Address field of the header of the ER NPDU.

Segmentation of ER NPDUs is not permitted; hence, no Segmentation Part is present. The total length of the ER NPDU in octets is placed in the Segment Length field of the ER NPDU header. This field is not changed during the lifetime of the ER NPDU. If the originator of the ER NPDU determines that the size of the ER NPDU exceeds the maximum service data unit size of the underlying service, the ER NPDU is truncated to the maximum service data unit size and forwarded with no other change.

The requirement that the underlying service assumed by the CLNP must be capable of supporting a service data unit size of at least 512 octets guarantees that the entire header of the discarded DT NPDU can be conveyed in the data field of any ER NPDU.

4.3.9.10.2 Processing of Received Error Reports

When an ER NPDU is decomposed upon reaching its destination, information required to interpret and act upon the Error Report is obtained as follows:

1. The NET recovered from the NPAI in the Source Address field of the ER NPDU header is used to identify the Network entity which generated the Error Report.

2. The reason for generating the Error Report is extracted from the Options Part of the NPDU header.

3. The entire header of the discarded DT NPDU is extracted from the data field of the ER NPDU to assist in determining the nature of the error.

ER NPDUs are routed and forwarded by ATN Intermediate-system Network entities in the same way as DT NPDUs.

4.3.9.10.3 Relationship of Data NPDU Options to Error Report NPDUs

The generation of an Error Report is controlled by options that are present in the corresponding DT NPDU. The presence of options in the original DT NPDU that are not supported by the system which has discarded that NPDU may cause the suppression of an Error Report even if the original DT NPDU indicated that an Error Report should be generated in the event of a discard.

The processing of an Error Report is controlled by options which are present in the corresponding DT NPDU. In particular, options selected for the original DT NPDU affect which options are included in the corresponding ER NPDU.

The selection of options for an ER NPDU are specified as follows:

1. If the Priority Option or the QOS Maintenance Option is selected in the original DT NPDU, and the system generating the ER NPDU supports the option, then the ER NPDU specifies the option.

2. If the Security Option is selected in the DT NPDU, and the system generating the Error Report supports this option, then the ER NPDU specifies the option using the value that was specified in the original DT NPDU. If the system does not support the Security Option, an Error Report must not be generated for a DT NPDU that selects the Security Option.

3. The Record Route Option, if selected in the DT NPDU, is specified in the ER NPDU.

The values of the optional parameters above may be derived as a local matter, or they may be based upon the corresponding values in the original DT NPDU.

4.3.9.11 PDU Header Error Detection

The PDU HEADER ERROR DETECTION function protects against failure of ATN IS or ES entities due to the processing of erroneous information in the NPDU header. The PDU HEADER ERROR DETECTION function uses a checksum computed on the entire NPDU header. The checksum is verified at each point at which the NPDU header is processed. If the checksum calculation fails, the NPDU is discarded. If NPDU header fields are modified (e.g., due to operation of the PDU LIFETIME function), then the checksum is modified so that the checksum remains valid. The use of the Header Error Detection function is optional, and is selected by the originating Network entity. If the function is not used, the checksum field of the NPDU header is set to zero.

If the function is selected by the originating Network entity, the value of the checksum field causes the following conditions to be satisfied:

$$\Sigma\ a_{i\ (1 \le i \le L)}\ (\mathrm{mod}\ 255) = 0 \qquad \textbf{(9.1)}$$

$$\Sigma\ (L - i + 1)a_{i\ (1 \le i \le L)}\ (\mathrm{mod}\ 255) = 0 \qquad \textbf{(9.2)}$$

where L = the number of octets in the NPDU header, and a_i = the value of the octet at position i. The first octet in the NPDU header is considered to occupy position i = 1. When the function is in use, neither octet of the checksum field is set to zero.

An efficient algorithm for calculating and checking the checksum octets is provided in Annex D of ISO 8073 and ISO 8602. The checksum is easy to compute and does not impose a serious burden on implementations. However, it will not detect insertion or loss of leading or trailing zero octets, nor will it detect some forms of octet misordering.

4.3.10 ISO 8473 Optional Internetwork Protocol Functions

ISO 8473 internetwork protocol options are selected by the ATN ES Network entity which originates ISO 8473 NPDUs. As a part of the ISO 8473 header, options are conveyed between peer Network entities via ATN subnetworks, and are evaluated in turn by each receiving ATN intermediate-system. The information contained in options conveyed via the ISO 8473 CLNP header is delivered unchanged to each successive ATN entity along the end-to-end path between source and destination ES.

4.3.10.1 Padding Function

The PADDING Function allows extending the length of ISO 8473 NPDUs beyond the length required to convey the NSDU, in order to accommodate those ESs and ISs which place sizing constraints upon NPDUs to facilitate processing.

4.3.10.2 Security Function

The SECURITY function supports imposition of Network Layer security provisions by way of an options field conveyed within the ISO 8473 header. The information contained within this options field may be specified in a global context (i.e. by the international standard), or within the context of the addressing authority responsible for the assignment of the NPDU's source or destination NSAP Address. These contexts are known respectively as the Globally Unique, Source and Destination Unique Formats.

ATN Conformant systems are only required to recognise this options field when it is specified in the global context. Although a source or destination NSAP Address assigned using the ATN NSAP Addressing Plan could be used to identify ATN Security Information in the source or destination context, this manual does not mandate support of the source or destination specific formats for the ISO 8473 security parameter, and hence to avoid service irregularities, neither format should be used.

The Security options field is included in the ISO 8473 header by an ES when the NS User provides a Security Label with an NSDU. In the ATN, this is always encoded using the Globally Unique Format, and is the encoding of the ATN Security Label provided on the N-UNITDATA.Request. As discussed in 4.3.8, the security options parameter is referenced by the inter-domain forwarding function and used to determine the route that an NPDU follows. It is, however, never modified by an IS.

When the NPDU reaches its destination, the value of the Security options field is provided to the destination NS use as the Security Label associated with the NSDU.

4.3.10.3 Source Routing Function

The SOURCE ROUTING Function allows specification of a particular path (i.e., sequence of ISs) through which a particular NPDU either should pass or must pass. The former is described as Partial Source Routing, and the latter is described as Complete Source Routing. The path is defined by a supplied list of NETs, which is conveyed within the NPDU header.

4.3.10.4 Record Route Function

The RECORD ROUTE function records the path taken by an NPDU as it traverses a series of ATN ISs. A recorded route consists of a list of NETs held in a parameter within the options part of the NPDU header. The length of this parameter is determined by the originating Network entity, and does not change as the NPDU traverses the Network. The list is constructed as the NPDU is forwarded along a path towards its destination. Only the titles of ATN Intermediate-system Network entities are included in the recorded route; the NET of the originator of the NPDU is not recorded in the list.

When an ATN IS processes an NPDU containing the Record Route option, the IS adds its own NET at the end of the list of recorded NETs. An indicator is maintained to identify the next available octet to be used for recording of route. This indicator is updated as entries are added to the list using the following procedure:

1. The length of the entry to be added to the list is added to the value of the next available octet indicator, and this sum is compared with the length of the Record Route parameter.

2. If the addition of the entry to the list would exceed the size of the parameter, the next available octet indicator is set to indicate that route recording has been terminated. The NET is not added to the list.

3. If the addition of the entry would not exceed the size of the Record Route parameter, the next available octet indicator is updated with the new value, and the NET is added to the head of the list after the other entries have been moved.

Two forms of the RECORD ROUTE function are possible. The first form is referred to as Complete Route Recording. It requires that the list of NETs be a complete and accurate record of all ATN ISs visited by an NPDU (including Derived NPDUs), except when a shortage of space in the record route option field causes termination of recording of route, as described in Step 2 above. When Complete Route Recording is selected, NPDU reassembly at ATN ISs may be performed only when the Derived NPDUs that are reassembled all took the same route; otherwise, the NPDU is discarded, and if selected, an Error Report is generated. The second form is referred to as Partial Route Recording. It also requires a record of ATN ISs visited by an NPDU. When Partial Route Recording is selected, NPDU reassembly at ATN ISs is always permitted. When reassembly is performed at an ATN IS, the route recorded in any of the Derived NPDUs may be placed in the NPDU resulting from the reassembly.

When a shortage of space in the option field causes termination of the RECORD ROUTE function, the NPDU may still be forwarded to its final destination, without further addition of NETs.

The Record Route function is intended to be used in the diagnosis of subnetwork and/or routing problems.

4.3.10.5 Quality of Service Maintenance Function

The QUALITY OF SERVICE MAINTENANCE function allows the originating Network entity to indicate to ATN Intermediate-systems the relative importance of certain qualities of service for routing decisions made on an individual internetwork packet basis. This information is conveyed to ATN Intermediate-system Network entities in a parameter in the options part of the NPDU header. This option is used to resolve routing ties, where more than one path is available for routing of an NPDU toward its destination. Network entities make use of this information in selecting a route when more than one route satisfying other routing criteria is available.

The ISO 8473 CLNP QUALITY OF SERVICE MAINTENANCE function may be encoded in one of three ways, denoted Source Address Specific, Destination Address Specific and Globally Unique. The first two choices allow selection of an option coding scheme which is associated with the authority defining either source or destination NSAP addresses, while the latter choice uses an internationally agreed upon coding of the relative importance of three subnetwork QOS parameters. These qualities of service include Expense, Transit Delay and Residual Error Probability.

The **Globally Unique** format for the QUALITY OF SERVICE MAINTENANCE function indicates the relative importance of three subnetwork QOS parameters: Expense; Transit Delay; and Residual Error Probability. This option is expressed as a four bit mask within one octet in the protocol header; there is no specified default value for this mask. If no value for **Quality of Service Maintenance** is indicated within the CLNP packet, Network entities use local route selection rules, making their best effort to deliver the CLNP packet. The omission of the **Quality of Service**

Maintenance option is equivalent to requesting that ATN ISs optimise offered throughput. In those instances where the QOS requested cannot be maintained, ATN Network entities will attempt to deliver the NPDU at any available QOS.

4.3.10.6 Priority Function

The PRIORITY function provides a means whereby the resources of ATN ES and ATN IS Network entities, (i.e., outgoing transmission queues and buffers) can be used to process higher-priority NPDUs ahead of lower-priority NPDUs. The PRIORITY function influences the dynamic reordering of the CLNP packet queue within ATN ISs and ESs. This queue management technique allows the proper allocation of packets among available subnetworks, as well as the proper ordering of packets for transfer within a given subnetwork.

The PRIORITY function supports the use of a number between 0 and 14 to indicate the relative importance of each connectionless internetwork protocol packet. The highest Network layer priority is associated with CLNP Level 14, while the lowest priority is associated with CLNP Level 0; Level 15 is a reserved value. CLNP Priority 0 is the default priority, and is used where no priority value is explicitly indicated.

ATN use of the Priority Function is discussed in 4.3.7.

4.3.10.7 Congestion Notification Function

The CONGESTION NOTIFICATION FUNCTION allows originating ATN ESs to take appropriate action when congestion is experienced within the ATN internet.

An ATN IS is viewed as congested when inadequate buffer space is available to maintain and process output queues. ATN ISs detect and indicate congestion based upon the depth of the output queue selected for an NPDU (according to its destination address or other routing information).

ATN Intermediate-systems informs the originating Network entity of congestion between the source and destination NSAP through the use of a flag in the **QOS Maintenance Parameter** option header. When the depth of a particular output queue exceeds a certain proportion of the depth of that queue, an ATN Intermediate-system will start to discard NPDUs; at this time, the ATN Intermediate-system sets the *Congestion Experienced* flag in the next NPDU to be forwarded toward one or more source Network entities and continues to do so until the congestion condition is alleviated.

The value of the *Congestion Experienced* flag is initially set to zero **[0]** by the originator of the NPDU and is set to one **[1]** by any ATN Intermediate-system which processes the NPDU to indicate that that ATN Intermediate-system is experiencing congestion. The method of initiating Congestion Notification is a local matter.

4.3.10.8 Echo Request and Response

The Echo Request function is invoked by Network Layer Management to obtain information about the dynamic state of the Network Layer with respect to (a) the reachability of specific Network entities, and (b) the characteristics of the path or paths that can be created between Network Entities through the operation of Network Layer routing functions. Together with the Echo Response function, it fulfils the same role as “Ping” and “Traceroute” in the Internet Protocol suite.

An Echo Request is generated as a result of a request made on a local management interface. Its destination is the NET of another Network Entity i.e. the Network Entity for which reachability is to be determined, or the route traced. When the Echo Request is received by that Network Entity, an Echo Response is returned to the sending Network Entity.

A returned Echo Response may then be analysed to determine information about the route between two network entities.

4.3.11 Notes on the CLNP APRLs

The following notes have been prepared to provide implementors with background information on conformance requirements which may differ from normal practice.

4.3.11.1 Security

Mandatory implementation of the security parameter is required to support ATN Routing Control functions. As a type 2 function, every ATN System must support this parameter is connectivity is to be maintained.

4.3.11.2 Complete Route Recording

Complete Route Recording is not permitted on the ATN due to concerns over the packet sizes that could be required and the consequential impact on air-ground data links and the transfer of safety related data.

4.3.11.3 Source Routing

Neither Complete Source Routing nor Partial Source Routing are permitted on the ATN. This is because source routing could be used to overcome or otherwise interfere with ATN Routing Control.

4.3.11.4 Priority

Priority is a mandatory ATN requirement. All ATN Systems must not only recognise the priority parameter, but must also prioritise their output queues and implement priority based discard algorithms, if it is necessary to discard packets during periods of congestion. This feature is essential to ensure that safety related data is not impeded if the ATN is congested with routine data.

4.3.11.5 Padding

NPDU padding is not permitted on the ATN as it would interfere with the compression algorithm used by the Mobile SNDCF. The Local Reference Compression mechanism includes no facilities for compressing padding and such NPDUs are sent uncompressed, resulting in a significant increase in the overhead on air-ground data links.

4.4 The Implementation of the Routing Information Exchange Protocols

In support of the ISO 8473 connectionless network layer protocol, ISO has defined a family of three routing information exchange protocols, specified by ISO 9542, ISO/IEC 10589 and ISO/IEC 10747, respectively.

ISO 9542 specifies a protocol for use between ESs and ISs. This protocol enables ISs to identify the NSAP Addresses located on each adjacent ES, and for ESs to determine the location of each adjacent IS. ESs then have a simple routing decision in the absence of any precise knowledge about the location of a packet's destination: they choose an adjacent IS and send the packet to it. It is then the IS's responsibility to route the packet either to its destination, or to an IS nearer to it. When the packet is passed to an ES or IS that is also known to be adjacent to the originating ES, then ISO 9542 allows the IS to notify the ES of the direct path, so that it may be used for all further packets to that destination.

ISO/IEC 10589 is a routing information exchange protocol for use between ISs within the same RD. This protocol freely exchanges all routing information known by each IS to all other ISs. Each IS then has a complete routing map of the RD from which it can calculate optimal routes. This is a simple and robust approach that exploits the requirements for common routing procedures and trust. However, it is hence not suitable for inter-RD routing information exchange. ISO has thus defined a different routing information exchange protocol for communication between RDs. This is specified in ISO/IEC 10747, and is known as the Inter-Domain Routing Protocol (IDRP).

Reflecting the environment of limited trust and different route selection algorithms, rather than exchanging general topology data, IDRP exchanges processed data; IDRP advertises routes to destinations and enables an RD to advertise only the routes that it wants to. It is thus said to support policy based routing. Each RD implements its own routing policy which reflects its security policy and other technical considerations.

4.4.1 ES-IS Implementation Considerations

4.4.1.1 Overview

ISO 9542 specifies a very simple datagram protocol which is suitable for use on all sorts of networks, although it achieves its greatest potential on Broadcast subnetworks. The protocol supports two functions: Configuration Information and Redirection Information.

The Configuration Information function enables End Systems to discover the existence of Intermediate Systems and vice-versa. On broadcast subnetworks, such as an Ethernet, each End System regularly sends an "End System Hello" message reporting the network addresses it hosts to the multicast address *all intermediate systems*. Similarly, each Intermediate System regularly sends an "Intermediate System Hello" message reporting its own identity to the multicast address *all end systems*. End Systems and Intermediate Systems always listen to their respective multicast addresses and can hence "discover" the existence of Intermediate Systems and End Systems, respectively.

In OSI, End Systems have a very simple routing decision: if they do not know the location of the destination of a packet, they send it to any Intermediate System they have discovered through the Configuration Information function.

The Intermediate System should then relay the packet on to its destination. However, if the destination is on the same subnetwork as the source, or another Intermediate System would have been a better choice, then the Route Redirection Information function can be used to inform the End System of the better routing decision. A redirection message is sent to the End System by the Intermediate System, which identifies the subnetwork address that is more appropriate for the destination network address. The End System can then use this subnetwork address in future.

The protocol can also support routing in the absence of an End System. In such cases, instead of the End System sending the packet to any Intermediate System, it sends it to the multicast address *all end systems*. If the End System which is the packet’s true destination receives the packet then it returns an End System Hello to the sender to report the correct subnetwork address, and communication can proceed.

The Configuration Information function may also be used on general topology subnetworks e.g. "X.25 Networks". In such cases, it can still be used to determine the addresses supported by each system, by passing Hello messages over a virtual circuit. However, dynamic discovery of the systems themselves is not really possible given that the DTE Addresses must be known before a virtual circuit can be established.

In the ATN, the Configuration Information function is also used with mobile networks. The air-ground data links specified by ICAO, all appear externally as X.25 data networks. However, the systems reachable over such networks may come and go depending on their geographic position. Their availability may be notified by a “Join Event”, or it may be determined through a polling strategy, a subnetwork connection established and communication take place. An exchange of ISO 9542 Configuration Information is required as part of this procedure.

4.4.1.2 ATN Use of ISO 9542

In the air-to-ground environment, the operation of the ISO 9542 protocol is mandatory, in order to allow adjacent ground and airborne routers connected via a mobile subnetwork to monitor connectivity changes.

The ISO 9542 routing protocol is the recommended protocol for performing these functions over ATN fixed subnetworks.

ISO 9542 is also required when ISO/IEC 10589 is implemented (see 0).

4.4.2 The ES-IS Protocol

4.4.2.1.1 PDU Formats and Use

ISO 9542 operates among the systems attached to a single subnetwork, independently from the routing organisation. It is used to allow systems on the subnetwork to discover each other (configuration), and if necessary to provide minimal routing information to ESs (route redirection).

ISO 9542 specifies three PDU types: the End System Hello (ESH) PDU, the Intermediate System Hello (ISH) PDU, and the Redirect (RD) PDU.

For each type of ISO 9542 PDU, Table 4-2, Table 4-3, Table 4-4 and Table 4-5 respectively indicate:

ISO 9542 PDUs	Main Contents
ESH	**Source address parameter**: Address(es) of the NSAP(s) supported by the ES originating the ESH PDU (an ESH may convey any number of NSAPs supported by the ES in the limit of subnetwork data units size, but in the end, the ES must have reported information about all its NSAPs, via one or several ESHs)
ISH	**Source address parameter:** NET of the IS sending the ISH PDU (the protocol allows only one NET in each ISH)
RD	**Source address parameter:** NET of the IS sending the RD PDU (only one NET); **Destination address parameter:** Destination NSAP address of the PDUs affected by the redirection (and possibly a mask selecting a "class" of NSAPs); Subnetwork address of the new network entity (on the same subnetwork) to which the redirected PDUs will be sent for the first hop from the ES (better path to destination)

Table 4-2 ISO 9542 PDU Types

ISO 9542 PDUs	Generation of PDUs
ESH	By each ES: On timer expiry or on other events, such as the ES or a new local SNPA becoming operational, a distant ES or IS becoming operational, or after another ES has performed a Query Configuration function (Configuration Response)
ISH	By each IS: On timer expiry or on other events, such as the IS or a new local SNPA becoming operational or a distant ES or IS becoming operational (Configuration Notification)
RD	By any IS: After reception of a data PDU, when the IS detects that there is a better path to reach the destination NSAP, or that it cannot route to this destination NSAP (Request Redirect)

Table 4-3 Generation of ISO 9542 PDUs

1. the main contents of the PDU,
2. the type of systems which generates this PDU,
3. the event which triggers its generation,
4. the destination systems of this PDU,
5. its functional role.

The basic transmission mechanism for ISO 9542 configuration information is broadcast. When the underlying subnetwork does not support broadcast or multi-cast the SNDCF may have to provide the required adaptation.

Two broadcast subnetwork destination addresses are possible:

I. "All ESs network entities", or

I. "All ISs network entities".

ISO 9542 PDUs	**Propagation of PDUs**
ESH	• Transmitted on each SNPA the ES is attached to (the transmitted PDUs may be different but they must provide the same information) • Transmitted from an ES in response to a query configuration • Transmitted to all the ISs on the subnetwork
ISH	• Transmitted on each SNPA the IS is attached to • to all the ESs on each subnetwork the IS is attached to
RD	• Transmitted by any IS • Transmitted to the ES originating the PDU when the IS knows a better path

Table 4-4 Propagation of ISO 9542 PDUs

ISO 9542 PDUs	Functional Role
ESH	**CONFIGURATION** • Allows all the ISs to discover the existence and reachability (SNPA) of an ES on the same subnetwork, along with the NSAPs this ES supports • Allows the ESs to discover the existence and reachability of another ES on the same subnetwork, along with the NSAPs this ES supports
ISH	**CONFIGURATION** • Allows all the ISs to discover the existence and reachability (SNPA) of an IS on the same subnetwork along with the NET of that IS (when ISO 9542 is used between ISs) • Allows all the ESs to discover the existence and reachability (SNPA) of an IS on the same subnetwork along with the NET of this IS
RD	**ROUTE REDIRECTION** • Allows an IS to inform the source ES (on the subnetwork) of a better path to reach a destination NSAP (by indicating another IS corresponding to a better first hop on the same subnetwork, or directly the destination ES if it is on the same subnetwork) • It may also relate to a "class" of NSAPs (using Address Masks)

Table 4-5 Role of ISO 9542 PDUs

Consequently, in the "normal" use of the protocol, all the ISO 9542 PDUs generated by each ES are sent to all the ISs on the same subnetwork, and all the ISO 9542 PDUs generated by each IS are sent to all the ESs on the same subnetwork.

4.4.2.1.2 Main protocol functions

ISO 9542 may be implemented by a simple state machine, and a single function is specified to respond to each incoming event. These functions are discussed below.

4.4.2.1.2.1 Report Configuration Function

This function is used by ESs and ISs to inform each other of their reachability and current subnetwork address(es). Additionally, the NET of ISs and the NSAP(s) of ESs are made available to other systems on the subnetwork. This function is invoked on timer expiry or on other event detection.

4.4.2.1.2.2 Record Configuration Function

The record configuration function is implemented in ESs and ISs. It is in charge of the receipt of ESH and ISH PDUs. This function extracts configuration information from the received packets and updates the local Network entity’s RIB.

4.4.2.1.2.3 Flush Old Configuration Function

This function is executed to remove configuration entries in the RIB when this information becomes obsolete. The function is either executed on timer expiry or on other event detection (SNPA re-initialisation).

4.4.2.1.2.4 Query Configuration Function

This function is executed by an ES attached to a broadcast subnetwork when no IS is reachable on the subnetwork and when the ES Route PDU function is not able to determine the SNPA address associated with the current destination NSAP.

When the ES needs to route an NPDU to a destination NSAP whose SNPA is unknown, it performs a broadcast on the subnetwork by sending the NPDU to "All ES entities on the Subnetwork".

Either the destination ES is attached to the subnetwork and the originator ES receives an ESH from the destination system, or no ESH is received and the destination may be declared unreachable.

4.4.2.1.2.5 Configuration Response Function

This function is performed by an ES on receipt of a NPDU addressed to one of its NSAPs, with broadcast destination SNPA address. This is the result of another ES having performed the Query Configuration Function.

The receiving ES builds an ESH PDU and sends it back to the originator ES.

4.4.2.1.2.6 Configuration Notification Function

This function is performed by an ES or IS in order to quickly transmit configuration information (ESH or ISH) to a system which has newly become available and which has issued an ESH or ISH PDU. The Hello PDU is specifically addressed to the newly reachable system.

4.4.2.1.2.7 Request Redirect Function

This function is performed by an IS having received an NPDU from an ES on the subnetwork. It is used to inform the originator ES that this NPDU should directly have been sent to another system on the subnetwork.

The Redirect information contained in the *Redirect PDU* (RD PDU) issued by the IS informs the originator ES of a better path to the NPDU destination.

4.4.2.1.2.8 Record Redirect Function

This function is implemented in ESs and is in charge of recording the redirection information received from an IS. The local Network Entity RIB is updated by this function.

4.4.2.1.2.9 Refresh Redirect Function

The purpose of this function is to increase the longevity of a redirection without allowing an incorrect route to persist indefinitely. In an ES, on receipt of an NPDU the previous hop of which maps the next hop address stored with some redirection information, and the source of which maps the destination address stored with the redirection information, the corresponding redirection holding timer is reset.

4.4.2.1.2.10 Flush Old Redirect Function

This function is performed to remove redirection entries in the RIB when this information becomes obsolete. The function is either executed on timer expiry or on event detection (SNPA re-initialisation).

4.4.2.1.2.11 PDU Header Error Detection

This function is performed by ESs or ISs in order to protect themselves against failures due to the processing of erroneous information in the PDU header. This function performs computation and verification of a checksum and discards the PDU in case of inconsistency.

4.4.2.1.2.11.1 Protocol Error Processing Function

An ISO 9542 PDU which is not discarded by the PDU Header Error Detection Function is discarded by the Protocol Error Processing Function if its encoding does not comply with the provisions of the ISO 9542 protocol.

4.4.2.1.3 ISO 9542 Operation Among ESs

When ISO 9542 is used among the ESs of a single subnetwork, the ESH PDUs are transmitted with the same destination subnetwork address ("All ISs"), and the ESs that wish to receive information about the other ESs validate the reception of the ESHs by validating this address; thus they are aware of the existence and reachability of the other ESs.

This allows optimisation, namely by anticipating the information contained in the RD PDUs, when the destination NSAP is supported by an ES on the same subnetwork.

The operation of ISO 9542 among the ESs generates no additional information transmission (compared with the "standard operation").

4.4.2.1.4 ISO 9542 Operation as an Initiation Phase for the Routing Protocols

In the same way, when ISO 9542 operates among the ISs attached to a single subnetwork, the ISs validate the reception of the ISHs normally destined for the ESs, by validating the corresponding subnetwork address ("All ESs").

This allows the ISs to discover their neighbour ISs existence and reachability and may be used as an initialisation phase for the routing protocols.

4.4.2.2 ISO 9542 Operation over Fixed Ground Subnetworks

4.4.2.2.1 Overview

The use of ISO 9542 over ATN ground subnetworks is a recommended practice. However, either static routing information or other routing protocols could be used to provide the same type of functions as ISO 9542.

If ISO 9542 is not operated over ground subnetworks, a facility must fulfil the following requirements

1. each system must be able to discover the existence of neighbour systems attached to the same subnetwork,

2. the NSAP and SNPA addresses of neighbour ESs and the NET and SNPA addresses of neighbour ISs must be made available to each IS directly connected to the local subnetwork,

3. each IS must be able to dynamically monitor connectivity changes over the local subnetwork

4.4.2.2.2 General Topology Subnetworks

In the case ISO 9542 is operated over ground ATN subnetworks, it seems reasonable to advise against the support of configuration information over general topology subnetwork (non-broadcast subnetwork). Furthermore, it can be very costly to simulate broadcast over non-broadcast subnetworks. However, in some cases (high-bandwidth subnetworks), this solution can be chosen.

On the other hand, the support of ISO 9542 redirection information on general topology subnetwork may be advised, since it is not costly and may prove useful to ascertain local topology.

4.4.2.2.3 Broadcast Subnetworks

As far as broadcast subnetworks are concerned, the full use of ISO 9542 is recommended, since this protocol was designed for operation over this kind of subnetwork. The use of ISO 9542 over broadcast subnetworks is not too costly and allows to dynamically ascertain local configuration changes.

4.4.2.2.4 Point to Point Subnetworks

As far as point to point subnetworks are concerned, the use of ISO 9542 is recommended, and especially the support of the configuration information. The use of ISO 9542 protocol over point-to-point subnetworks is not too costly.

4.4.2.3 ISO 9542 Operation over Air-ground Mobile Subnetworks

When a new aircraft enters the coverage of a ground router directly connected to a mobile subnetwork, an initialisation phase is triggered so that communication can be established between peer ground and airborne routers.

Once this initialisation phase has been performed, it is necessary for each router to forward its local NET information to the newly reachable routers on the subnetwork.

This action is performed via the exchange of an ISO 9542 ISH PDU, and is discussed in more detail in section two, which deals with the Route Initiation procedure.

4.4.2.4 Notes on the ISO 9542 APRLs

These notes provide background information for implementors on the ISO 9542 APRLs contained in the ATN Internet SARPs. It should also be noted that the APRLs are specific to the use of ISO 9542 to support Route Initiation over air-ground data links. There are no APRLs specified for other uses of ISO 9542 (e.g. to support ES to IS routing).

4.4.2.4.1 Route Redirection Information

Route Redirection Information has no role to play in Route Initiation and is hence excluded from the requirements.

4.4.2.4.2 Configuration Notification

Configuration Notification has no role to play in Route Initiation and is hence excluded from the requirements.

4.4.3 Intra-Domain Routing Implementation Considerations

Intra-Domain Routing operates internally and independently within each ATN Routing Domain. The protocol used to support Intra-Domain Routing within an ATN Routing Domain is a local issue, provided that the general ATN Routing requirements are met.

However, it is recommended that a Routing Domain operate ISO/IEC 10589 IS to IS Intra-Domain Routing Information Exchange Protocol (also called here "IS-IS") as its Intra-Domain Routing Protocol.

This part of the Guidance Material first describes general Intra-Domain Routing goals. The operation of ISO/IEC 10589 for intra-domain routing information propagation within the ATN RDs is then described. Note that the description of ISO/IEC 10589 operation essentially applies to the ATN fixed environment, i.e., to the ground ATN RDs, and in particular AINSC and ATSC RDs. If an alternative intra-domain routing protocol is used, then it must satisfy these goals.

4.4.3.1 ATN Intra-Domain Routing Goals

A. Intra-Domain Routing must be able to route CLNP packets within the local Routing Domain, in order to perform end-to-end routing in the ATN.

B. Intra-Domain Routing must be integrated within the general structure of ATN Routing. Particularly, it must operate within the ATN Network Layer of the ISs located within the Routing Domain.

C. Intra-Domain Routing must meet the following general routing goals:

1. ATN Intra-Domain Routing must be efficient (i.e. induce as little overhead as possible and fulfil the user needs),

2. ATN Intra-Domain Routing must cope with the differences between the interconnected subnetworks (e.g. bandwidth),

3. ATN Intra-Domain Routing must be resilient to failures and adaptable to configuration changes,

4. ATN Intra-Domain Routing must support error control and diagnosis.

4.4.3.1.1 General Requirements

A. The ATN Intra-Domain Routing may use any type of routing procedure, namely:

1. Static routing or quasi-static routing (allowing alternate paths), where pre-determined paths are loaded into the Routing Information database through System Management,

2. Centralised (dynamic) routing, where each system of the RD reports information about its local environment to a central facility, which in turn computes the routes and returns them to all the systems of the RD,

3. Distributed adaptive (dynamic) routing, where all the systems of the RD dynamically sense their local environment and directly exchange Routing Information among themselves, using an Intra-Domain Routing Information dissemination Protocol.

B. Routing Information should preferably be propagated by an Intra-Domain Routing Information Exchange Protocol. However, this is not mandatory, provided that the general Intra-Domain Routing requirements are met .

C. When used, the Intra-Domain Routing Information Exchange Protocol must provide mechanisms for the exchange of connectivity and topology information among ATN Routers within an RD. It must support dynamic configuration of ATN Internet Routing tables on a domain-wide basis. (see Clause 6.2.3.2. of ISO/IEC 10589 Intra-Domain Routing Information Exchange Protocol).

D. Distributed adaptive routing should preferably be used for Intra-Domain routing in the ATN, for performance considerations. Indeed, these procedures are robust and they automatically and quickly adapt to configuration changes.

E. ISO/IEC 10589 IS to IS Intra-Domain Routing Information Exchange Protocol performs distributed adaptive routing, and more precisely link state routing, where each system independently computes its routes, using a path minimisation algorithm.

F. Intra-Domain Routing may be hierarchically organised to manage large RDs (like ISO/IEC 10589 IS to IS, that allows two intra-domain routing levels).

G. If ISO 9542 ES to IS Routing Protocol is used, it should cooperate with Intra-Domain Routing, so that the ISs of the local RD can dynamically determine their local environment.

H. A RD may use means other than a Routing Information Exchange Protocol to update the Routing Information database (e.g. for RDs with a very simple topology and a limited number of routers). However, the general requirements for ATN Routing must be met. Particularly, the performance should allow timely update of the RIB, for resilience and adaptability.

I. Routing Information dissemination throughout the RD, must allow each IS of the RD to build its local Routing Information database, so that this database can be used to route the CLNP packets within the local domain .

J. Intra-Domain Routing must operate within the Network Layer of each Router and End System of the local RD.

K. Intra-Domain Routing should preferably take into account the distinction made in ISO-OSI Routing between the ESs and the ISs roles, although this is not mandatory .

L. Intra-Domain Routing must be integrated within the ATN Routing Framework described in Chapter two. It must cooperate with the other elements contributing to the ATN Internetworking and Routing, namely the ATN NSAP Addressing Plan, the ATN Internetwork Protocol, and the other ATN Routing Protocols (ISO/IEC 10747 IDRP and ISO 9542 ES to IS Protocol), in order to meet the ATN Intra-Domain Routing Goals defined in 4.4.3.1.

4.4.3.1.2 Intra-Domain Requirements relevant to Inter-Domain Routing

1) Intra-Domain routing must be able to route CLNP packets issued by an ES belonging to the local RD or to an external RD and bound to a destination ES belonging to the local RD or to an external RD.

2) When the local RD acts as a Transit RD, routing of the CLNP packets by the local Intra-Domain Routing procedure may require the encapsulation of the CLNP packets within other CLNP packets conveying locally known NSAP addresses. The decision to encapsulate the CLNP packets and the encapsulation operations (including the locally known NSAP addresses determination) must be performed by Inter-Domain Routing, in the BIS where the packets enter the local RD. The reverse operation must be performed by Inter-Domain Routing, in the BIS where the packets leave the local RD.

Note.— It is important to note however, that when an CLNP packet crosses several RDs , the routing criteria within each RD may differ. Moreover, a RD may use routing metrics that are not *consistent with the QOS parameters conveyed within CLNP packets. Consequently, it may be impossible to optimise a given criterion all along the end-to-end path.*

4.4.3.2 Overview of ISO 10589

ISO/IEC 10589. is for use within a single routing domain, and enables Intermediate Systems (ISs) to learn the topology of their local routing domain, and to identify the quality of service available over each potential path to a given destination.

ISs within a Routing Domain may discover each other dynamically using the ISO 9542 Intermediate System Hello message. They then use specific 10589 hello messages to determine each other's exact status.

The protocol supports a type of routing procedure known as a *link state routing*. In *link state routing*, Intermediate Systems broadcast information about their local environment to all other Intermediate Systems within the routing domain. Each system thereby builds up a complete "topological map" of the entire routing domain.

Under 10589, periodically, and whenever topology changes occur, each IS constructs a Link State Protocol Data Unit (LSP). This is then copied (flooded) to all other ISs within the same routing domain. Where possible, this is by direct transfer, but may involve ISs forwarding LSPs to other ISs, when ISs are not fully interconnected.

In general terms, an LSP identifies the generating IS's neighbour ISs (i.e. those which it has active communications links), the End Systems (ESs) to which the IS also has links, (discovered by ISO 9542) and the quality of service metrics pertinent to each link. Once an IS has available to it the current LSP from every active IS, it can construct the topological map of the routing domain, and then perform routing decisions using a suitable routing algorithm, such as "shortest path first".

Clearly, as the number of ISs and ESs increases, the overhead involved in LSP transfer will increase rapidly, and to ensure that the overhead does not become excessive the ISO standard structures a Routing Domain into one or more Routing Areas.

4.4.3.2.1 Routing Areas

A routing domain is made up of a set of routing areas, each characterised by a set of unique address prefixes known as the *area addresses*; all Network Addresses within the same routing area must be prefixed by one of these area address. When two ISs discover each other, they will determine whether or not they are in the same Routing Area.

Within a given routing area, each IS will generate an LSP specific to the routing area (Level 1 LSP), and flood it to all other ISs within the same routing area. This LSP identifies:

- the address prefixes of their local End Systems (and of the IS itself)
- the identity of adjacent ISs (i.e. those ISs in the local routing area with which the IS is in communication and can exchange ISO 8473 PDUs) and the associated quality of service parameters
- the identity of adjacent End Systems (i.e. those ESs in the local routing area with which the IS is in communication and can exchange NPDUs) and the associated quality of service parameters.

Through level 1 LSPs, each IS thus learns the current topology and connectivity of its local routing area. Note that Level 1 LSPs may be received from ISs in other routing areas, but these will be discarded when it is determined that there is no overlap in the area addresses covered.

Within each level 1 routing area some ISs also operate as level 2 routers, and identify themselves as such in their level 1 LSPs, and during the dynamic discovery phase.

Level 2 routers flood a second type of LSP (Level 2 LSP) to all other Level 2 routers in the routing domain (i.e. both within the local routing area and all other routing areas). A level 2 LSP identifies:

- the set of area addresses that characterise the local routing area
- the identity of adjacent level 2 ISs (i.e. the level 2 ISs in the routing domain with which the IS is in communication and can exchange NPDUs) and the associated quality of service parameters
- the address prefixes of any End Systems, or groups of End Systems, which are reachable through the level 2 IS, but are not included in the set of area addresses. These are typically address prefixes for destination in other routing domains and reachable through this IS.

Level 2 ISs are thus able to learn the current topology of the level 2 subdomain and hence the connectivity of level 1 routing areas. Access points to other routing domains are also identified. NPDUs destined for addresses outside of a local routing area, may be sent by a level 1 only IS to its nearest level 2 IS, and hence to a level 2 IS in the destination routing area, or to one from which the destination address is reachable. It may then be forwarded to the actual destination.

This two level hierarchy allows very large routing domains to be constructed. Most changes are typically limited to the local routing area, and only major changes affect level 2 routing, but without consequential level 1 LSP exchanges in other routing areas. The extent of routing information exchange is thus limited, with only a marginal effect on routing efficiency.

4.4.3.2.2 Partition Repair

Level 1 routing areas may become disjoint, either due to failures or mis-configuration, and 10589 has the ability to repair such failures by routing between level 1 routing area partitions through the level 2 subdomain. This is a necessary function since the level 1/level 2 structure is essentially an artificial one created to maintain efficiency, and it would be highly undesirable to prevent communication when a path exists and the only barrier to communication is a purely artificial constraint.

Partition repair is effected by the level 2 IS that is the partition designated intermediate system. All level 2 ISs within a non-disjoint level 1 routing area can identify each other through their level 1 LSPs, and rules exist to determine the partition designated intermediate system. Level 2 ISs report the current partition designated intermediate system for their local routing area in Level 2 LSPs.

If a partition designated intermediate system receives a level 2 LSP from an IS in the same routing area which reports a different partition designated intermediate system then a disjoint routing area is assumed. NPDUs to be transferred between the partitions are routed through each partition's partition designated intermediate system.

4.4.3.2.3 Support for Inter-Domain Routing

ISO 10589 also recognises that some ISs may also be Boundary ISs, that is they are at the periphery of Routing Domain and have links to other similar Boundary ISs in other Routing Domains. In order to support routing to such Boundary ISs, Level 2 LSPs may carry *Reachable Address Prefixes*. These are address prefixes that characterise the Routing Domains reachable through a given Boundary IS, and the intra-domain routing function is, using this information, able to route NPDUs addressed to systems in other Routing Domains, and via the appropriate Boundary IS.

4.4.4 IDRP Implementation Considerations

4.4.4.1 Overview

ISs within the same Routing Domain communicate with a high degree of mutual trust. They accept unquestioningly the routing information supplied to them, with the consequence that bad routing information will lead to routing problems. This is acceptable in this environment because all these systems will be under the same administrative authority. However, when "firewalls" are required between different parts of an Administrative Domain, or when communication between different Administrative Domains is necessary, then a different approach is required.

ISO/IEC 10747 specifies a routing information exchange protocol for use between Routing Domains i.e. when the environment is one of mutual distrust and/or when firewalls are required. The protocol does not operate between any IS, but only between specially designated *Boundary Intermediate Systems (BISs).* A BIS can be regarded as fulfilling the same role as the Internet's Exterior Gateway.

Multiple BISs within the same Routing Domain are permitted. Their behaviour is co-ordinated so that they operate as if they were the same BIS. A Routing Domain always provides consistent routing information regardless of how many BISs is supports.

The protocol - the Inter-domain Routing Protocol (IDRP) - is naturally connection mode and is specified to operate over ISO 8473. BISs *connect* to one another and exchange routing information over these BIS-BIS connections.

IDRP is a vector distant routing protocol. BISs advertise to another BIS, only the routes that they want to advertise to that BIS. The protocol is said to be policy driven, in that routes are only advertised when permitted by the effective Routing Policy, and contain only the information the Routing Policy allows to be advertised.

4.4.4.2 Routing Policy

Within an OSI RD, in general routing decisions are made on the basis of performance, taking into account the QOS available over a given subnetwork connection and the QOS required by the sender of an NPDU. However, routing between RDs is also subject to the imposition of Routing Policy, where a Routing Policy is a set of rules laid down by an Administrator responsible for a RD that primarily determine:

1. Whether the RD permits NPDUs for which neither the source nor the destination is in the RD to transit through the RD, and if so, the RDs to which transit facilities are offered;

2. The internal NSAP Addresses for which routes are advertised to adjacent RDs, and the scope of any further distribution.

Routing Policy is necessary because even when connectivity exits, when systems are owned by different organisations, those organisations will want to exercise control over the use made of connections so that only those users authorised to use a communications resource may do so, and that data only passes through physical systems and communications networks that are trusted to undertake the required task and provide the QOS demanded. For example, a CAA or Aeronautical Industry administrative domain may choose to restrict the outside ATN domains that may use its routing services based on security or other policy related requirements. In general, an ATN domain may receive Operational Communications, Administrative Communications and/or APC related traffic. Depending on its policies, a domain may choose to exclude the reception or transmission of these traffic types.

The overhead of routing policy is not always necessary, and that is why RDs exist. A RD is in general no more than a set of interconnected systems where routing may be performed on performance considerations, and where a simple and robust intra-domain routing protocol may as a result be implemented.

4.4.4.3 BIS-BIS Communications

BISs exchange routing information in a pair-wise fashion. They use the services of ISO 8473 to communicate routing information; the BIS-BIS protocol includes procedures that ensure the reliable transport of routing information, including recovery from the loss of an ISO 8473 Data PDU. The BIS-BIS protocol is thus connection mode in operation and has similar features to the ISO 8073 Class 4 transport protocol.

BISs must establish BIS-BIS connections prior to the exchange of routing information. If more than one BIS is present in a RD then these BISs must form BIS-BIS connections with each other. The BISs within a RD form BIS-BIS connections with BISs in other RDs according to configuration information provided by a System Manager. When two RDs are linked by a BIS-BIS connection, then the RDs are said to be adjacent to each other. A BIS-BIS connection is established following the exchange of OPEN PDUs between two BISs.

Each BIS maintains two information bases per BIS-BIS connection. These are the adj-RIB-out and the adj-RIB-in. A BIS places the routes it wishes to advertise to another BIS in the adj-RIB-out. The BIS-BIS protocol then copies the contents of the adj-RIB-out to the corresponding adj-RIB-in in the remote BIS, and subsequently ensures that they remain identical. A BIS may then use the routes received into an adj-RIB-in as it wishes.

The BIS-BIS protocol uses the UPDATE PDU to copy routes from the adj-RIB-out. An UPDATE PDU may carry multiple routes and may advise on the removal or replacement of existing routes. When an UPDATE PDU is received, the BIS updates the appropriate Adj-RIBs-In. There is also a RIB REFRESH PDU for periodic re-synchronisation of the adj-RIB-out and adj-RIB-in.

The BIS-BIS protocol maintains the Adj-RIB-out and Adj-RIB-in synchronisation as long as the BIS-BIS connection exists. If the connection is lost then the associated information bases, and the routes are discarded.

The BIS-BIS protocol is full duplex and UPDATE PDUs are transferred in both directions. Contained in the UPDATE PDU is protocol control information to provide flow control and reliability through retransmission. When there are no routes to be exchanged, a separate KEEPALIVE PDU may be exchanged to keep the connection open. The BIS-BIS connection may be explicitly terminated through use of a CEASE PDU.

Routing Policy information is exchanged as part of a route to the extent of information limiting the scope of its onward distribution. However, the main impact of routing policy is on the manipulation of routes within a BIS.

4.5 Mobile SNDCF Implementation Considerations

The ATN specification is predicated on the use of the Connectionless Network Protocol (CLNP) specified in ISO 8473 and the Inter-Domain Routing Protocol (IDRP) specified in ISO/IEC 10747. CLNP provides the unifying end to end internetwork protocol, and IDRP provides the basis for the policy based routing necessary in an internetwork formed from many different organisations, and with safety related operational requirements.

The mobile networks are a key component of the ATN. Air Traffic Control (ATC) applications require a data link between an Air Traffic Control Centre and each aircraft under its control; this requirement is satisfied by the mobile networks. However, the usable bandwidth of each mobile network is low (of the order of 2400 bits/s or lower). ATC applications tend to consist of the regular exchange of short messages and, in such an environment, the size of the CLNP header becomes a serious overhead. Considering this, ICAO has developed a set of procedures, and supporting protocol, to provide compression of CLNP headers over low bandwidth data links. The resulting specification is presented in this document.

When this specification is used, a CLNP header of the order of sixty octets can be compressed down to at most fourteen octets.

4.5.1 Implementation Model

The current generation of ICAO Mobile Networks all provide a network access service compliant with ISO 8208 (ITU-TS recommendation X.25). The CLNP specification already provides a set of procedures for passing CLNP packets over X.25 virtual circuits; ISO 8473 defines such procedures as a Subnetwork Dependent Convergence Function (SNDCF). The procedures for compression of CLNP headers over ICAO Mobile Subnetworks are based on the X.25 SNDCF, and indeed may be negotiated down to this SNDCF. The specification of these procedures is known as the Mobile SNDCF.

The implementation model for the Mobile SNDCF is illustrated in Figure 4-2 Implementation Model of the Mobile SNDCF. Note that the specification is not necessarily restricted to X.25. In principle, this specification may be readily adapted to any connection mode data link.

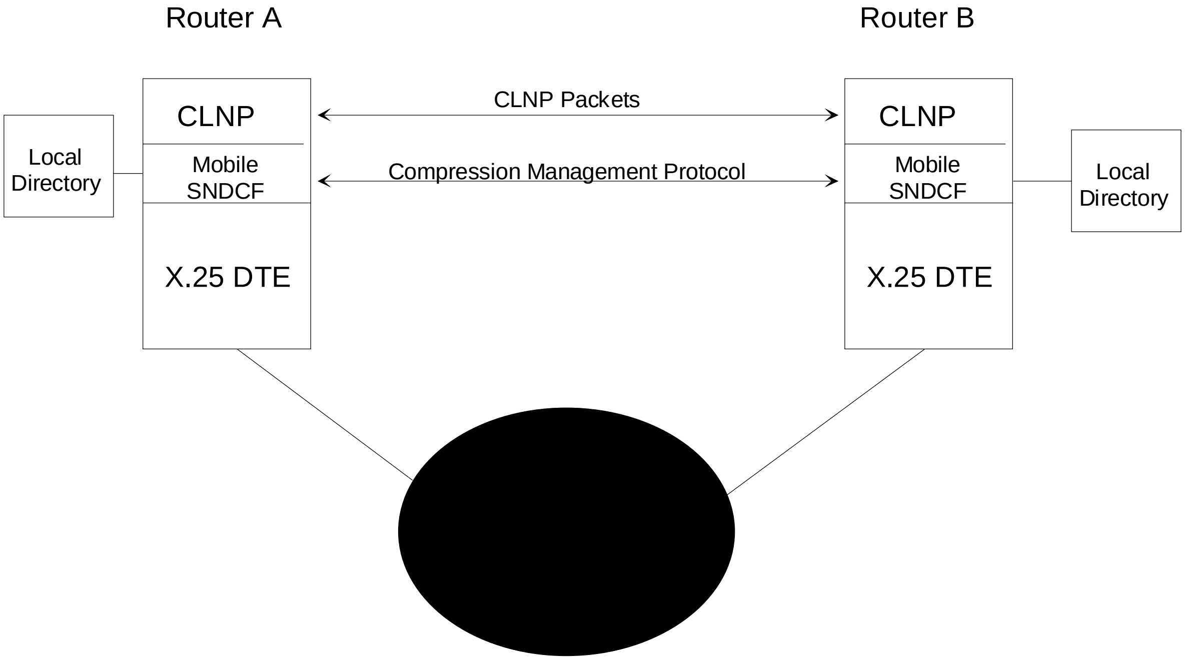

Figure 4-2 Implementation Model of the Mobile SNDCF

The compression procedures are assumed to be implemented over a single data link between two routers, or a host and a router. In very simple topologies, they could be implemented between two hosts. The figure illustrates the typical case, which is between two routers, with the illustration of each router simplified such that only a single subnetwork stack is shown.

From an architectural perspective, the CLNP implementations in each router exchange CLNP Data and Error Packets over an X.25 virtual circuit using the procedures specified by the Mobile SNDCF. In addition, the implementations of the Mobile SNDCF also need to exchange information related to the management of the compression algorithm. A local management protocol is specified for this; this protocol is passed over the same virtual circuit as are CLNP packets with compressed headers.

Note that the format of the compressed headers is such that they can be distinguished from normal CLNP packets, and well as IS-IS, ES-IS and NLSP packets, and the local management protocol.

In each router, the Mobile SNDCF maintains a local directory for use by the compression algorithm. A separate local directory is maintain for each virtual circuit over which CLNP header compression is in use. This is true even when more than one virtual circuit is concurrently available to the same router or host. The local directory contains the state information specific to the operation of the compression algorithm over a single virtual circuit, and the prime purpose of the local management protocol is to maintain synchronisation of the local directories at each end of a virtual circuit.

The local directory consists of entries numbered from zero to a maximum of 32767, each entry consisting of:

1. A pair of NSAP Addresses, known as the inward and outward NSAP Addresses respectively;

2. The ISO 8473 protocol version number;

3. The value of the security options parameter (see ISO 8473 Clause 7.5.3), which may be empty;

The directory is initially empty. The minimum directory size that may be supported is 128 entries.

Note that the algorithm is suitable only for uses of the security parameter that support "simple security", such as passwords or simple traffic class identifiers, which are likely to be constants for packets sent between the same NSAP pair. It is not suitable for "strong security" where the security parameter contains a checksum (encrypted or otherwise) binding the contents of the security parameter to the packet’s user data.

4.5.2 Overview of Compression Algorithm

When a virtual circuit is first opened, call user data is used to declare the use of the Mobile SNDCF instead of the normal ISO 8208 SNDCF, and to pass negotiable parameters (e.g. directory size). If fast select is available, then the called router may negotiate down from the values of the negotiable parameters. If not, then the called router must accept them unconditionally, or refuse the connection.

Whenever a CLNP packet is queued for transmission over the virtual circuit, the local directory for that virtual circuit is queried to see if an entry exists for which:

a. the outward NSAP Address is identical to the packet’s destination NSAP Address, and

b. the inward NSAP address is identical to the packet’s source address, and

c. the protocol version number is the same as that contain in the packet header, and

d. either the security parameter is absent in both cases, or the security parameter in the directory is identical to that in the packet header.

If the above condition is satisfied, and the packet header does not contain the source routing or route recording optional parameters, or more than seven octets of padding, then the CLNP packet may be replaced by a compressed header.

The actual format of the compressed header is dependent on whether the segmentation part is present in the original packet header and, if so, whether the packet is a derived or initial PDU. In all these cases, the compressed header includes the priority (if present) and the QoS Maintenance bits (if present) in a packed form, and the local directory entry number, as the "local reference" field. The segmentation part, when present, is copied unchanged in to the compressed header.

When a packet with a compressed header is received, the local reference is extracted and the corresponding entry found in the local directory. The original PDU header is then reconstructed from the information contained in the local directory and the compressed header.

Note that the reconstruction of the packet header does not aim to restore the padding octets, if any, to their original values. For such reasons the algorithm is not applied to CLNP packets encapsulated by a security protocol such as NLSP, which generates an integrity check on the entire packet.

If, when a CLNP packet with a compressed header is received, the indicated local directory entry does not exist, then this is an error condition reported to the peer SNDCF by the local management protocol. An SNDCF Error PDU is specified for this purpose.

4.5.2.1 Creating Local Directory Entries

A local directory entry is created when a CLNP packet is queued for transfer over the virtual circuit and no suitable entry could be found in the local directory. An entry is then created using the source and destination NSAP Address (inward and outward NSAP Addresses), protocol identifier, and security parameter (if present) in the packet header. Each side of the connection has a range of entry numbers (local references) which it is permitted to allocate, and a suitable (unused) entry number is selected from that range, to correspond to the newly created directory entry.

The allocated directory entry number is then inserted into the packet header as a new optional parameter, and the packet header and segment lengths and header checksum adjusted to ensure that the header is syntactically correct. The packet is then transferred over the virtual circuit.

Whenever an uncompressed CLNP packet is received over a virtual circuit supporting the Mobile SNDCF, its header is inspected for the addition of such a local reference parameter. If found it is removed, the header and segment lengths and checksum adjusted appropriately, and a local directory entry created for that local reference using the source and destination NSAP Address (outward and inward NSAP Addresses), protocol identifier, and security parameter (if present) in the packet header. By such a mechanism the local directories are synchronised. As the definition of the inward and outward NSAP Addresses is asymmetric, a local reference may be used in either direction with the same, albeit reversed, semantics.

Once a local directory entry is created, it remains valid for the lifetime of the virtual circuit; the local directory is disposed of when the virtual circuit is cleared. Communication over mobile subnetworks is typically for a limited period, and directory sizes can generally be chosen such that there is sufficient capacity available for the lifetime of the virtual circuit. If the directory becomes full then packets between further NSAP pairs are simply sent uncompressed.

However, it is possible that in some circumstances, the communications path may be long lived and it will be necessary to re-use directory entries. To satisfy such requirements, the use of the local reference cancellation mechanism may be negotiated when the connection is established.

4.5.2.2 Re-use of Directory Entries

Two local management protocol packets are specified for this purpose. A local reference cancellation request PDU enables one side of the virtual circuit to identify a range of local references (under its control) that it wants to cancel, and hence make available for re-use. When such a PDU is received, the identified local references are cancelled, and a response PDU returned. Once a response PDU has been received by the initiator of the cancellation request, then the local references can be re-used.

Certain error conditions may indicate that the local directories at each end of the virtual circuit have lost synchronisation. if this situation occurs then the virtual circuit is reset, and the local directories returned to their initial state.