EUROCONTROL

ATNP/WG2/
WP/172
10 October 1995

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Banff 9.10.95-13.10.95

Proposed Initial Guidance Material for ATN Internet SARPs

Presented By Henk Hof

Prepared by Tony Whyman

SUMMARY

This is a rough edit of existing material into the format for the Guidance Material agreed at the Rome meeting. It is provided as an initial contribution towards the development of ATN Internet Guidance Material. It should be noted that work on selecting existing ATN Manual text has not been completed and there is still considerable selection and editing work to be done on this subject.

DOCUMENT CONTROL LOG

SECTION	DATE	REV. NO.	REASON FOR CHANGE OR REFERENCE TO CHANGE
	10-Oct-95	Issue 1.0	

TABLE OF CONTENTS

1. Introduction

1.1 Background

In January 1989, the Air Navigation Commission (ANC) expanded the terms of reference of the Secondary Surveillance Radar Improvements and Collision Avoidance Systems Panel (SICASP) to include the development of ICAO material as necessary to permit, to the maximum extent practicable, systems commonality and interoperability between ATS data links, including satellite data links.

The task emerged from the work of the Special Committee on Future Air Navigation Systems (FANS) which emphasised the need for the interchange of digital data over dissimilar aeronautical data links. The committee also recommended that the principles of the International Organisation for Standardisation (ISO) open systems interconnection (OSI) architecture be applied in developing aeronautical data links in order to provide for their interoperability.

Subsequent studies undertaken by the SICAS Panel resulted in the concept of the aeronautical telecommunication network (ATN) which is intended to support computer-to-computer communications operated by civil aviation authorities and aeronautical operating agencies. At its fourth meeting, the SICAS Panel developed a description of the ATN and recommended it be published as an ICAO manual. The first edition of the manual was published in 1991, and the second edition was subsequently developed by the SICAS Panel and recommended for publication at the fifth meeting of the panel, and is expected to be published by ICAO during 1995. The development of the ATN continues with the objective of recommending Standards and Recommended Practices (SARPs) and Guidance Material for the ATN during 1996, for inclusion in Annex 10 at that time.

Following the completion of the work on the ATN Manual (Second Edition) by the SICAS Panel, the Air Navigation Commission transferred the work of developing SARPs and Guidance Material to the ATN Panel (ATNP).

The concept developed by SICASP was of a multi-user multi-vendor internetwork, that would integrate the many different air-ground and ground-ground networking technologies that are currently in place and being planned. In addition, this internetwork would be designed to meet the exacting Quality of Service (QoS) requirements of aeronautical applications, and to respect the ITU and national regulations that applied to each air-ground data link.

1.2 Scope

This document provides guidance material for ATN Implementors, Service Providers and Users.

1.3 Purpose of Document

In line with normal ICAO practice, this document has been developed as a companion to the ATN Internet SARPs. It may be read alongside the SARPs, in order to provide a greater understanding of the specification itself, or it may be read instead of the SARPs by readers that simply want to understand the ATN Concept rather than the detail of the specification.

2. The ATN Concept

2.1 The ATN Specification

The ATN is a CLNP Internetwork that interconnects for the purpose of data interchange:

- Existing, planned and future ATS and Aeronautical Industry Networks
- ICAO Mobile Data Communications Networks
- ATS and Aeronautical Industry ATM Systems, including those onward aircraft in flight.

The specification of these networks and systems is outside of the scope of the ATN Internet, while the specification of the ATN Internet is concerned with the architecture of the ATN, how data packets are routed through the ATN, and the specification of the ATN Routers, which provide the essential packet interchange and routing facilities that enable ATM Systems to communicate across a variety of networking technologies.

The ATN Internet SARPs are therefore concerned with the following functional areas:

- The selection and specification of the data communications protocols used to format and pass user data packets throughout the ATN;
- The selection and specification of the Routing Information Exchange Protocols used to support the proper operation of ATN Routers;
- Security and Quality of Service Maintenance;
- The specification of ATN Routers;
- The specification of the End System Components necessary for ATN Access;
- The specification of the procedures for supporting ATN Mobile Routing.

ATN Mobile Routing itself comprises several functional areas:

- The Management of Routes to Mobile Systems in the Ground ATN;
- The use of Mobile Networks including procedures for Route Initiation (i.e. the establishment of communications with a mobile system);
- Data Compression over low bandwidth Mobile Networks.

Where possible, the ATN uses communications protocols that have already been specified by the International Standards Organisation (ISO) or the International Telecommunications Union (ITU). The ATN Internet SARPs are therefore concerned only with the identification of these protocols and their adaptation (i.e. profiling) for aeronautical use.

The main area of original specification in the ATN Internet SARPs is in the specification of the procedures for supporting ATN Mobile Routing. In particular, the routing policies that support mobile routing in line user and application requirements, the Route Initiation procedures, and the Data Compression procedures for use over low bandwidth networks, are all unique to the ATN Internet SARPs.

2.2 An ATN Overview

This section is concerned with the ATN Architecture and the Service it provides to its users. It provides introductory material to the ATN Concept, especially targeted at the reader that requires only limited information on the internal operation of the ATN.

However, first it is worth considering who or what is an ATN user. In principle, the ATN User is an ATM application, or some other application supporting an aeronautical application. But, this is very much an end system view. From the networking point of view, there are many interfaces over which "a user" accesses a service. At each such interface, each user can be considered to be an ATN User. In the remainder of this chapter, the term "ATN User" is used in this sense, i.e. as a user of the network service or transport service, depending on context.

2.2.1 The ATN: a User's Perspective

The ATN is a data communications internetwork that:

1. provides a common communications service for all ATSC and AINSC applications that require either ground/ground or air-ground data communications services.

2. integrates and uses existing communications networks and infrastructure wherever possible.

3. provides a communications service which meets the security and safety requirements of ATSC and AINSC applications.

4. accommodates the different grades of service required by each ATSC and AINSC application.

While the above might, at first sight, appear ambitious, the reality is that for the ATN's users, the internetwork will be straightforward and simple to use. This is because OSI architecture deliberately places the responsibility for routing and maintaining an internetwork's operational status on the "routers" and therefore enables the End Systems (cf. Host Computers) to have only a minimal networking capability.

2.2.1.1 The Individual ATN User

The ATN provides its users with a robust and reliable communications service, together with the option of a datagram service. Formally, all communications aspects of a user's system are part of the ATN, but from a "user's point of view", the ATN is out there, separate from their own system. It is this "user's view" of the ATN that is illustrated in Figure 2-1. This figure shows the ATN as an abstract "cloud" which indeed is all the user need be aware of, with its complexity hidden from view. At this level, the ATN is a simple network that provides a datagram service to its users.

A ground based ATN user's system, which might be anything from a complete ATC system to an entry level PC, accesses ATN services via some ATN access point. This access point is a notional socket into which the user "plugs" their system and thereby gains access to the ATN. However, this socket is not as tangible as an electrical power socket. A user's access to the ATN is first via an "access subnetwork", such as an Ethernet or an X.25 PSDN, and then an ATN Router. The user's system is directly connected to the access subnetwork, and this may very well involve a physical connection provided by a wall-socket, and, using the access subnetwork, the user's system communicates with the ATN Router. It is then through the ATN Router that access is gained to ATN services.

The communications capabilities of the user's system must obviously include the hardware and software necessary to use the "access subnetwork". Furthermore, the user's system

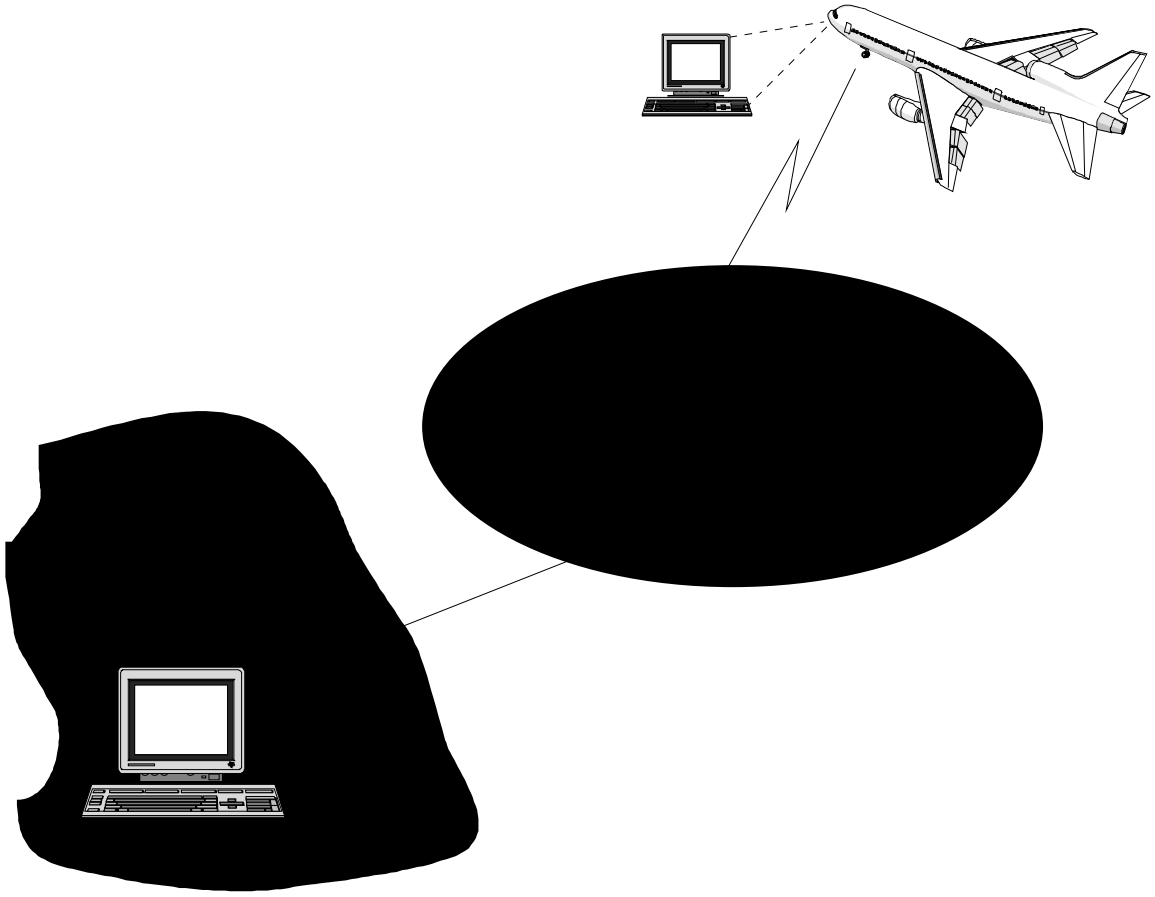

Figure 2-1 Individual End User's View of the ATN

must also support the ISO 8473 Connectionless Network Protocol in order to be part of the ATN Internet, and is recommended to support the ISO 9542 End System to Intermediate System Routing Protocol.

CLNP is a simple protocol supporting the transfer of "datagrams" i.e. packets of data transferred from sender to receiver without the need for a connection to be established in advance. Data transferred using CLNP is formatted as a block of data preceded by a protocol header containing the addresses of the sender and destination, the priority of the data, any security label associated with it, and quality of service requirements. Header and data must together not exceed 64 kilobytes.

An ATN user may, at any time send a CLNP formatted datagram to any valid destination address. The user does this by passing the datagram over the access subnetwork to the ATN Router. The ATN Router will inspect the protocol header, and it is then the ATN Router's responsibility to forward the datagram through the ATN to the ATN Router which provides ATN access to the addressed destination. How it does this is internal to the ATN and hence hidden from the user, although the forwarding process must respect the data priority and the Quality of Service and Security requirements identified in the protocol header. Once the datagram has arrived at the ATN Router which provides ATN access to the addressed destination, it is then transferred over the destination's access subnetwork to the destination user. If the destination user is offline (e.g., switched off), the datagram is discarded and an error report is optionally returned to the sender.

The above is essentially how the user perceives the ATN. The simple CLNP is the protocol ATN users use to communicate, and permits those users to exchange information as discrete blocks of data.

The other protocol that users are recommended to support - the ES-IS protocol - is really just for local administration. The user's system uses the ES-IS protocol to report its own address to the ATN Router, and this information is regularly repeated so that the ATN Router can monitor a user's online status. It is also used to report the existence and operational status of an ATN Router to its users, and enables an ATN user to have access to multiple ATN Routers, possibly over different access subnetworks, so as to provide a high availability service.

The ATN itself does not make any demands on the syntax or semantics of the data carried in a CLNP packet. However, the simplicity of the service does carry a penalty and this is that delivery of datagrams is not guaranteed. When a user transfers an ISO 8473 formatted packet to an ATN Router, that user is only guaranteed a probability of delivery dependent on the data priority. The probability of delivery is high, and while no targets have yet been set for delivery probability, 97% - 98% is certainly realistic. Considerations that affect this figure include:

1. the error rates on subnetworks such as Ethernets which may lose data in transit due to line errors (although this consideration does not apply to X.25 subnetworks and similar examples, which provide a reliable transfer service)

2. network overload which results in low priority data being discarded in order to free up congested resources

3. component failures.

The actual delivery probability that is provided is a design issue. Once actual targets have been provided then it is possible to design a network to meet the requirement. This is achieved by minimizing the use of lower reliability subnetworks, increasing overall network capacity, and through component redundancy.

However, the network can never provide a 100% delivery probability. When an ATN user does require reliable data transfer, then the end to end ISO 8073 class 4 transport protocol is required, in addition to the CLNP. This protocol itself uses CLNP packets to convey information between ATN users. The protocol can detect data loss and recovers from it by retransmission. It can also provide end to end flow control and multiplexing of different data streams between the same pair of users. When this protocol is used, the impact of a comparatively low delivery probability is on mean transit delay (the average time it takes to transfer data from source to destination). This is because recovery from data loss is by retransmission, and hence the lower the delivery probability, the longer the mean transit delay. There is hence a need to offset the impact of an increased mean transit delay against the cost and design implications of higher delivery probability.

ATN users that do not require a high delivery probability (this class includes time critical applications such as radar related data transfer,) could in principle directly use the transfer service provided by CLNP, but this is not permitted in the ATN. ATM applications for which the ISO 8073 COTP Class 4 is not appropriate are instead required to use the ISO 8602 connectionless transport protocol, which specifies a format for data transferred by the CLNP. The advantage of this protocol is that it decouples the internal structure of a user's system and the applications it hosts, from network routing. This is because ISO 8602 enables multiple users to be reached through one network address rather than one per user, which would be less efficient from the network point of view, and the number of such addresses is limited.

2.2.1.2 The User as an Organization

While the previous description is satisfactory from the individual user's point, it does assume that there is some external ATN Service Provider, that provides the ATN Router and hides ATN complexity from the end user. However, while this may indeed be true for many ATN users, when the ATN user is an organization with multiple systems to consider;

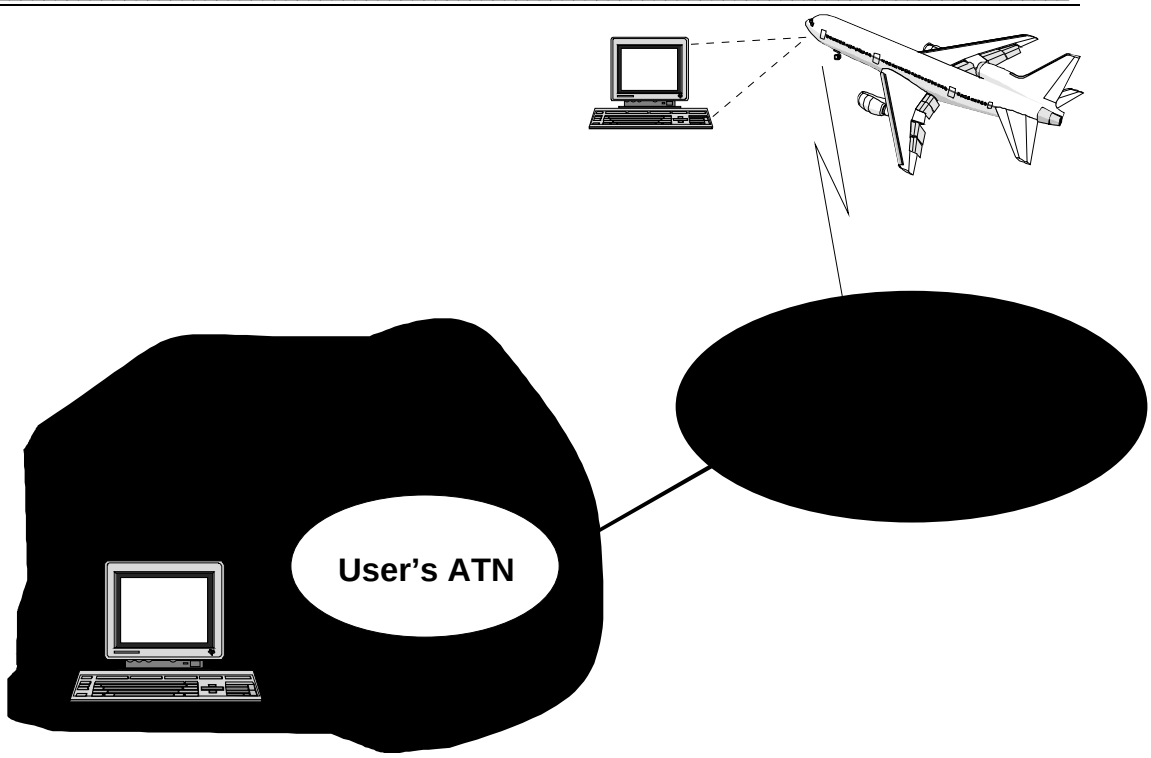

Figure 2-2 Organizational End User's View of the ATN

has many subnetworks of its own; and also wishes to operate ATN Routers, then the organization will also be an ATN Service Provider and hence needs to be aware of some of the internal complexity.

Figure 2-2 illustrates the changed perception. The "organizational" ATN user has both Host Computers which are individual ATN users as before, but also operates a portion of the ATN cloud, with at least one link to the rest of the ATN.

The portion of the ATN operated by the organizational user may be no more than a single ATN Router. Alternatively, a larger organizational user may operate a large number of ATN Routers, interconnected by various subnetworks also operated by the organizational user, and providing ATN access to all the systems owned by the organizational user which require ATN access. Such Routers may also be general purpose and be part of that user's own internal network. However, regardless of how many ATN Routers there are within an organization, the ATN Routers and the Host Computers to which they provide ATN access, typically form what is known as a Routing Domain. The Routing Domain is a structure specified in the ISO standards and imposed on the ATN Internet in order to enable a structured approach to be taken to solving the routing problem.

Within a Routing Domain, ATN users are recommended to use the ISO/IEC 10589 intra-domain routing protocol. This is a simple and robust routing information exchange protocol that is specified for use between systems that mutually trust each other (i.e., belong to the same user). This protocol exchanges connectivity information throughout the Routing Domain and enables each ATN Router to build up a compete topology map of the Routing Domain, so that every ATN Router knows which routers within the Routing Domain provide access to which Host Computers, and how the routers themselves are interconnected. Routes can then be plotted through the Routing Domain, and CLNP packets forwarded to their addressed destinations within the Routing Domain.

Within an ATN Routing Domain, there will be one or more ATN Routers that are permitted to route CLNP packets to external destinations, i.e., addressed destinations that are located in the "rest of the ATN". These routers are known as Boundary Intermediate Systems (BISs), because they exist at the boundaries of Routing Domains.

The ATN simply consists of multiple Routing Domains, each operated by an ATN participant. Each such Routing Domain is self-consistent and capable of internal routing. However, key to the ATN being a single internetwork as opposed to a collection of separate Routing Domains, is the capability of inter-domain routing between BISs.

In the ATN, it is mandatory for a BIS to support the ISO/IEC 10747 Inter-Domain Routing Protocol (IDRP). For inter-domain communications, this protocol requires that BISs communicate directly over a common subnetwork, which may be owned by the owner of either BIS, or by a third party. Rather than exchanging connectivity information, as is done between routers within a Routing Domain, BISs advertise *routes* to each other, where a route consists of the set of addresses which identifies the destinations reachable over the router, and information about the route's path including the Quality of Service and Security available over the route.

It is the BIS's responsibility to determine which routes, if any, it will advertise to another BIS, and the use it will make of routes which it receives. When the BISs within a Routing Domain receive alternative routes to the same destination, then they must collectively determine which is the best route and hence which of the alternatives will be used. The set of rules which determines the advertisement and use of routes is known as a Routing Policy, and each organizational user of the ATN must determine and apply their own Routing Policy.

It is the need for policy based routing between different organizations that underlies the need for the existence of Routing Domains. Policy based routing enables users to control external access to their communications resources, and to protect themselves from problems elsewhere in the internetwork. BISs may also, depending on Routing Policy, advertise to BISs in other Routing Domains routes that have been received from another Routing Domain, and thereby offer transit facilities. However, Routing Policy may also prevent such routes from being re-advertised and hence deny transit facilities.

Organizational ATN users must therefore ensure that they either have direct connections with the ATN Routing Domains with which communication is necessary, or that those Routing Domains with which direct connections exist also offer suitable transit facilities to the remainder. In principle, this could be done on a bilateral basis between ATN organizational users on an "as needs" basis. However, in practice, this is unlikely to be an efficient strategy and may actually prevent useful communication by putting too high a cost on establishing a usable path even when connectivity already exists.

Instead, it is intended that ATN interconnections are coordinated on both a regional and worldwide basis, so that ATN backbones (of Routing Domains offering general transit facilities) are created, with either a clear apportionment of costs, or a known tariff, for use of transit facilities. This way users can gain access to the full capabilities of the ATN quickly and cheaply.

2.2.1.3 Mobile Users

The ATN will incorporate many "mobile" subnetworks. Examples of such subnetworks include SSR Mode S, AMSS and VDL. If an aircraft were to attach to one mobile subnetwork only and never to any other, then even though sometimes it may be attached and at other times not attached, this has no consequence for the ATN. This is because from the point of view of the rest of the ATN, it would be no different from a fixed system that was occasionally off-line. However, that is not how mobile subnetworks are used. [c5 t 0115] An aircraft will attach to many different mobile subnetworks during the course of its flight. A long haul aircraft may move between the coverage areas of different satellites; an aircraft flying over a land mass will fly between different Mode S subnetworks as it passes over different countries. And, at the same time, the applications on board the aircraft will need to maintain contact with applications on the ground. Mobile platforms thus require special routing considerations.

In the ATN, mobile "platforms" are treated in a similar manner as organizational users. That is, the systems on board an aircraft are required to form a Routing Domain and hence must include an ATN Router that is also a BIS. This is partly because the ISO/IEC 10747 routing protocol provides a relatively efficient mechanism for the transfer of routing information over low bandwidth links, but also because aircraft are almost always organizationally separate to the ground systems with which they are in contact and the same requirements for policy based routing apply.

The existence of mobile users has a significant impact on the organization of the ground based ATN. While the ground topology will change only slowly, each aircraft's point of contact with the ground ATN will change rapidly with a consequent impact on the volume of routing information exchanged, and the routing tables in each router. A strategy is necessary for containing this high rate of information flow, and also to avoid the problems of routing instability caused by a rapid turnover of routing information.

This strategy is based on the notion of an aircraft's "home". The "home" of an aircraft does not necessarily relate to an airline's headquarters, its maintenance facilities, or indeed any geographical concept of "home". It is simply a particular ATN Routing Domain, and, in principle, any ATN RD will do. It may be an RD belonging to an aircraft's airline, but equally it may belong to a Service Provider or an Administration. Typically, all aircraft belonging to the same airline, or the General Aviation (GA) aircraft of a single country share the same home. Through the ISO/IEC 10747 routing protocol, a route to an aircraft's home is known throughout the fixed ATN.

As regards routes to the aircraft themselves, the routing policies used in the ATN constrain the distribution of routing information about a given aircraft. The constraints ensure that the routing information is propagated to the aircraft's home and those RDs along the path to the home only. [c5 t 0145]

With ISO/IEC 10747, a CLNP packet is routed not by destination address as such, but by address prefixes. Packets are routed along a route which provides an address prefix which is best (i.e., the longest match) with the destination address. In the ATN, both the route to the home and to the aircraft itself are characterized by address prefixes to the actual addresses contained within the aircraft. However, the route to the home is characterized by a shorter prefix than is the route to the aircraft itself. Typically, the address prefix that characterizes the route to the home is a prefix to all an airline's aircraft.

Thus, when a CLNP packet is sent to an address in an aircraft from an arbitrary point within the ATN, it will typically follow the route to the home. This is because this route is known throughout the ATN and it provides a prefix for the destination address. However, as soon as the CLNP packet reaches the home RD, or indeed, any RD on the path between the home RD and the aircraft, the route to the aircraft provides a longer match in respect of the address prefix, and hence the packet now follows the route to the aircraft and its destination.

By this technique an almost optimal route is followed while constraining the distribution of routing information to mobiles to a limited set of RDs, and hence minimizing the impact of mobiles on the ATN.

2.2.1.4 Routing Control

The ATN may be used for Operational Communications, Administrative Communications, Systems Management Communications and for General Communications. Although some parts of the ATN may allow the sharing of facilities between these different classes of data, there will usually be a strict separation of communications resources between these different classes of data. The ATN supports this separation by specifying a separate traffic type for each class of data, and enabling each route through the ATN to be labelled according to the class of data which it may convey. ATN Routers are required to relay user

data along only those routes available for its class of data. The requirement for strict separation is thus implemented and enforced by the ATN routing procedures.

2.2.2 ATN Users and Service Providers

The above discussion has illustrated the fact that there is not one ATN interface, but instead there are many ATN interfaces, each of which serves a different user in a different role. In order to avoid confusion, a taxonomy of interfaces has been developed. This taxonomy identifies each significant interface as a *reference point*, and at each such reference point, there is an interface between two ATN entities, one taking on the role of a user, and the other as the service provider. Figure 2-3 illustrates the location of each ATN Reference Point, where the layers of the OSI reference model are represented as numbered rectangles, with the numbers 1 to 7 corresponding to the physical, data link, network, transport, session, presentation and application layers respectively. Figure 2-1(a) illustrates the reference points by abstraction from Figure 2-2, while Figure 2-1(b) provides a more formal model of the ATN.

1. Reference Point One, the Transport Reference Point, is the OSI Transport Service interface and follows ISO 8072. This reference point is wholly contained within an ATN Host Computer, and represents access to the ATN Internet by an ATN Host Computer at the Transport Layer level. The user of the service provided in this example, is the OSI Session Entity; the service provider is the transport layer entity.

2. Reference Point Two, the Network User Reference Point is the interface between the services of the network layers located in an ATN Host Computer and an ATN Router providing access to the ATN Internet. It comprises the OSI protocols used to access ATN Services.

   Note. - An ATN Router relays data between ATN Host Computers either directly to another ATN Host Computer or via one or more futher ATN routers, which may or may not belong to other ATN Service Providers. When both Host Computer and Router are owned by the same organization, then the protocols that provide this interface are not mandated; the specification only recommends an appropriate stack.

3. Reference Point Three, the Network Provider Reference Point, is at the interface between two Routers belonging to different organizations. It comprises the OSI protocols used to support end-to-end communications via multiple ATN Routers, possibly via multiple subnetworks.

   Note.– When both Routers belong to the same ATN Service Provider then the protocols that provide this interface are not mandated; the specification only recommends an appropriate stack.

4. Reference Point Four, the Subnetwork Provider Reference Point, is at the interface between an ATN Host Computer or an ATN Router and a subnetwork. It comprises the OSI or subnetwork specific protocols used to access the service provided by that subnetwork and identifies the services provided by a real subnetwork used to connect two ATN components. This reference point identifies the lower boundary of the scope of the ATN Internet SARPs.

The provider of the service at reference point 4 is out of the scope of this document. As discussed above, the ATN places only very limited constraints on the service provided at reference point 4, and this enables almost any subnetwork to be used as an ATN subnetwork.

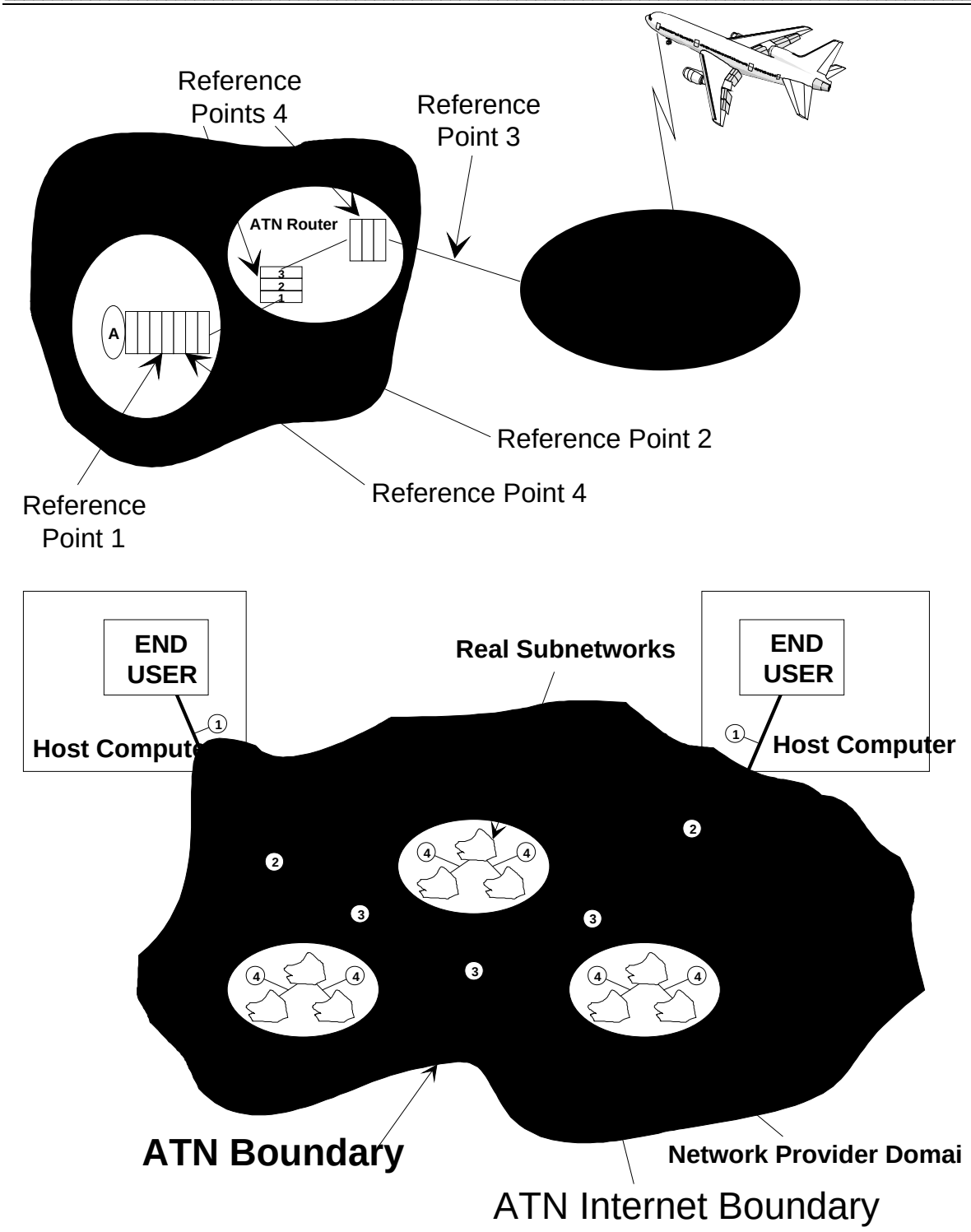

Figure 2-3 ATN User and Service Provider Reference Points

2.3 ATN Architectural Components

2.3.1 The OSI Reference Model

The ATN is an implementation of OSI and frequently refers the OSI Reference Model. It is therefore useful to consider what the OSI Reference Model means in practice and introduce

some of the concepts it defines. The “seven layers” of the reference model are illustrated in the figure opposite.

The reference model is a layered model building on the layered architecture introduced with X.25, and identifies two types of Systems:

- **End Systems:** which are Host Computers, the users of network services, and which comprise seven protocol layers, providing communications services to applications.

- **Intermediate Systems:** which are either Routers or Packet switches, and comprise only the three layers appropriate to network communications.

End Systems may either communicate directly, using the services of a physical communications medium, or communicate via one or more Intermediate Systems. The definition of each protocol layer is:

- **Application Layer:** contains all the information (or semantics) that is exchanged between End Systems. In particular, it contains all user information that is exchanged. It also provides the means to allow the End Systems to agree to the semantics of the information exchanged.

- **Presentation Layer:** provides the means to represent the information exchanged (i.e. the Syntax) between the End Systems without changing the semantics of the information.

- **Session Layer:** provides the means to mark significant part of the information exchanged between systems: for example, a Unit or Word, a page, or a chapter.

- **Transport Layer:** provides end-to-end control and information interchange with the level of reliability that is needed for the using application. The services provided to the upper layers are independent of the underlying network implementation. The Transport Layer is therefore the “user’s liaison, acting as the go-between for the user and the network, enhancing the network’s service to that required by the application.

- **Network Layer:** provides the means to establish, maintain and terminate the switched connections between End Systems, or to transfer datagrams between two End Systems. Addressing and routing functions are included in the Network Layer.

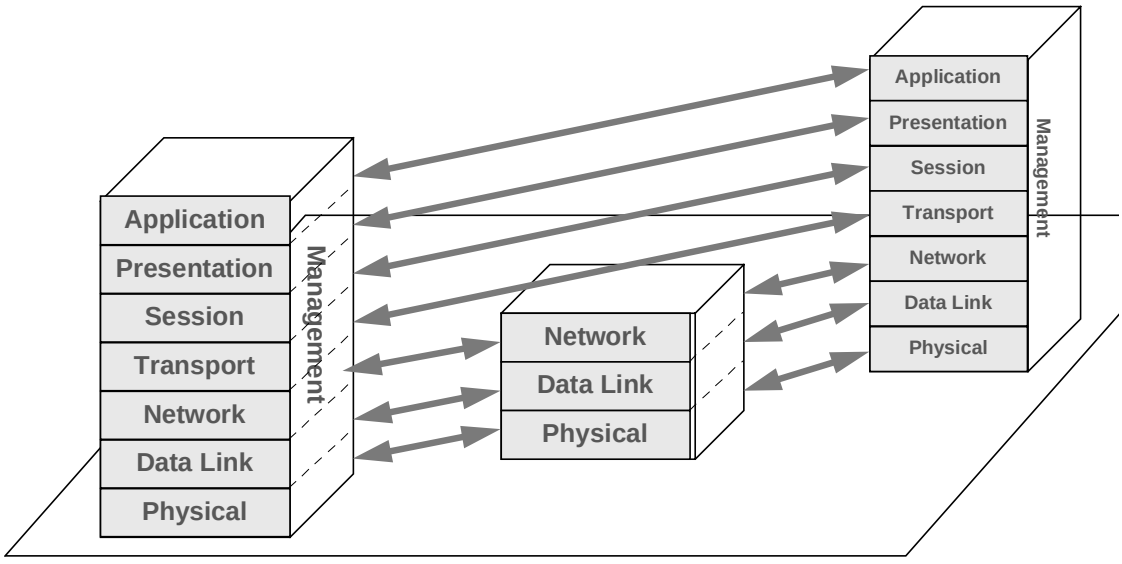

Figure 2-4 The OSI Reference Model

- **Data Link Layer:** provides the synchronisation and error control for the information transmitted over the physical link.

- **Physical Layer:** provides the functional and procedural characteristics to activate, maintain and deactivate the physical connection. It also includes the electrical and mechanical characteristics of the physical interface to the external transmission media.

The seven layer model has proved remarkably resilient to change since it was first introduced, although it has been considerably enhanced over the years. The original reference model considered only connection mode communications. It was later amended to include connectionless communications, and now also includes a Security Model, a Naming and Addressing Model, and a Systems Management Model. A Quality of Service (QoS) Management Framework is a likely future addition, as this is now becoming a subject generating major interest.

OSI Reference Model terminology is used extensively in both the ATN SARPs and Guidance Material.

2.3.2 ATN Functional Components

The ATN comprises the following functional components:

- End Systems (ESs) (i.e. Host Computers where aeronautical applications may reside)

- Intermediate Systems (ISs) (i.e. ATN Routers)

The relationships between these components are illustrated in Figure 2-5.

The OSI layer 1-4 aspects of ESs and all ATN ISs comprise the ATN Internet. The ATN Internet provides data transfer services to ATN ESs. Through ESs, ATM applications gain access to ATN services and are hence able to exchange application specific data.

The ATN also recognizes the existence of subnetworks, and such subnetworks, when used to provide communication paths between ESs and ISs, and ISs, may also be viewed as being part of the ATN. Subnetworks are characterized by the ATN as being:

- Ground subnetworks

- Mobile subnetworks

- Aircraft subnetworks

Ground, Mobile and Aircraft subnetworks are used to interconnect the components described above.

2.3.2.1 End System Model

The function of an ATN End System is to provide the end-user applications with an OSI compliant communications interface to enable them to communicate with remote end-user applications. An ATN End System is the representation in ATN Architecture of a Host Computer supporting one or more CNS/ATM applications.

ATN End System implementation of the protocols required for Layers 1 and 2 (i.e. Physical and Data Link), and subnetwork access functions in layer 3, is purely a local issue and wholly dependent on the subnetwork to which the particular End System is attached, as such definition of these protocols is outside the scope of the SARPs.

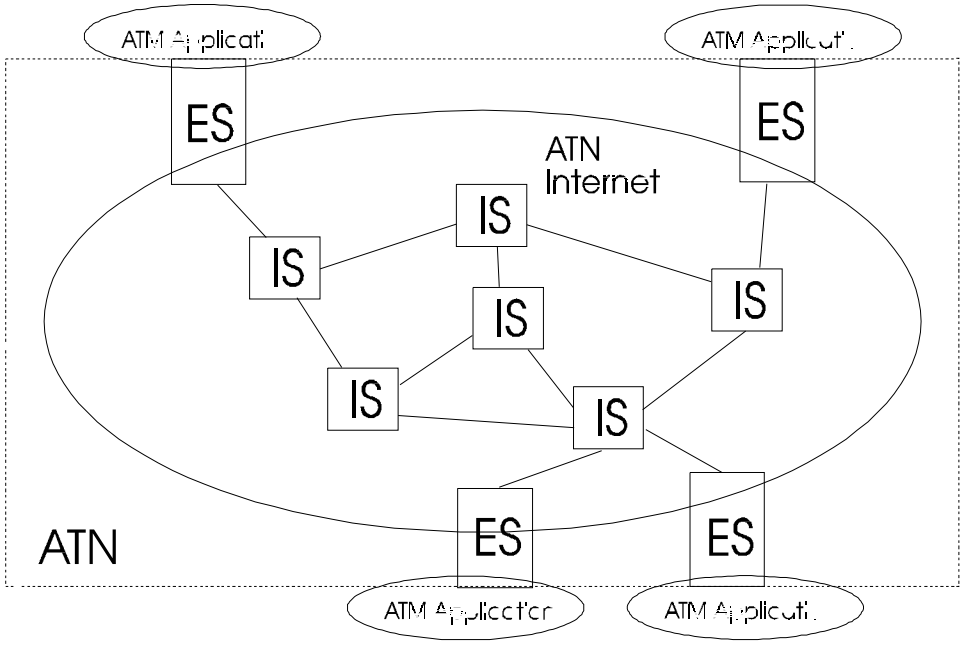

Figure 2-5 ATN Functional Components

ATN End System protocols and functions in the transport layer, and those in the Network Layer which are subnetwork independent or are concerned with the convergence of subnetwork dependencies with subnetwork independent protocols and functions, are within the scope of the SARPs.

ATN End System higher layer protocols and functions in support of ATM applications are defined in Parts 2, 3 and 4 of the SARPs.

2.3.2.2 Intermediate System Model

The functions of the Intermediate System are to perform the relaying and routing of ISO 8473 NPDUs between other Intermediate Systems and End Systems. An ATN Intermediate System is the representation in ATN Architecture of a Router interconnecting two or more ATN Networks for the purpose of data interchange between ATN End Systems connected directly or indirectly to those ATN Networks.

The protocol support required for the Physical and Data Link layers of an ATN Intermediate System are purely dependent on the subnetwork to which they are attached and are therefore a local issue and outside the scope of the SARPs.

ATN Intermediate System protocols and functions in the Network Layer which are subnetwork independent or are concerned with the convergence of subnetwork dependencies with subnetwork independent protocols and functions, are within the scope of the SARPs.

The functions and data structures in support of routing and relaying are discussed below.

2.3.3 Administrative Domains and Routing Domains

In order to develop a scaleable routing architecture, the ATN has adopted the ISO Routing Framework, presented in ISO TR 9575 and illustrated in Figure 2-6. This provides the structure necessary to support routing in the complex ATN ground environment and to Mobile Systems.

The ISO Routing Framework first recognises that Host computers, routers and networks are owned and operated by different organisations, and therefore defines the *Administrative Domain*. An Administrative Domain comprises the Hosts computers, routers and networks operated by the same organisation. The purpose of the Administrative Domain is to clearly indicate the domain of an organisation's responsibility and to differentiate communication within an organisation from communication between organisations.

However, the most appropriate structures for routing control do not necessarily always follow organisational boundaries, and this is recognised by the definition of the *Routing Domain.* A Routing Domain simply comprises a set of Host Computers and Routers owned by the same organisation, and which implement a common routing algorithm. There may be many Routing Domains within a single Administrative Domain.

The routing framework also classifies routers according to their role. Those routers that operate solely within a Routing Domain are termed Intermediate Systems, while those that support inter-domain routing are termed Boundary Intermediate Systems (also referred to as Boundary Routers).

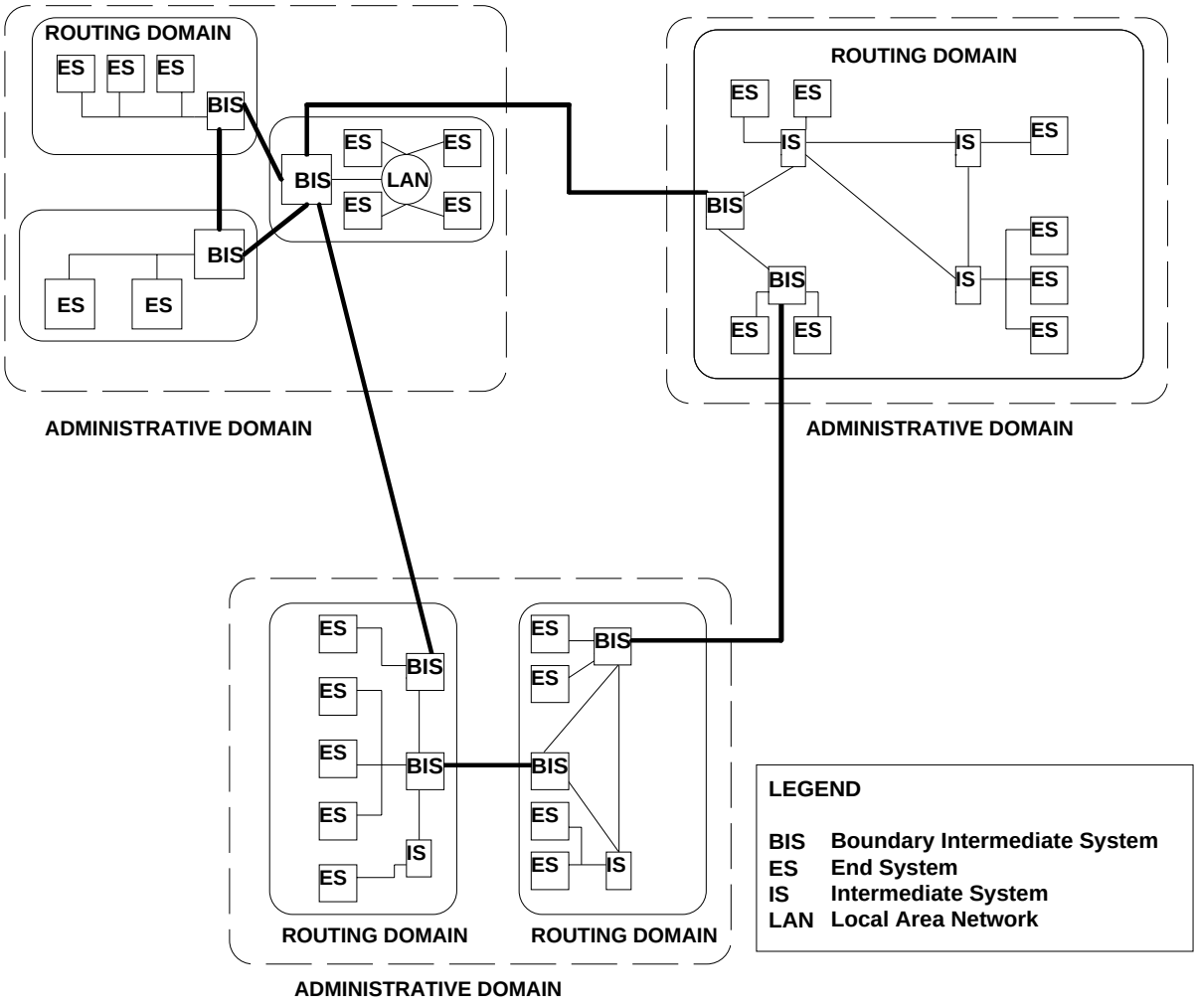

Figure 2-6 ISO Routing Framework

2.3.4 Addressing

Every system within a network such as the ATN, must have a unique address. This address may then be used to identify the source and destination of a packet sent through the network. ATN routers use a packet's destination address to determine how the packet is routed to its destination.

An address Is therefore more than a unique identifier for each system, and to be truly useful, it must be possible to use an address to find out how to reach the addressed system i.e. to select the most appropriate route. That is an address must somehow relate to a network's topology.

A useful example of this concept is provided by telephone numbers. The ITU has published a global numbering plan for telephone number allocation and, in principle, each telephone number consists of a "country code", an "area code", an "exchange code", and a "subscriber number". Telephone numbers are closely related to the topology of the telephone network. Given a subscriber's telephone number it is possible to identify the country and area in which their local exchange is located, and by using this close relationship between topology and telephone numbers, the routing of telephone calls can be readily accomplished. As long as, for example, each inter-area telephone exchange has routing tables that identify the routes to each other area within the same country, telephone calls between different areas within the same country can be readily made. Only within an area does the connectivity between exchanges inside the area, need to be known.

Routing Domains can be viewed as being like telephone areas, and like all subscriber numbers in a telephone area, the addresses of systems within the same Routing Domain should all have a common prefix. Then a packet sent to any system in the Routing Domain, can be sent to the Routing Domain without the routers along the way having to have any knowledge of the topology of the networks and routers within that Routing Domain.

Routing Domains are, however, a more flexible concept than telephone areas. The requirement for a single common address prefix is not absolute, and it is possible to have more than one address prefix that characterises a single Routing Domain. The geographical country is also not present in either the ISO Routing Framework, or as a fixed quantity in the Address Plan. Instead, there is the very general concept of the Routing Domain Confederation (see 2.6 below).

There is also no requirement in the ISO Routing Framework for the address prefixes that characterise adjacent (i.e. linked by a common network) Routing Domains, to have any similarity (i.e. for there to be another (shorter) address prefix common to each Routing Domain's address prefix).

If all inter-Domain interconnections are simply developed on an ad hoc basis with no aim to create a Global ATN Internet, then any lack of similarity between the address prefixes assigned to adjacent Routing Domains is not an issue. However, if a scaleable routing architecture (i.e. one which permits effectively unlimited growth) is to result then there does need to be some similarity between the address prefixes characterising adjacent Routing Domains. Then it will be possible to group Routing Domains together and advertise routes to a group of Routing Domains, rather than to each individually. This is similar to telephone networks grouping of all the areas in one country together and treating them as a whole from other countries. With such a strategy it is possible to develop a scaleable routing architecture such that the further away a router is from a packet's destination, the less detailed the routing information needs be to successfully route the packet.

This is a very important feature of a scaleable architecture, because if the amount of routing information required by at least one router is in proportion to the size of the ATN Internet then the maximum size that router can be, places a limit on the size of the network as a whole.

2.3.5 ATN Islands

2.3.6 The "Home" of an ATN Mobile

2.4 ATN Protocol Architecture

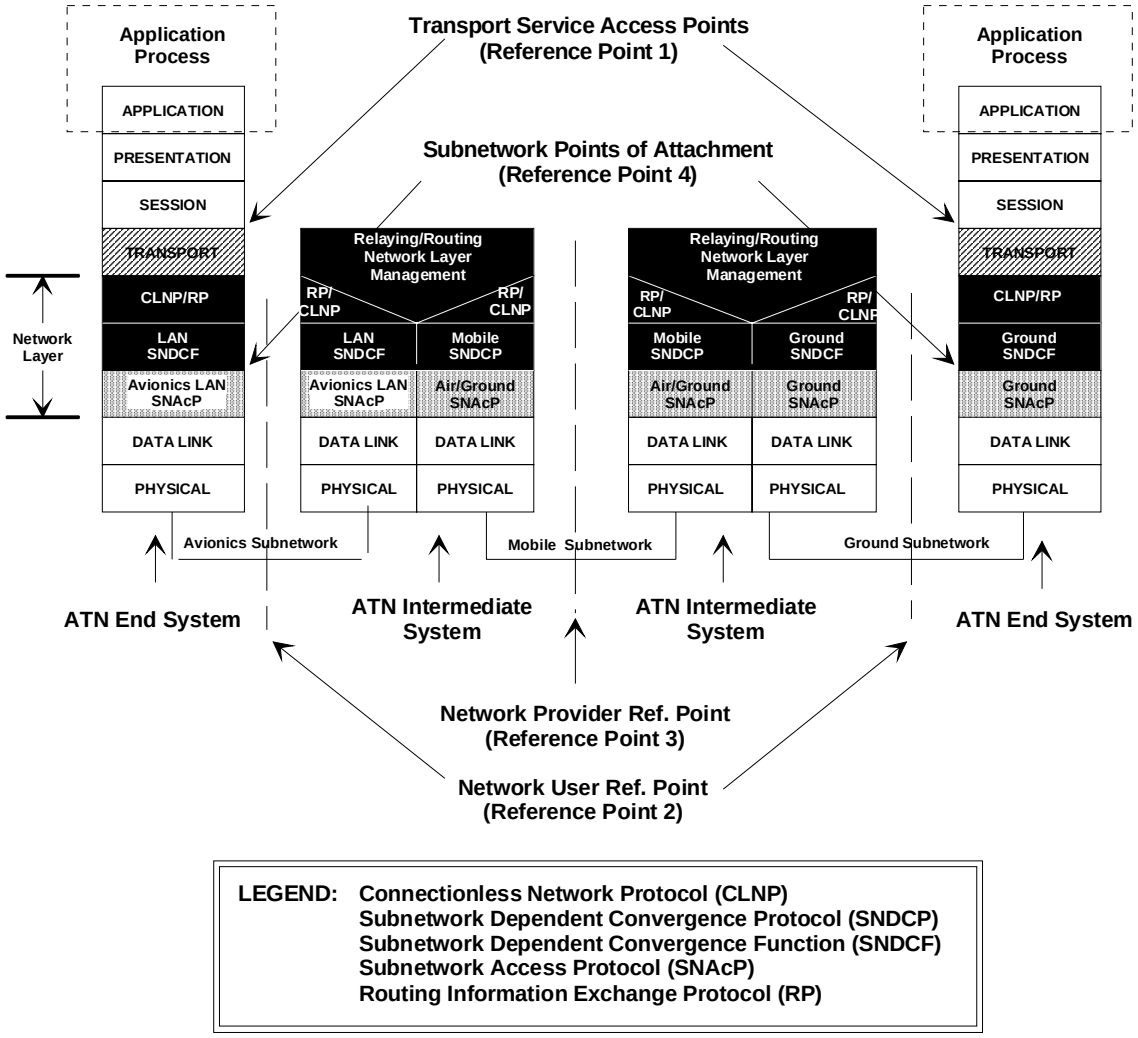

Figure 2-7 ATN Protocol Architecture

2.4.1 The ATN Transport Layer

The OSI Transport Layer service provides transparent transfer of data between Transport Service users. All protocols defined in the Transport Layer have an 'End-to-End' significance, where the 'Ends' are defined as co-operating transport entities on two ATN host computers. The Transport protocol operates only between end systems. Within the ATN, Transport Layer entities communicate over the ATN using the Network Service provided by the ATN Network Layer Entities.

The ATN protocols follow the reference model specified by ISO in ISO 7498-1.

The ATN protocol architecture is illustrated in Figure 2-7, and specifically illustrates the use of a mobile subnetwork for air-ground communications. This protocol model has been derived directly from the OSI Reference Model.

There are two modes of the transport service, the Connectionless mode Transport Service and the Connection-mode Transport Service. The connectionless mode service allows two transport users to exchange individual datagrams, without flow control or the need to have previously established a connection, but with no guarantee of delivery. The connection-mode service allows two transport service users to negotiate a communications channel

with a set of common characteristics, including reliable delivery of data units, and guaranteed (very high probability) order of delivery.

The two OSI protocols that provide the two modes of the transport service have separate specifications, and operate independently. Based on the higher level protocols operating within a given ATN host computer, one or both of the transport protocols may be implemented. Neither transport protocol is concerned with routing and relaying of data between End Systems, which is the responsibility of the Network Layer. The protocol in support of the CLTS is specified in ISO 8602, and the protocol in support of the COTS is specified in ISO 8073. The implementation of these protocols within the ATN is further described in Chapter 8.

The Transport Service boundary corresponds with ATN reference point 1.

2.4.2 The ATN Network Layer

The OSI Network Layer Service, like the OSI transport service is specified to provide both a connection mode and a connectionless mode service. However, in the ATN, the Network Layer Service is restricted to the connectionless mode only. This is because, unlike the transport layer, the same network protocols must be implemented in every system in the internetwork, if interoperability is to be guaranteed. In the case of the transport layer, the mode of the service required depends on the requirements of the users, and those End Systems that implement the same applications must also implement the same transport layer protocols. However, the internetwork itself must relay the data of all users, regardless of the mode of the transport service used. In order to provide universal connectivity, a consistent set of protocols must be implemented across the internetwork. Even if universal connectivity was ruled out, in practice, most ISs would still have to support all modes implemented by ESs, because of the tendency for data pathways to cross each other, regardless of the network service mode supported by each such data pathway.

It is thus cost effective to support only one mode of the network service. Implementation costs are reduced, and the complexity of validation is also reduced.

The Network Layer Service is independent of the Transport Layer Service and may be used by ISO 8602 to provide the CLTS, and by ISO 8073 (class 4 procedures only) to provide the COTS.

The OSI Network Layer comprises three sub-layers or *roles*:

- Subnetwork Independent Convergence Role, which is responsible for providing a consistent Network Layer Service regardless of the underlying subnetwork
- Subnetwork Dependent Convergence Role, which decouples the specification of the Subnetwork Independent Convergence Role from individual subnetwork characteristics.
- Subnetwork Access Role, which contains those aspects of the network layer specific to each subnetwork.

2.4.2.1 The Subnetwork Independent Role

In an ES, the Subnetwork Independent Role is responsible for providing the OSI Network Service independent of the real subnetwork(s) to which the ES is attached. In an IS, the Subnetwork Independent Role is responsible for the routing and relaying of user data along its route between the two communicating users. The protocols that support the exchange of routing information are also contained within this functional area.

In support of the connectionless mode Network Service, it is a mandatory requirement that all ATN ESs and ISs implement the ISO 8473 internetworking protocol. This is a subnetwork independent protocol and supports the relaying of connectionless data PDUs

over multiple subnetworks. By choosing such a protocol as its unifying characteristic, the ATN is cast as a subnetwork independent internetwork. CLNP supports the ISO global network addressing plan, quality of service specification, congestion control, and segmentation and reassembly of data packets. Additionally, provisions exist within CLNP for diagnostic actions such as end-to-end route recording and error reporting.

Three Routing Information Exchange Protocols are also specified in support of ISO 8473 within the ATN. These are:

- ISO 9542 - the End-System to Intermediate-System (ES-IS) protocol
- ISO 10589 - the Intermediate-System to Intermediate-System (IS-IS) intra-domain routing information exchange protocol
- ISO/IEC 10747 - the Inter-Domain Routing Protocol (IDRP)

The use of these protocols is discussed in more detail in Chapter 11.

2.4.2.1.1 End-System to Intermediate System Routing Protocol

The ISO 9542 ES-IS protocol provides a mechanism for ESs and ISs to exchange connectivity information within a local subnetwork environment. It is recommended for implementation in all ATN ESs and all ATN ISs that support ES attachment. In this role, its use applies to reference point 2.

The protocol enables ESs and ISs to dynamically discover each other when attached to the same subnetwork (only on broadcast subnetworks), and for ISs to inform ESs of optimal routes. In the absence of ISs (on broadcast subnetworks), ESs may also locate each other on an as needs basis.

The ES-IS protocol also complements the IS-IS routing protocols to support dynamic discovery of other ISs and/or their NETs, and is also used in a similar manner to support the Inter-Domain Routing Protocol over mobile subnetworks.

2.4.2.1.2 Intra-Domain Routing Information Exchange Protocol

The ISO 10589 IS-IS intra-domain routing information exchange protocol is used by ISs within the same Routing Domain to exchange connectivity and QOS information. It is recommended for implementation in all ATN ISs. As the ISs within a single Routing Domain are always operated by the same organization, this protocol is not used at any of the ATN interfaces identified by reference points.

The protocol works at two levels. Level 1 operates within the same Routing Area, while level 2 operates between Routing Areas. From the information exchanged by this protocol, ISs build up a topography map of the local Routing Area at level 1, or Routing Area connectivity, at level 2. From this map, optimal routes can be plotted, and the relevant information provided to each IS's Forwarding Information Base.

2.4.2.1.3 The Inter-Domain Routing Protocol (IDRP)

The ATN has adopted the ISO/IEC 10747 Inter-domain Routing Protocol, for the exchange of dynamic routing information at the inter-domain level. IDRP is a "vector distant" routing protocol and is concerned with the distribution of *routes* where a route comprises a set of address prefixes for all destinations along the route and the route's path i.e. the list of Routing Domains through which the route passes in order to reach those destinations. In addition, a route may be further characterised by various service quality metrics (e.g. transit delay).

Under IDRP, specialised Boundary Routers in each Routing Domain advertise to Boundary Routers in adjacent Routing Domains, routes to the systems contained in that Routing Domain. Typically, there is a route for each performance metric and security category supported, and the destination of these routes is the Address Prefix(es) that characterises the Routing Domain. The receiving Routing Domains then store this information and use it when they need to route packets to destinations within the other Routing Domain. A route so received may also be re-advertised to other Routing Domains adjacent to the Routing Domain that first received it, and onwards throughout the ATN Internet. Ultimately, every Routing Domain in the ATN Internet can receive a route to every other Routing Domain.

However, without any other functionality, IDRP would not provide a scaleable approach to routing. In order to provide such a scaleable architecture, IDRP enables the aggregation of routes to Routing Domains with common address prefixes, into a single route. It is thereby possible for the number of routes known to any one router to be kept within realistic limits without reducing connectivity within the Internetwork.

2.4.2.2 Subnetwork Dependent Role

The OSI Subnetwork Dependent Role is responsible for decoupling the functions of the subnetwork independent role from the characteristics of different subnetworks and provides a consistent service to any protocols implemented by the subnetwork independent role. In doing so, it may implement a convergence protocol, implemented on a hop-by-hop basis, independently over each subnetwork. This is a Subnetwork Dependent Convergence Protocol .

ISO 8473 may be adapted to all known subnetwork types and hence a SNDCP is not specifically required. However, each subnetwork class does require a different adaptation, and each such adaptation is known as a Subnetwork Dependent Convergence Function. Chapter 10 discusses the SNDCFs that may be used to interface ISO 8473 to ATN subnetworks.

However, while ISO 8473 does not require an SNDCP, there is justifiable concern over the ISO 8473 protocol overhead in respect of the low bandwidth communications provided by the mobile subnetworks. For this reason, an SNDCP has been specified to provide compression of the ISO 8473 protocol header over mobile subnetworks. This SNDCP is further discussed in Chapter 10.

2.4.2.3 Subnetwork Access Role

The Subnetwork Access Role comprises the functions necessary to support access to a specific subnetwork. This is dependent on the specification of each subnetwork and is hence outside of the scope of this document. The service provided by the Subnetwork Access Role to the Subnetwork Dependent Role is at ATN reference point 4, which identifies the lower boundary of this manual.

2.5 Policy Based Routing

The intuitive view of routing in a packet based network is generally termed “performance based routing”. In this mode of operation, all communications paths are available, and a router’s objective is to choose the best out of those available, using metrics such as “hop count”, “capacity”, “transit delay”, “cost”, etc. in order to determine which is “best”.

However, while this may be the most appropriate strategy within an organisation, when packets are routed between organisations, or over commercial networks, the fact that a route is available (i.e. connectivity exists) may not always be the only reason to consider its use, other policy based criteria may apply. The application of such policy criteria to routing is know as “policy based routing”, and is another feature of IDRP.

Policy based routing has always been applied informally, using static configuration of routing tables. However, IDRP formalises policy based rules for route selection within the context of a dynamic routing framework.

Policy is applied at two points. Firstly, when a route is received from another Routing Domain, a policy decision is taken on whether to use it, either at all, or in preference to alternative routes to the same destination. And, secondly, a policy based decision is made when a route is considered for onward advertisement to an adjacent Routing Domain. Through routing policy, a network manager can choose both the received routes that are accepted for use, and those which it is prepared to offer for the use of other Routing Domains. For example, through the implementation of appropriate policy rules, a Routing Domain connected to many other Routing Domains, can be a Transit Routing Domain i.e. relaying between those Routing Domains, or an End Routing Domain, i.e. only accepting packets addressed to local destinations.

2.6 Routing Domain Confederations

Although the structuring of an internetwork into Administrative and Routing Domains enables a structured approach to routing to be developed, this is not in itself readily scaleable. Once there exists a large number of Routing Domains, the structuring problem re-asserts itself, and there is a need to provide another level to the Routing Framework, and so on. This problem is resolved in a recursive fashion by the Routing Domain Confederation.

A Routing Domain Confederation (RDC) is a set of Routing Domains and/or RDCs which have agreed to join together and form a Routing Domain Confederation. The formation of a RDC is done by private arrangement between its members without any need for global co-ordination. From the outside, an RDC appears exactly like a single Routing Domain in the sense that the routes that CLNP PDUs can follow cannot re-enter an RDC, no more than they can re-enter a Routing Domain. All Routing Domains within an RDC must also be reachable from each other without the route passing through a Routing Domain that is outside of the RDC; this is a simple consequence of a route not being able to re-enter an RDC.

Routing Policies can refer to entire RDCs in the same way that single RDs are referred to, which enables the straightforward specification of routing policy rules that apply to whole classes of RD. There is no requirement for there to be co-ordination of routing strategies or the adoption of any common routing policy rules. However, efficiencies can result from the co-ordination of Addressing Plans and policies.

Figure 2-8 illustrates the RDC concept. RDCs are simply groupings of Routing Domains. A Routing Domain may be a member of zero, one or more RDCs, and hence RDCs may overlap, may be nested, and may be disjoint. RDCs are first a shorthand way of referring to communities of Routing Domains, but are at their most powerful when they are closely related to Address assignment and when combined with IDRP's features for *route information reduction* and *route aggregation* (see 2.6.2 below). RDCs are also essential for ensuring that the size of a route's path information does not itself become a limit of the size (or more specifically the diameter) of the Internet.

2.6.1 Limiting the Size of Path Information

In complex Internet topologies, it is possible that routes may loop back on themselves if some mechanism is not introduced to detect and suppress looping routes. This is simply achieved in IDRP by including the unique identifier of each Routing Domain that a route passes through, as part of a route's path information. A Routing Domain adds its identifier to every route that it advertises, and a simple loop test may then be introduced for each received route. However, a consequence of this is that the path information associated with each route grows each time that the route is re-advertised.

The IDRP protocol limits the length of the message that conveys each route and, anyway, routers will need to impose a limit on message length for practical implementation reasons. There is thus a limit on the number of Routing Domain Identifiers that the path information can contain, and, without RDCs, this limit will provide an upper bound on the number of Routing Domains through which a route may pass. If all Routing Domains in an Internet are to be able to communicate with each other, then this limit translates into a limit on the "diameter" of the Internet, and hence a point beyond which the Internet cannot grow.

However, in IDRP, path information reduction is also a feature the RDC.

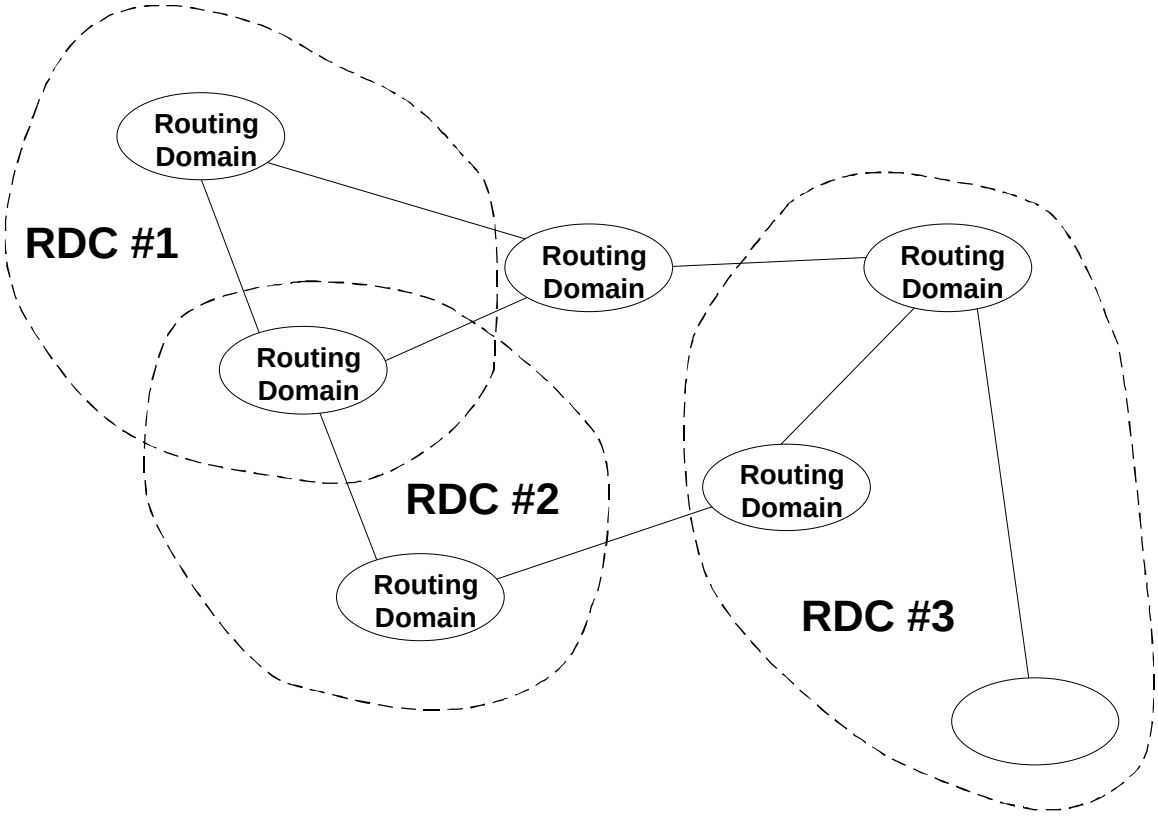

Figure 2-8 Routing Domain Confederations

When a route is advertised to a Routing Domain outside of the RDC, the Routing Domain Identifiers in the route's path information that identify Routing Domains in the RDC, are replaced by a single identifier - that of the RDC itself. Through such a mechanism, path information may be reduced, and a scaleable routing architecture achieved. The proper deployment of RDCs ensures that the diameter of the ATN Internet is not limited by the capability of routers to process path information.

The entire ATN is itself specified as an RDC. This enables the interconnection of the ATN with other Internets without limiting interconnection scenarios due to the total network diameter becoming greater than the maximum permitted by routers' path information handling capabilities.

2.6.2 Route Aggregation and RDCs

Route Aggregation is the process by which two or more routes are combine into a single route that replaces the original route. Route Aggregation is complemented by Route Information Reduction, which is the process by which the set of address prefixes that identifies the destination(s) of a route is replaced by fewer shorter address prefixes.

Typically, when two or more routes are aggregated, the destination address prefixes are combined together as the destination of the aggregated route, and Route Information Reduction is then applied to this combined set of address prefixes. The result of these two processes is a overall reduction in the number of routes without increasing the detail associated with the route's destination.

Route Aggregation may occur at any at point in an Internet. However, RDC boundaries can provide an ideal point at which to perform aggregation. This is not only because the path information can also be simultaneously reduced, but also because RDCs help simplify the management of Route Information Reduction.

For example, if an RDC is formed from all Routing Domains with a common six octet address prefix, then whenever a route exits that RDC it is possible to aggregate all routes to destinations inside the RDC and for the destination of that route to always comprise that six octet address prefix only. This being irrespective of whether all Routing Domains within the RDC are currently online, or whether all address combinations are even allocated. No ambiguity exists because of the fact that no Routing Domains with addresses deriving from that six octet address prefix can exist outside of the RDC.

Although it is not essential to define an RDC for this purpose, RDCs simplify the management of the reduction of addressing information.

RDCs thus perform an essential and key role in the implementation of a scaleable Internet. By reducing path information at RDC boundaries and providing a straightforward approach to controlling route aggregation, RDCs can be used to ensure that routing is not a limit on the size of the ATN Internet.

2.7 Routing in the ATN Ground Environment

2.7.1 A General Model for ATN Routing

A general model of ATN Routing is shown in Figure 2-9. In this model, the ATN consists of a fixed ground network which links satellite, VHF and Mode S ground stations together with ground based Host computers, including both large scale data processing engines and workstations. ATM avionics on board aircraft are then linked to the rest of the network through, satellite, VHF and Mode S datalinks, as appropriate, and may have more than one air/ground datalink in use simultaneously.

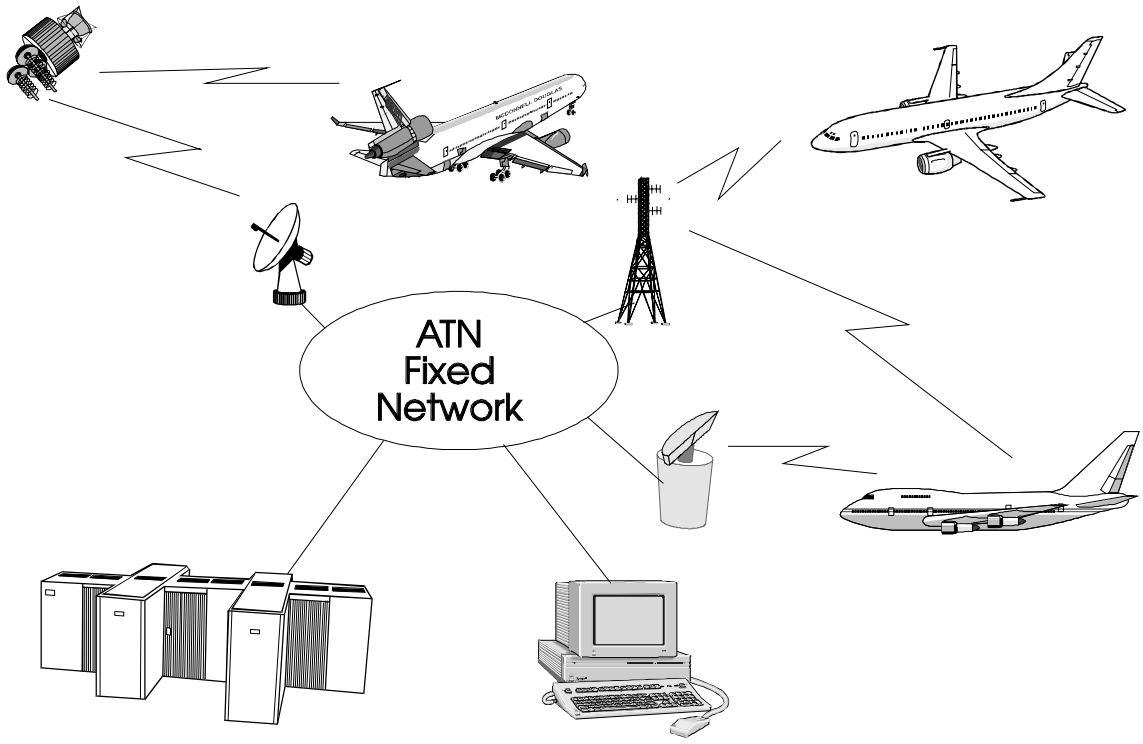

Figure 2-9 General Model of ATN Routing

2.7.2 Routing in the Ground Environment

The fixed network is not a single entity but itself consists of many different networks all linked together, as illustrated in Figure 2-10. The ATN ground environment will consist of multiple networks, owned by different administrations and organisations, and implemented using many different technologies. In some cases, these will be existing networks with spare capacity made available to the ATN. Others will be new networks implemented specifically to support ATN use. There will be X.25 Private Packet Switched Data Networks (PPSDNs), Frame Relay Data Networks, Integrated Services Digital Networks (ISDNs), Local Area Networks (LANs) e.g. Ethernet, and others. These networks are then linked together through routers which provide the connectivity between the different types of data network, and to the air/ground networks; host computers are directly connected to a nearby data network, typically a LAN.

User data is switched by the routers as discrete packets formatted according the ISO Connectionless Network Protocol (CLNP). Each packet is viewed as a separate event and routed according to a “route map” of the ATN. In the ATN, each router has a portion of the full ATN route map and builds and maintains this route map dynamically using routing information passed to it by its neighbouring (adjacent) routers.

Host computers communicate with each other either directly over a common data network, or use the services of a router to provide a communications path to a Host on another data network. It is the responsibility of the routers working together to find a suitable path through the networks which they interconnect, and data may travel through many different routers and via many different networks on its journey between two Hosts. In order to build an ATN route map for this purpose, the routers exchange, amongst themselves, information on which hosts are local to them (i.e. reachable via a single data network and with no intermediate router), and on how they relate to other routers. From such information, the routers can plot the course of data through the ATN.

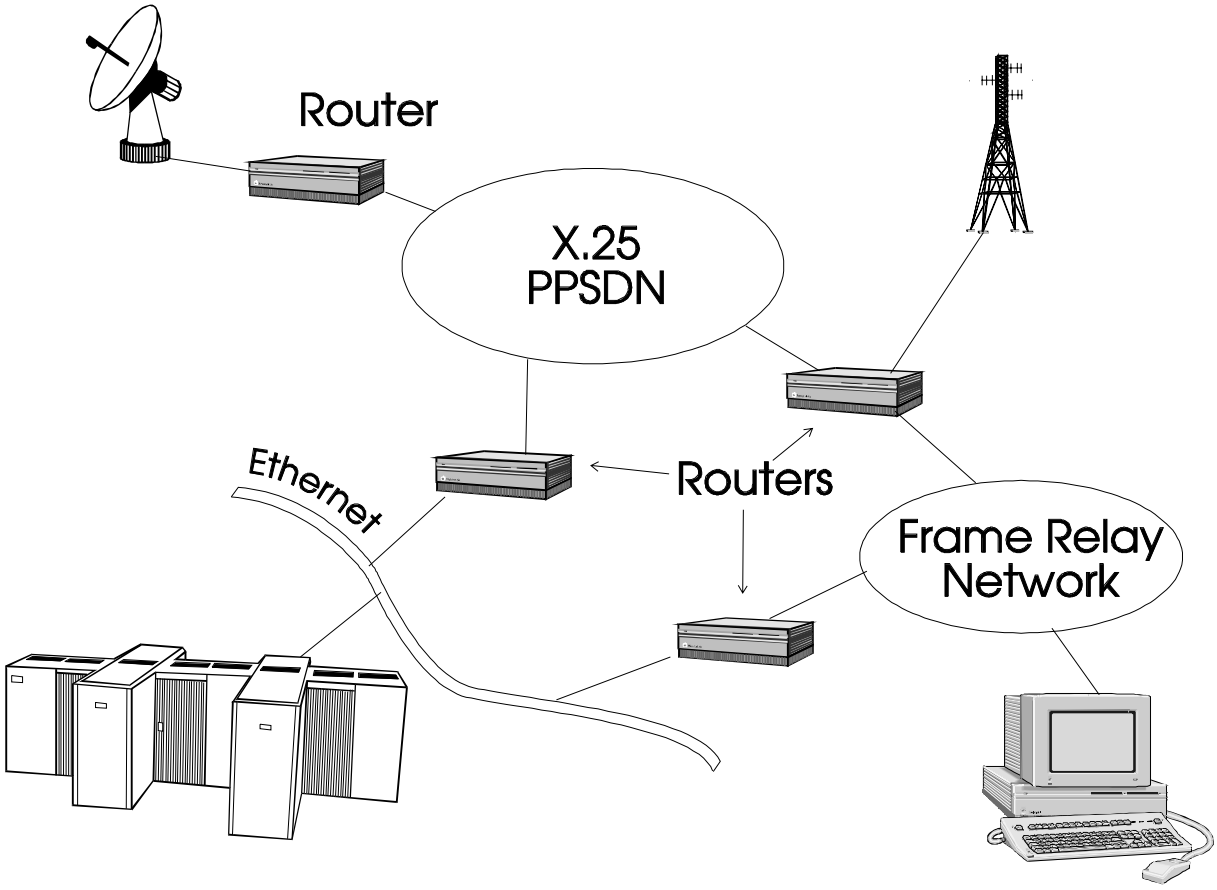

Figure 2-10 The ATN Ground Environment

2.7.3 The ATN Ground Environment

The ATN Ground Environment will comprise an Administrative Domain for each organisation participating in the ATN, and each such organisation will implement one or more Routing Domains, with IDRP used to exchange routing information.

In the ATN, in addition to the ATN wide RDC, it is anticipated that Administrations and ATN regions will, wherever possible, organise their addressing plans and form RDCs, such that route aggregation can keep the amount of routing information passed between organisations and regions to an absolute minimum.

The ATN Addressing Plan apportions a separate part of the address space to each ICAO Administration and to each IATA airline and other organisations. This allows for great flexibility in use, however, participating organisations are strongly recommended to co-ordinate the allocation of address to maximise the possibilities of route aggregation. For example, in Europe, Administrations should implement a co-ordinated addressing plan with a unique address prefix for Europe and address assignment that reflects the actual topology of the European ATN Internet. For similar reasons, airlines, and especially small regional airlines should consider service provider relative addresses.

2.8 The Mobile Routing Concept

2.8.1 Mobility and Routing Domains

While the scaleability of an Internet demands that Routing Domains near to each other are characterised by similar address prefixes, this is not an absolute requirement. Routing

Domains can be adjacent, have totally dissimilar address prefixes and still interconnect successfully. Furthermore, with a dynamic routing protocol, such as IDRP, two Routing Domains need only to interconnect when they need to, and are both active on the same network. The onward re-advertisement of routes can inform the rest of the ATN Internet about such a temporary connectivity while it exists, and the loss of connectivity when it occurs. A Routing Domain can thus temporarily join an Internet at one point of attachment, then disconnect and join the Internet at some other point, the only impact being in the efficiency of routing information distribution, and eventually on scaleability.

This property of the routing architecture and of IDRP, is exploited by the ATN to support Mobile Routing.

In the ATN, the systems onboard an aircraft form a Routing Domain unique to that aircraft and characterised by one address prefix for ATSC systems, and another for AISC systems. As an aircraft proceeds on its route, it interconnects with ground based Routing Domains over the various air/ground networks, the actual network used and Routing Domain interconnected with dependent on the aircraft's actual position, and the airline's routing policy. Routing Information is then exchanged between ground Routing Domains, using IDRP, so that all ground Routing Domains are aware of the current route to that aircraft. This is illustrated in Figure 2-11.

In this example, there are four ground based Routing Domains RD1 through to RD4. RD1, RD2 and RD3 all support air/ground datalinks, while RD4 depends on the other three for air/ground communications. The aircraft currently has communications over air/ground datalinks with both RD2 and RD3.

Using IDRP, both RD2 and RD3 advertise a route to the aircraft's systems, to RD4. RD4 chooses between these two available routes using its own Routing Policy, which might, for example, favour the route through RD3. Similarly, the aircraft's router must choose between the routes to RD4 offered by RD2 and RD3. It need not make the same choice as RD4.

As the aircraft continues on its journey, it may lose communication with RD3. For example, it goes out of range of the VHF datalink it was using to communicate with RD3. RD3 informs RD4 of this situation by issuing the appropriate IDRP protocol to withdraw the route, and RD4 now changes to using the route offered by RD2, as it is now the only route to the aircraft. The aircraft's router also recognises the loss of communication with RD3 and must now route all traffic via RD2.

Further on the journey, the aircraft comes into contact with an air/ground datalink offering communication with RD1. A datalink is established and routing information exchanged. RD1 now advertises the new route to the aircraft, to RD4. RD4 now once again has two routes to the aircraft and must make a choice between them using its local routing policy rules. It might, for example, now prefer the route through RD1, in which case all data to the aircraft is now routed via RD1. The router in the aircraft also goes through a similar decision process.

While the topology of the ATN ground environment is much more complex than the above example, this is essentially how mobile communications is implemented by the ATN.

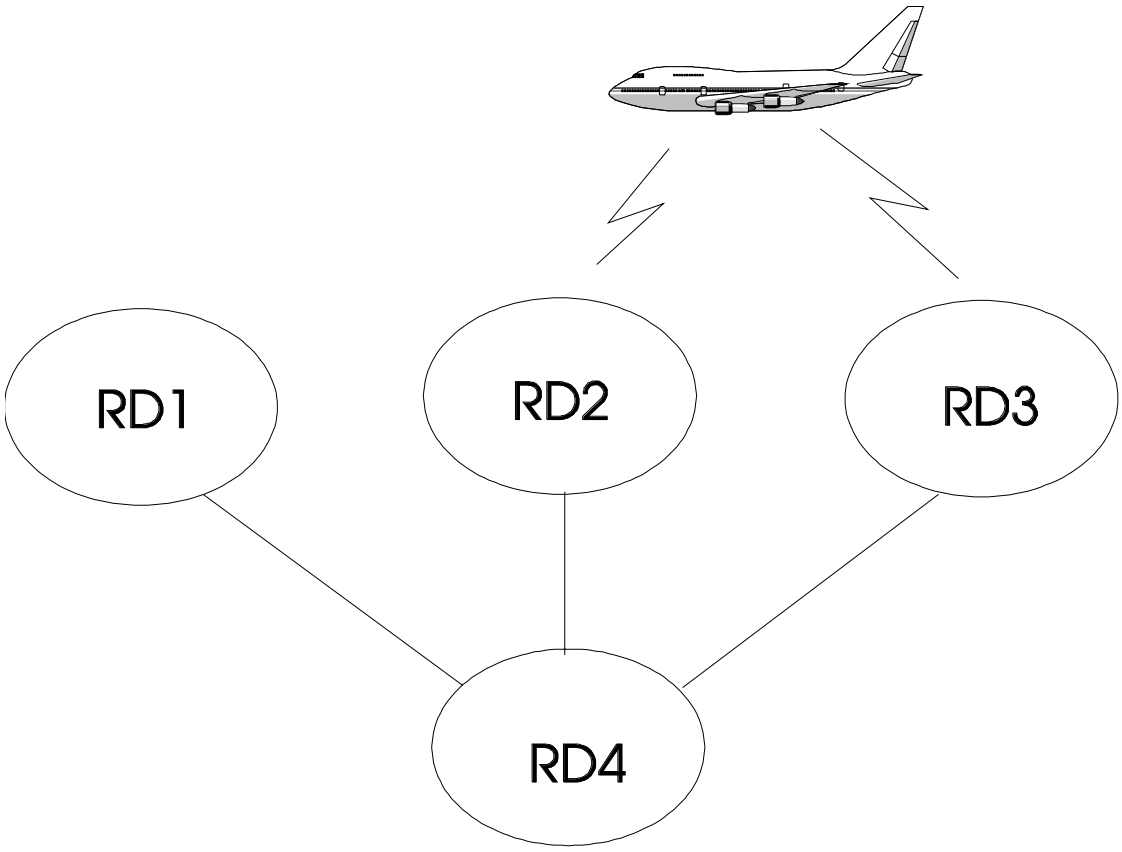

Figure 2-11 Mobile Routing Example

2.8.2 Containing the Impact of Mobility

While the principles of mobile routing outlined above are straightforward they are not scaleable using the existing IDRP mechanisms associated with Route Aggregation and RDCs. The problem is that even if an aircraft is given an address prefix similar to the address prefixes that characterise the ground Routing Domains at the start of its journey, such a similarity is unlikely to be maintained for the duration of the flight. Route Aggregation possibilities are thus very limited.

Instead, an alternative mechanism has been developed to permit mobility within a scaleable Internet architecture, building on two concepts: the ATN Island, and the “Home” domain (see 2.8.4 below). In addition, the ATN Addressing Plan specifies a common address prefix for all aircraft and, subordinate to that address prefix, specifies a unique address prefix for the aircraft belonging to each airline, and the General Aviation Aircraft of each country.

2.8.3 Routing to Mobiles within an ATN Island

An ATN Island is simply an ATN region comprising a number of Routing Domains, some of which support air/ground datalinks. These Routing Domains form an RDC, as illustrated in Figure 2-12, and an ATN Island is essentially an RDC in which certain Routing Policy rules are followed. All ATN Routing Domains that have air/ground datalink are members of an ATN Island and, although most ATN Routing Domains which do not have air/ground datalink capability will also be members of ATN Islands, they do not have to be and can still have access to routes to aircraft if they are not a member of an ATN Island RDC. Routes to destinations in ground based Routing Domains will be exchanged by ATN Routing Domains, both within an Island and between Islands. However, this is outside of the context of the ATN Island. The ATN island exists to support routing to mobiles and only applies to this case.

Within each ATN Island, at least one Routing Domain forms the Island's *backbone*. This is another RDC comprising all backbone Routing Domains in the same ATN Island.

Within the ATN Island, the Backbone RDC provides a default route to *all aircraft*, as illustrated in Figure 2-12, this is advertised to all other Routing Domains within the Island as a route to the common address prefix for all aircraft.

Routing Domains with routes to aircraft then have a simple routing policy rule to determine to which adjacent Routing Domain they must advertise such a route[1]. This is the Routing Domain currently advertising the preferred route to *all aircraft*. This will be a backbone Routing Domain if such a Routing Domain is adjacent, otherwise it will be a Routing Domain that provides a route to the backbone. Either way the impact of such a policy rule is that the Backbone RDC is always informed about routes to all aircraft currently reachable via datalinks available to the Island's Routing Domains, and can thus act as default route providers for packets addressed to airborne systems.

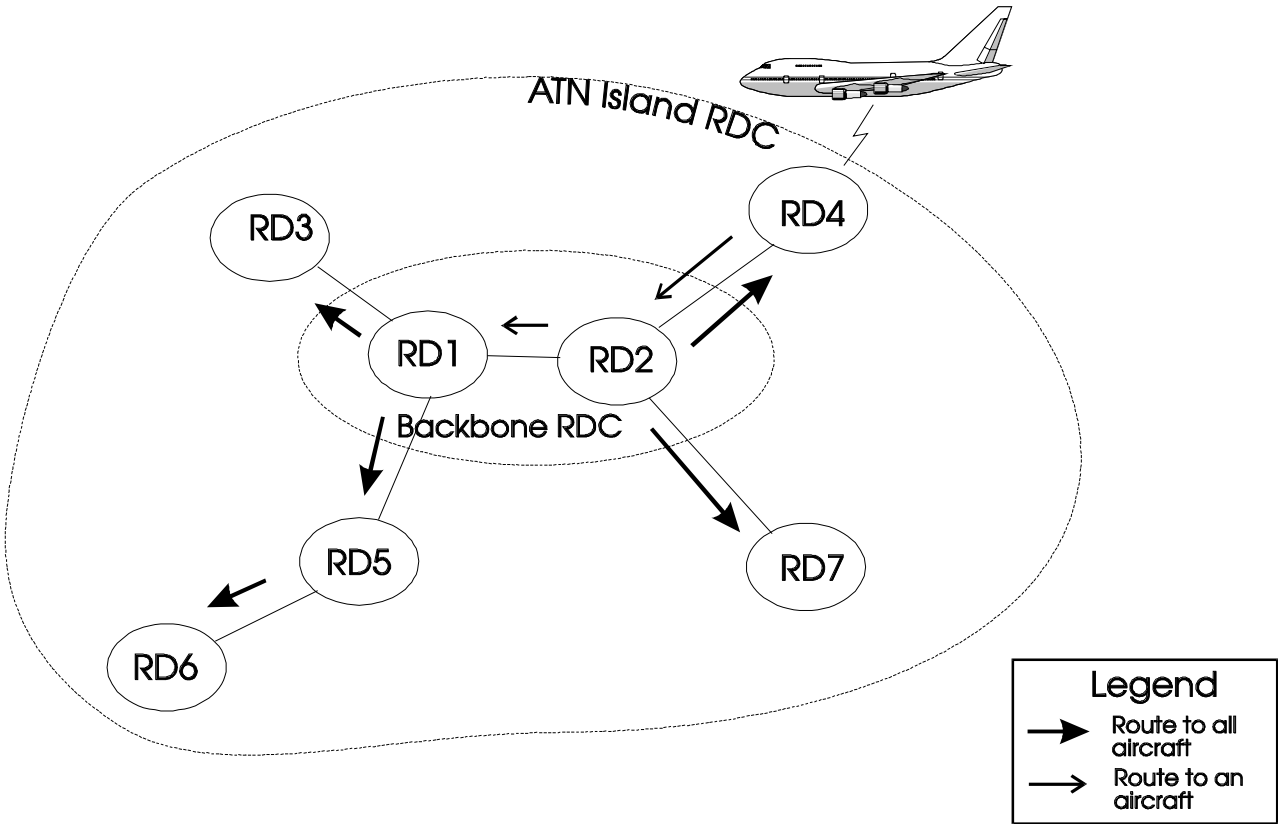

Figure 2-12 Mobile Routing Within an ATN Island

Routing Domains off the backbone also have a simple routing decision to make when they need to route a packet to a given aircraft. It is routed along the explicit route to the aircraft if it is known by them, or on the default route to all aircraft via the backbone, otherwise. Routing with IDRP always prefers routes with the longest matching address prefix. Therefore, the default route to all aircraft is always a shorter prefix of that for an explicit route to an aircraft, and this routing strategy happens automatically without any special provisions.

[1] A route to an aircraft is readily identifiable from the destination address prefix, as all address prefixes that characterise an aircraft Routing Domain descend from a unique address prefix.

The above is not the only policy rule that can apply to routes to aircraft. Routes to aircraft can be advertised to any other Routing Domain within the Island, provided that a policy rule is set up to allow this. This may be because there is a known communication requirement which makes bypassing the backbone desirable, or because it is desirable to provide a second (hot standby) route to aircraft from the backbone. The architecture accommodates these requirements. The only limitation on this is that imposed by the overhead of supporting routes to mobiles (see 2.8.7 below).

Within the Backbone RDC, all Routing Domains must exchange all routes to aircraft, which are advertised to them, they are then able to act as default routers to any aircraft currently in communication with the ATN Island. However, because the backbone routers need to know routes to all such aircraft, their capacity places a limit on the number of aircraft that can be handled by an ATN Island and hence on the effective size of the Island.

The ATN Island is only the first part of achieving a scaleable routing architecture for mobile routing. Its true benefit is to focus the overhead of handling the potentially large number of routes to aircraft on a few specialised routers in the backbone. Off the backbone, a Routing Domain with an air/ground datalink needs only the capacity to handle the aircraft supported by its datalink, and there is a similar impact on Routing Domains that are Transit Routing Domains providing a route between the backbone and an air/ground datalink equipped Routing Domain. For all other Routing Domains on the Island, there is no impact on routing overhead due to aircraft.

In the absence of a backbone, all routers within the Island would need to be explicitly informed with a separate route to each aircraft, if they were to be able to route to any aircraft currently in contact with the Island. This is because there is very little probability of route aggregation with routes to aircraft.

2.8.4 Routing to Mobiles between ATN Islands

ATN Islands can be set up such that their geographical spread matches Air Traffic Control communication requirements and, for ATC purposes, there may not be a requirement to provide inter-Island communications in respect of aircraft. However, airline operational requirements are perceived to require this, and hence the mobile routing concept is developed to provide a greater level of scaleability.

The mechanism used to achieve this derives from the concept of the “Home” domain.

Aircraft for which inter-Island communications are required must have a “Home” domain, which is a Routing Domain in an ATN Island’s backbone. This “home” need not be in either the ATN Island through which the aircraft is currently reachable, or in the ATN Island with which communication is required. The role of the “Home” domain is to advertise a default route to all the aircraft belonging to an airline, or the General Aviation aircraft of a given country of registration. This default route is advertised to all other ATN Island’s backbone routers.

The operation of the “Home” domain is illustrated in Figure 2-13. In this example, ATN1 is the ATN Island acting as the “Home” for all aircraft belonging the same as airline as the aircraft illustrated as currently reachable via ATN4. ATN1 advertises the default route to all such aircraft to all Islands in which it is in contact and, depending on local policy this route may be re-advertised to other Islands. In the figure, ATN3 re-advertises the default route on to ATN4.

The backbone routers of an ATN Island have a simple policy rule to implement for each explicit route to an aircraft that they have available. If a default route to all the aircraft in the

aircraft's airline or country of registration exists[2] then the actual route to the aircraft is advertised to the Routing Domain advertising that default route. Otherwise, the explicit route is not advertised outside of the Island. In Figure 2-13, the route to the aircraft is first advertised by ATN4 to ATN3 and then re-advertised to ATN1. In each case, the same policy rule is applied.

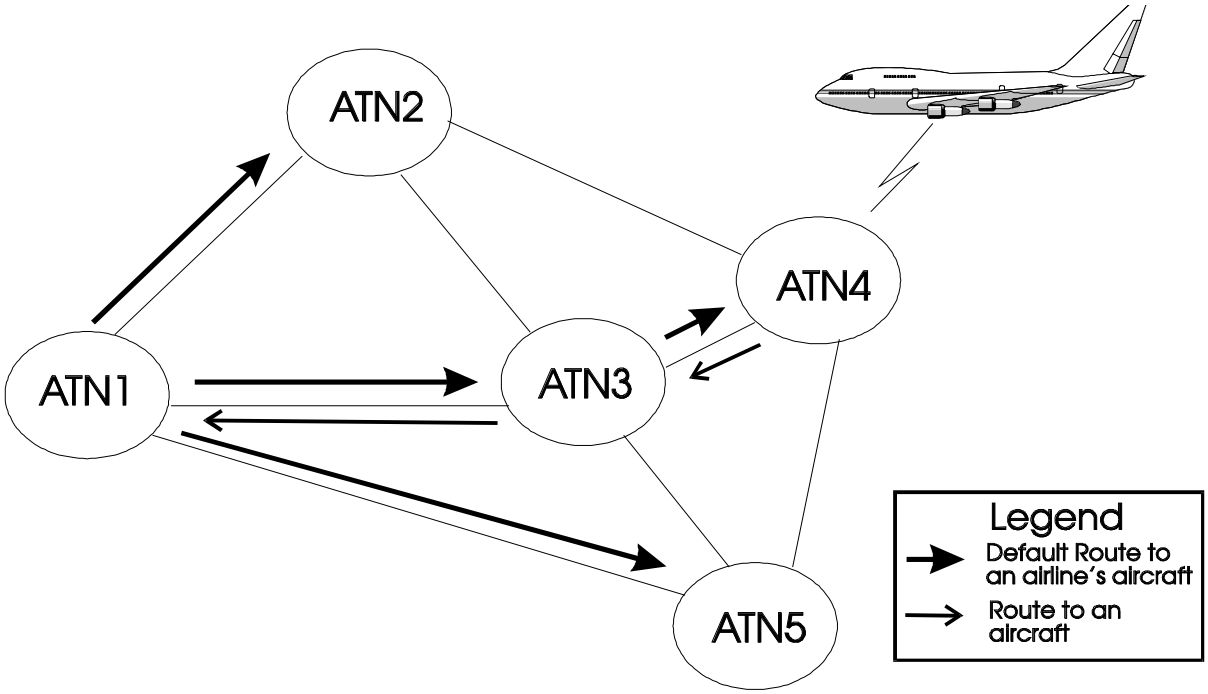

Figure 2-13 Inter-Island Routing

The impact of this rule is that the "Home" is always kept aware of routes to all of "its" aircraft. As it is also providing the default route to such aircraft, routers on other ATN Islands (e.g. ATN2) that have packets to route to one of that "Home's" aircraft will by default send those packets to the "Home" Routing Domain (ATN1), where the actual route to the aircraft is known, and thus the packet can be successfully routed to the destination aircraft (via ATN3 and ATN4).

In the above example, this is clearly non-optimal as ATN4 can be reached directly from ATN2. However, the loss of optimal routing is acceptable as, otherwise a scaleable architecture could not have been developed.

The impact of this strategy on routing overhead, is that an ATN Island backbone has to be capable of handling routes to all aircraft currently in contact with the Island, and all aircraft for which it is the "Home". Thus, and assuming that all ATN Islands are fully interconnected, if there are at most 'n' aircraft in contact with the Island, and the Island is "Home" to 'm' aircraft then:

n + m < "maximum number of routes to mobiles that can be handled by a backbone router"

[2] Such a route is generated by the "Home" Domain , and is readily identifiable from the destination address prefix, as all address prefixes that characterise an aircraft belonging to the same airline descend from a unique address prefix.

has to be true.

However, this limit is independent of the total number of ATN Islands or the total number of aircraft. It is thus possible to add more ATN Islands, or aircraft belonging to airlines whose "Homes" are on other Islands, without affecting this limit. The routing architecture thus allows for a much larger number of mobile systems than that permitted by a single ATN Island.

2.8.5 ATN External Interfaces and Mobiles

As discussed above, the ATN is itself an RDC and this will prove to be very useful should it ever prove necessary to provide access to ATN mobiles to other Internets. This is because at an RDC boundary, such as at the ATN boundary, Route Aggregation and reduction of path information can readily take place. In this case, it is possible to aggregate all routes to aircraft into a single route with a destination given by the address prefix for all aircraft. As the path information for such an aggregated route is also collapsed to a single ATN RDC identifier, the complexity of routing information exported at the ATN boundary can be kept to a simple single route that is independent of the number of aircraft and ATN internal complexity.

2.8.6 Impact on Air/Ground Datalinks

A final limiting factor on the ATN is the capacity of the air/ground datalinks. At present, these are low bandwidth communications channels and only the minimum routing information can be transferred over them.

IDRP is potentially an ideal protocol for this environment. Techniques such as RDCs and Route Aggregation can be used to minimise the information contained in each route. Furthermore, two or more routes to the same destination that differ only in security parameters, or service quality metrics, can be multiplexed together into a single message keeping the actual information exchanged to a bare minimum.

In addition, IDRP is a connection mode protocol and, as such, once a route has been advertised between a pair of Boundary Intermediate Systems it does not have to be retransmitted during the lifetime of the connection. A BIS-BIS connection is kept alive by the regular exchange of small "keepalive" packets, and once routing information has been exchanged it remains valid for the lifetime of the connection without having to be retransimitted.

The ATN uses these properties of IDRP to keep the transfer of routing information over an air/ground datalink to a minimum. When the datalink is first established, the airborne router will advertise a route to internal destinations for each combination of traffic (security) type and QoS metric supported. These routes will be combined into a single protocol message and downlinked for onward distribution through the ground ATN.

The ground router will also uplink routes to the aircraft and to keep the information down to a minimum, a further RDC is defined, comprising all ground ATN Routing Domains. This RDC, the "ATN Fixed RDC" ensures that for each uplinked route, the path information is collapsed to a single identifier, that for the ATN Fixed RDC.

The actual routes uplinked are subject to the policy of the ground router's Routing Domain. However, it is anticipated that routes will be provided to at least:

- the local Routing Domain (typically that providing Air Traffic Services), and
- the ATN as a whole,

in addition to other routes as determined by local policy.

The airborne router will then be able to choose between the alternative routes (via different) ground routers to these destinations.

2.8.7 The Impact of Routing Updates

The above discussion has illustrated how a scaleable routing architecture can be developed in support of mobile routing. It is now necessary to consider the factors that limit the number of routes to aircraft that an ATN Router can handle.

Each route known to a router occupies a certain amount of data storage and, while data store can be a limiting factor on the total number of routes handled, it is unlikely to be so in this case. The number of route updates that a router can handle is more than likely to be the limiting factor.

In the ground environment, route updates will usually only occur when changes occur in the local region of the Internet (changes further away are hidden by route aggregation). Typically the introduction of a new Routing Domain or interconnection, or the removal or loss of one of these will cause a change. However, the frequency of update is unlikely to be high.

However, with mobiles, such as aircraft, the situation is very different. Aircraft are constantly on the move, changing their point of attachment to the ATN, and hence generating routing updates. The impact of these updates needs to be minimised if the number of aircraft that can be handled by an ATN Island is to be maximised, and an important and useful feature of IDRP can be exploited in order to help meet this objective.

Vector distant routing protocols, such as IDRP, typically implement a “hold down” timer, which introduces a minimum delay between the receipt of a route and its re-advertisement. This timer is used to avoid instability due to frequent route changes, and the actual value of the timer is then usually a trade-off between a short timeout to give rapid response and a long timer to keep down routing overhead and minimise instability.

However, under IDRP, routing events that indicate a major change (i.e. new route or loss of a route) are not subject to a hold down timer, only those that report a minor change to an existing route are subject to a hold down timer. This means that IDRP is very responsive to connectivity changes while avoiding instability due to minor changes. For example, consider a simple extension to the previous example, illustrated in Figure 2-14.

In this example, RD4 provides a route to the aircraft, to RD5. When the aircraft loses contact with RD3, RD4 is immediately informed, as there is an effective zero length hold down timer for withdrawn routes. However, while RD4 recognises this event and switches to the route provided by RD2, it does not necessarily inform RD5 of this now minor change to the route immediately (the route still exists, only the detail of the path is different), and anyway, the update must be sent not less than the period **minRouteAdvertisementInterval** since any previous update. In this example, it should be noted that the minor change will not affect RD5’s routing decision, as it has no alternatives available.

Sometime later, the aircraft comes into contact with RD1. RD4 is immediately informed as this is a new route. However, even if RD4 switches to this new route, it does not inform RD5 of the change until the **minRouteAdvertisementInterval** has again expired.

This has important implications for the design of an ATN Island. If an Island’s air/ground datalinks are all connected to Routing Domains which are themselves adjacent to the Backbone RDC, all connectivity changes will be immediately reported to the Backbone giving a high route update rate. On the other hand, if there are intermediate Routing Domains between the backbone and the Routing Domains connected to air/ground datalinks, then the update frequency can be significantly reduced, without affecting the responsiveness to real connectivity changes.

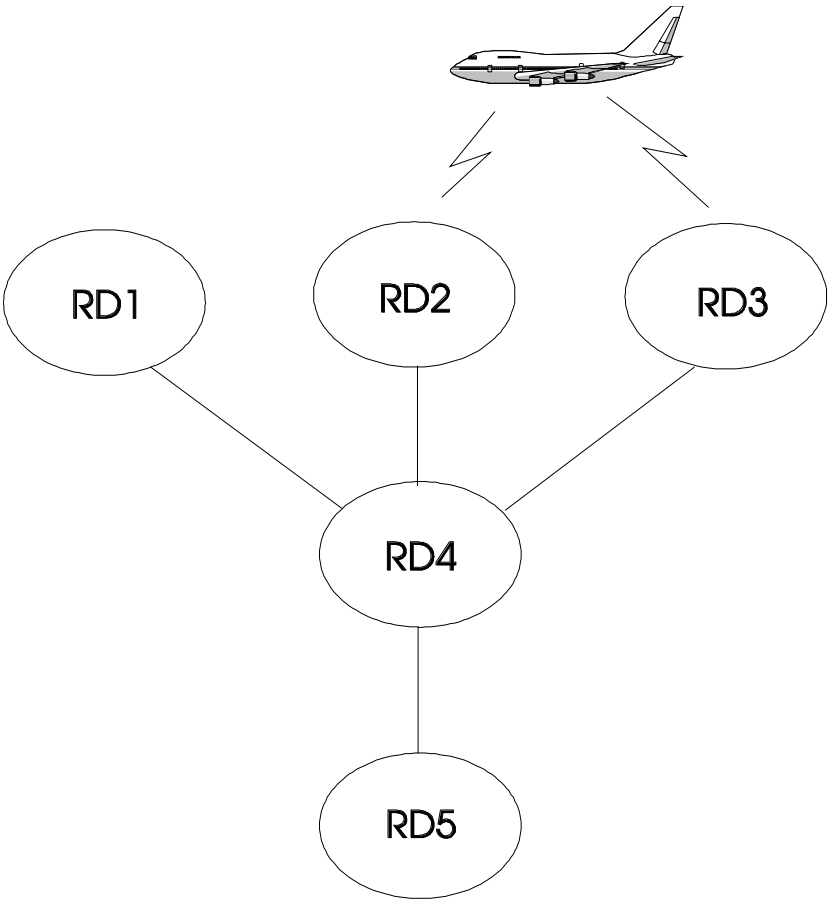

Figure 2-14 Impact of a Hold Down Timer

This is an important benefit derived from using IDRP to support mobile routing compared with, for example, a directory based approach to mobile routing. Under a directory based approach, there would be a central directory server on each ATN Island (c.f. the Backbone), updates on the position of aircraft would be sent direct to the directory, and other routers would consult the directory in order to determine the current location of a specific aircraft. In terms of overhead, this situation is analogous to an ATN Backbone Routing Domain directly connected to each Island Routing Domain with air/ground datalink capability, and the directory has to be able to take the full update rate. IDRP can, however, distribute the update load throughout the ATN Island.

Routes advertised to an aircraft's "Home" are also affected by the hold down timer and, in this case, RDCs and the Hold Timer work together to keep the routing overhead to an absolute minimum.

As an ATN Island is an RDC, routes advertised to other Islands have their path information for the transit through the RDC replaced by a single RDC identifier, and therefore, in many cases, changes in the route will not even be visible to another ATN Island. When changes are visible (e.g. a change in hop count or QoS metric), and such changes can be kept to a minimum by careful network design, then the Hold Timer limits the rate at which such changes can be advertised and prevents minor changes which are also short lived, being exported outside of the Island.

2.8.8 Failure Modes

In the pure ground-ground environment, loss of a router or a communications path can be readily recovered from provided an alternative route exists and routing policy permits its use. However, the situation is not so straightforward with the policy rules that support

mobile routing. The ATN Mobile Routing Concept depends upon two default route providers, the Island Backbone and the “Home”. Failure of either of these or loss of access to them will impact mobile routing.

2.8.8.1 Loss of the “Home”

Loss of the “Home” may come about from either the loss of the Routing Domain advertising a route to the “Home” for a given set of aircraft, or the loss of the communications path to it. The consequence of either failure is clear: the affected aircraft are now only reachable from systems on the ATN Island to which they are currently adjacent.

In practice, there should not be a single point of failure related to the “Home” Routing Domain. A Routing Domain may comprise many Boundary Routers, each of which may advertise the route to the “Home”. Only loss of all of these Boundary Routers will result in the complete loss of the route to the “Home”. Furthermore, there may be many communications paths, using different network technologies, linking two adjacent Routing Domains. Such concurrent links may be between the same pair of Boundary Routers, or between different pairs. Only if all such links are lost, will total loss of communications occur.

Therefore, it will always be possible to design a network topology that will avoid the loss of the “Home” being due to any single failure, and which can ensure that the probability of loss of the “Home” is kept within acceptable limits. Where inter-Island communications are required in support of air safety, then the design of the Inter-Island ATN topology must be supported by an appropriate failure mode analysis to ensure that safety limits are maintained.

2.8.8.2 Failure of an ATN Island Backbone

Failure of an ATN Island may also result from the failure of the Routing Domain(s) that comprise an Island’s Backbone, or of communications paths with an Island’s backbone. The consequence of such a failure is that the aircraft currently adjacent to the Island are only reachable from the Routing Domains supporting air/ground datalinks with those aircraft, and any other Routing Domains on the Island to which routing information to those aircraft is advertised according to explicit policy rules.

For similar reasons to those already discussed above in 2.8.8.1, there is no need for loss of an Island Backbone to be due to a single point of failure, and an appropriate network design should be developed for each ATN Island to ensure that the probability of the loss of the backbone is within acceptable limits.

2.8.9 Optional non-Use of IDRP

Simple networks can often avoid dynamic routing mechanisms in favour of statically defined routing tables, initialised by a System Manager. However, even in the early ATN, the existence of Mobile Systems does not permit the general use of static routing techniques. Aircraft may join and leave the air/ground subnetwork(s) at any time and this dynamic behaviour must be recognised by the routers and reflected in the routing tables. Some dynamic adaptive routing protocol is needed to support this requirement. IDRP is specified for this purpose. However, implementing IDRP functionality on an airborne router may not be practicable in early.

An alternative approach is possible using the ISO 9542 ES-IS protocol. An exchange of Intermediate System Hello (ISH) PDUs is already required as part of the route initiation process, and, in a limited topology, an exchange of ISH PDUs can be sufficient to provide the exchange of dynamic routing information necessary to support mobile routing. Furthermore, a regular exchange of ISH PDUs (part of the normal operation of ISO 9542) can be used to keep the link between ground and airborne routes “live” in the absence of IDRP.

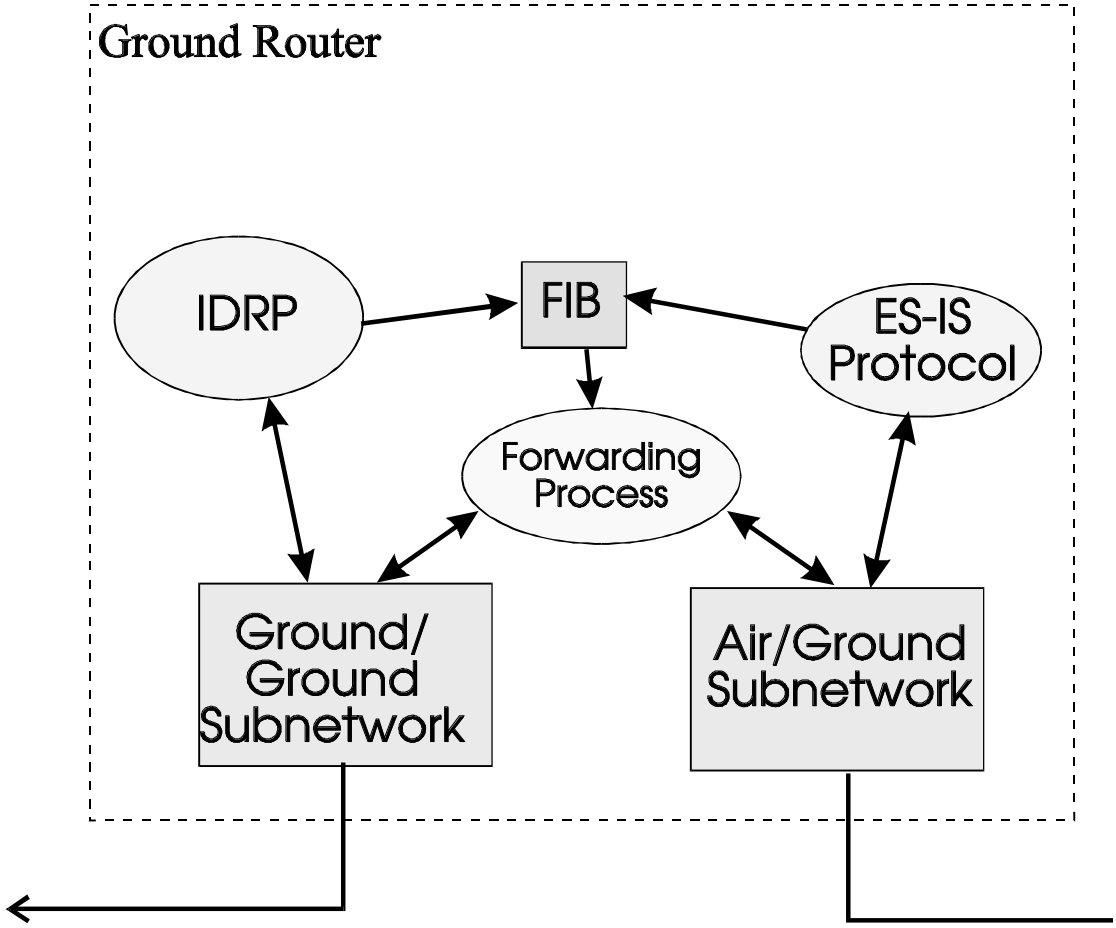

Figure 2-15 Architecture of an Initial Ground Network Router

Such a use of the ISH PDUs depends upon an assumed relationship between the Network Entity Title (NET) of each router - which is essentially the router's address - and the NSAP Addresses in the ground and airborne End Systems. The NET is exchanged as part of the ISH PDU. When the Air/Ground router receives an ISH PDU from an airborne router, it may infer from the ATN Addressing Plan the common NSAP address prefix of all NSAPs onboard that aircraft. This being the first eleven octets of the NET. This NSAP Address Prefix may then be used as the destination of a route to the NSAPs onboard that aircraft and the route entered into the ground router's Forwarding Information Base. It is then possible for the ground End Systems to send data to airborne End Systems on that aircraft.

The same process may also take place on the Airborne Router, on the receipt of an ISH PDU from the Air/Ground router, enabling airborne End Systems to send data to ground End Systems. The routing information remains current until either a regular exchange of ISH PDUs ceases, or the subnetwork connection is cleared, when the ground and airborne routers remove the associated routes from their forwarding information bases.

The architecture of a ground router implementing this functionality is illustrated in Figure 2-15. The architecture is straightforward enough with the ES-IS protocol active on both subnetworks. Both protocol entities update the Forwarding Information Base (FIB) which is, in turn, used by the Forwarding process to route packets.

As the ISH PDU mechanism is also used for route initiation in the full ATN, some convention for distinguishing between its use in this scenario and in the full ATN is necessary. This can be readily achieved by addressing conventions. A non-zero value in the NET's "SEL" field (254 decimal) is used to signal use of the above procedures.

Routing information learnt in this way by the Air/Ground Router may then be disseminated throughout the ATN Ground Environment using normal IDRP procedures.

2.9 Route Initiation

2.9.1 The Purpose of Route Initiation

ICAO has adopted the use of Policy Based Routing procedures for routing between ATN Routing Domains (RDs), including the support of routing to mobile systems. Dynamic Routing Information is exchanged using the procedures specified in ISO 10747 and used and disseminated according to local routing policies specified in accordance with the ATN SARPs. However, before routing information can be exchanged between any two Routing Domains, it is first necessary to establish a communications path between Boundary Routers[3] in each of those RDs. The establishment of such a communications path is known as "Route Initiation".

Route Initiation procedures are required whenever two ATN RDs need to be interconnected. Since the ATN SARPs specify that, on board an aircraft, the communications systems and the applications processors that they serve comprises a Routing Domain, Route Initiation procedures also apply to the establishment of air/ground communications.

Route Initiation commences when the decision is made to establish a communications path between two ATN RDs. Route Initiation finishes upon the initial exchange of routing information between the Boundary Routers, or the unsuccessful termination of the Route Initiation procedure.

Note: Boundary Routers within the same RD also exchange dynamic routing information using ISO 10747. The Route Initiation procedures are the same as for inter-domain connections except that both Routers will be under the control of the same administrator.

2.9.2 Ground-Ground Route Initiation

2.9.2.1 The Communications Environment

Ground-Ground communications typically use long lasting physical or logical communications paths. Route Initiation can normally be regarded as a rare event and will often be only semi-automated.

The communications networks in the ATN ground environment are outside the scope of the ATN SARPs, but can be assumed to include:

1. X.25 Public and Private Data Networks
2. Leased Lines
3. Integrated Services Digital Networks (ISDNs)
4. Frame Relay Services
5. The Public Switched Telephone Network (PSTN).

[3] The term Boundary Router may be read in most cases, as synonymous with the architectural entity "Boundary Intermediate System" (BIS). In practice, a Boundary Router includes a BIS along with Management Entities and and End Systems component to support such entities.

The actual choice of communications network is a matter for bilateral agreement between the organisations and states that wish to interconnect their RDs, and will depend on local availability, tariffs and policies. In many cases, high speed (e.g. V.32bis or V.34) Modems and the PSTN will be used as a backup for a dedicated data network.

The communications protocols used to provide the data link will also depend upon the communications network used and bilateral agreement. In the case of X.25 data networks, Frame Relay and communications services provided via the ISDN D-Channel, then the communications protocols are mandated by the data network provider. In the case of Leased Lines and the ISDN B-channel, then HDLC LAPB (ISO 7776) is the likely choice. For the PSTN, the asynchronous communications provided by V.32bis and V.34 Modems makes the Point-to-Point Protocol (PPP) as specified in RFC 1548, the likely choice.

Note: Route Initiation is not necessarily synonymous with the establishment of a communications link between two Boundary Routers. For example, the speed at which an ISDN B-Channel is established is such that it may be practicable to break the communication circuit during idle periods and re-establish it when there is data to send, whilst still maintaining a logical communications path between the two Boundary Routers. Route Initiation is concerned with the establishment of the logical communications path.

2.9.2.2 Summary of Procedures

The sequence of procedures for a typical ground-ground Routing Initiation is illustrated in Figure 2-16, and summarised below. They are discussed in greater depth in the following sections. This illustrates the co-ordination of two Systems (“A” and “B”) interconnecting over a common network. The procedures are:

1) Adjacent BIS MOs are established in both Systems. In each case, an MO is established to identify the other system and contains the parameters necessary to create and maintain a BIS-BIS connection with that system. Both systems will also have been configured with appropriate SNDCFs associated with each attached subnetwork.

2) A communications path is established over the subnetwork; typically one system is initiator and the other responder.

3) Establishment of the communications path is notified to the Systems Manager.

4) In response, the Systems Manager for each system adds a route to the local FIB and to the remote System, and

5) invokes the IDRP “Start Event” action, or re-run the decision process if a BIS-BIS connection already exists with the remote system.

6) On successful establishment of the BIS-BIS connection, Route Initiation completes.

Note: while the Systems Manager may be a real person explicitly issuing commands, the “Systems Manager” in the above description may alternatively be a procedural script carrying out an automatic action in respond to a Systems Management Notification.

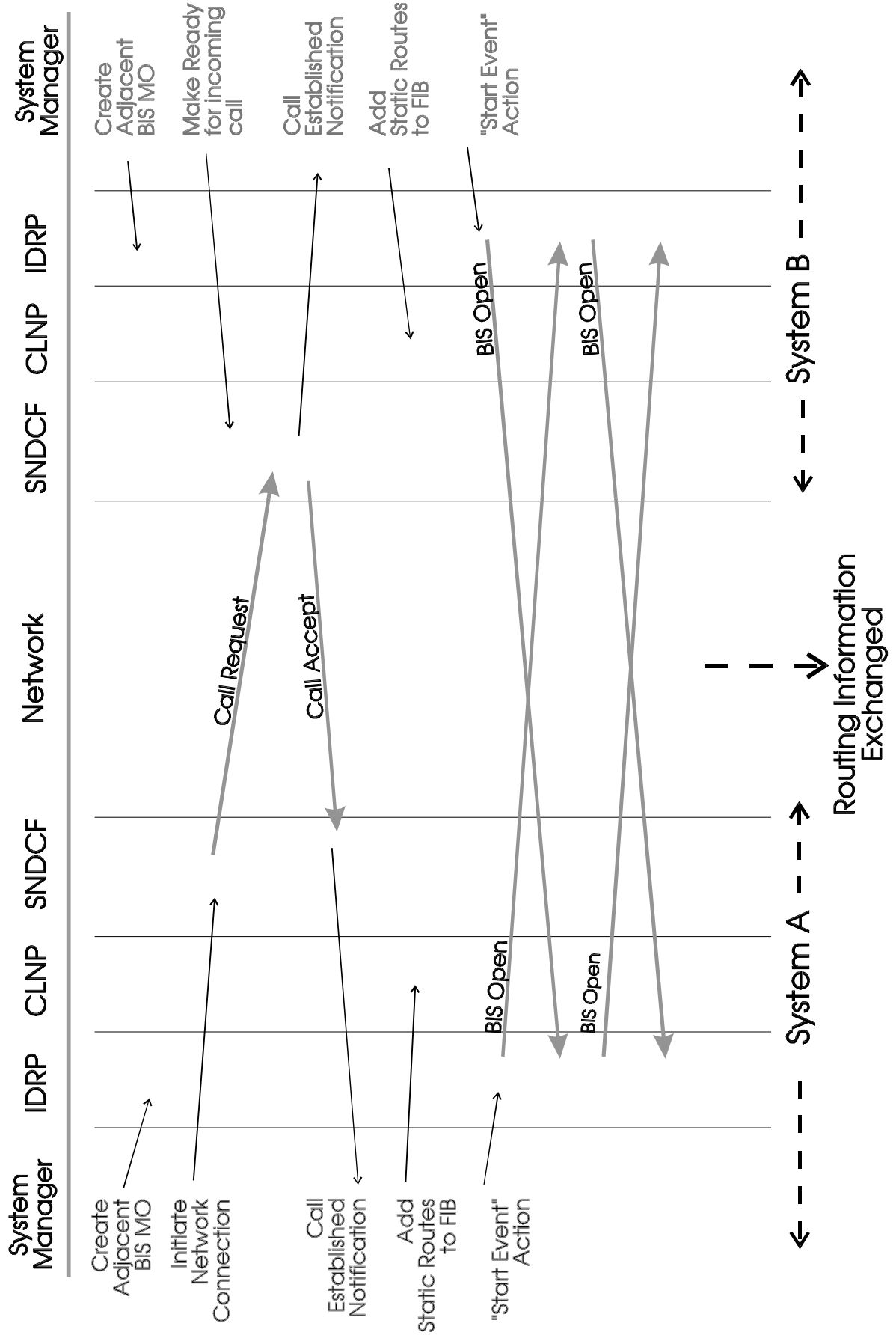

Figure 2-16 Ground-Ground Route Initiation Sequence

2.9.2.3 Initial Route Initiation

Route Initiation begins with the decision to establish a communications path between a pair of Boundary Routers, including the decision on which communications networks to use. The first procedure is to establish the underlying communications circuit between the Boundary Routers and hence to establish the logical communications path.

These procedures will be data network dependent and will require some sort of interaction between the respective Systems Managers. Typically, one Boundary Router will need to be in a passive state awaiting an incoming event (e.g. an X.25 call indication or a PSTN Ring Indication), while the other takes an active role and initiates circuit establishment (e.g. by generating an X.25 call request, or “dialling” the telephone call).

When appropriate to the type of data network used, the QoS, Security and Priority requested on any such call request, should be satisfactory for the exchange of routing information.

During this phase, there should normally be some validation to ensure that communications has been established with the correct remote system. This initial phase completes once the data link has been established.

2.9.2.4 Route Initiation in CLNP

The ATN SARPs specify the use of the Connectionless Network Protocol (CLNP) specified in ISO 8473 for ATN subnetwork independent communications. Establishing a data link (e.g. an X.25 virtual circuit) is a necessary condition for data to be exchanged between two Boundary Routers using CLNP, but not a sufficient condition. In order for the data link to be used by the CLNP Network Entity, and hence as a communications path for the forwarding of data packets, it is necessary to:

1. Assign an appropriate Subnetwork Dependent Convergence Function (SNDCF) to interface the data link to the Network Entity;

2. Update the Forwarding Information Base (FIB) to record statically known routes available over the data link and via the remote Boundary Router.

The former is necessary in order to match the characteristics of the actual network and communications protocol used over that network to the characteristics assumed by the CLNP Network Entity. The second is necessary in order to permit the exchange of dynamic routing information.

The SNDCF is typically specified for a network type and associated at system configuration time with a physical communication port. In most cases, the assignment of the SNDCF is implicit in the network over which communications is established, and no explicit action will need to be carried out to assign the SNDCF. Indeed, most implementations will required assignment of the SNDCF prior to establishment of the data link. However, for some network types there may be alternatives chosen at connection establishment time.

The FIB may be updated with any statically known routes that are known *a priori* to exist via the newly established data link, where a route consists of an NSAP Address prefix paired with an identifier for a data link. When forwarding data packets, the CLNP network entity locates the longest matching NSAP Address Prefix in the FIB, when matched against the packet’s destination NSAP Address, and then queues the packet for transmission over the associated data link. Multiple FIBs may also exist matching different QoS and security requirements. So that Routing Information may be exchanged, the FIB associated with the QoS level used for the exchange of Routing Information, must be updated to include, as a minimum, a route to the network entity located on each Boundary Router. to which a data link has been established.

Therefore, once a data link has been established to a remote Boundary Router, the System Manager must either directly, or via an automated procedure, insert into the FIB associated with the Security and QoS level used for the exchange of Routing Information, a route associating:

a) an NSAP Address prefix that is a prefix for the NET of the remote Boundary Router at the other end of the newly established data link. As a minimum, this prefix may be the complete NET. And,

b) the data link to that remote Boundary Router.

Note 1: the reverse must also take place when the data link is terminated i.e. the above route must be removed from the FIB.

Note 2: alternatively, such routes may be entered into the FIB at system initialisation. However, this strategy only gives satisfactory results if there is one and only one possible data path to the remote Boundary Router.

2.9.2.5 Route Initiation in IDRP

The ATN SARPs specify the use of the Inter-Domain Routing Protocol (IDRP) specified in ISO 10747 for the exchange of dynamic routing information between Boundary Routers. Once a communications path has been established between two Boundary Routers and sufficient static routing information entered into the local FIB in order to enable the forwarding of data packets to the remote Boundary Router itself, IDRP may be used to exchange dynamic routing information.

IDRP may only exchange dynamic routing information when a BIS-BIS connection has been established. This is a logical connection established by using the IDR Protocol, which in turn uses CLNP to transfer the protocol data units (BISPDUs) to the remote IDRP entity. A BIS-BIS connection supports the reliable transfer of dynamic routing information between Boundary Routers.

Prior to establishing a BIS-BIS connection it is necessary to create an “Adjacent BIS Managed Object” to provide the information necessary to establish and maintain a BIS-BIS connection with an explicitly identified remote Boundary Router. The information held includes the NET of the remote Boundary Router, authentication data, the specific IDRP procedures used to establish the BIS-BIS connection and timer values. One such MO exists for each remote Boundary Router with which IDRP may exchange routes. Typically, this MO is setup in advance of the underlying communications path, and will usually be created once agreement to interconnect has been reached.

Once the FIB has been updated with a route to the remote Boundary Router, the “start event” action is requested of the Adjacent BIS MO associated with that Remote Boundary Router. This initiates the procedures for creating the BIS-BIS connection and followed by the exchange of dynamic routing information. It is the final action of the Route Initiation procedure.

During establishment of the BIS-BIS connection either or both IDRP entities will take an active role in connection establishment, or one will be active and the other passive. The role, active or passive, is determined by information configured into the Adjacent BIS MO. If one IDRP entity is to be passive, then Systems Managers must ensure that the other is configured in the active role. If both IDRP entities are configured in the active role, then the BIS-BIS connection establishment procedures are less efficient, than if one is in the passive role. However, given that the loss of efficiency is small and typically of no consequence given that ground-ground BIS-BIS connections are usually long lived, Organisations and States are recommended by the SARPs to always configure the Adjacent BIS MOs for BIS-BIS connections between ground ATN Boundary Routers for

BIS-BIS connection establishment in the active role. This is to avoid to risk of both being configured in the passive role by mistake.

However, there is one exception to the above. That is when the newly established communications path is to a remote Boundary Router with which a BIS-BIS connection already exists. This is possible when multiple networks are available between the same pair of Boundary Routers. Multiple concurrent connections may be desirable in order to give high availability through redundancy and to provide additional data transfer capacity.

IDRP permits only a single BIS-BIS connection between a given pair of Boundary Routers, irrespective of the number of underlying connections and networks that may join them. Therefore, the Systems Manager should check to see if a BIS-BIS connection already exists to the remote Boundary Router and only invoke the Start Event Action if one does not already exist. This action will in any case, be ignored if issued when a connection does already exist.

However, other action may be appropriate if there is a need to recognise the different QoS that may be available when a new communications path is opened up (or lost), or a change in the Security Types that may be support by alternative communications paths to the same remote Boundary Router. In such cases, the SARPs require that the IDRP Decision Process is aware of the aggregate QoS and Security Restrictions over the communications paths to a given remote Boundary Router (Adjacent BIS). The SARPs require the Decision Process to update the QoS on received routes (when processing the adj-RIB-in) to reflect the QoS of the communications path and to use this updated QoS when determining the degree of preference of the route and when re-advertising it. They also require that the Decision Process does not place in the IDRP adj-RIB-out, any routes with Security Types incompatible with any restrictions that exist on the aggregate communications path. For example, if none of the available communications paths to a given remote Boundary Router permits the transfer of “Administrative” data, then a route with a Security Type reflecting administrative data may not be placed in the Adj-Rib-out for that Router (and hence advertised to it).

Therefore, whenever an additional communications path to a given remote Boundary Router becomes available (or is lost), the Systems Manager must cause the IDRP Decision Process to be re-run, instead of invoking the Start Event.

2.9.3 Air-Ground Route Initiation

Air-Ground Route Initiation is similar to ground-ground Route Initiation, but differs for the following reasons:

I. ICAO specified subnetworks are used for air-ground communications with their procedures for use mandated by SARPs rather than subject to bilateral negotiation.

II. Route Initiation typically starts as soon as communication is possible e.g. an aircraft coming into range of a Mode S Interrogator, and, in consequence Route Initiation starts as soon as the Systems Manager is notified of the possibility of communications (e.g. capture by a Mode S Interrogator).

III. It is not realistic to pre-configure Adjacent BIS MOs for every aircraft that may come into contact with a given ground ATN Router; these MOs must be set up as part of the Route Initiation Procedure.

IV. Special procedures are necessary to identify the NET of a remote ground or airborne Router during the Route Initiation procedure as, in general, it is not possible to know this in advance.

V. Due to avionics limitations, not all aircraft will be able to implement IDRP and interim procedures inferring route availability over air-ground links must be accommodated.

2.9.3.1 Communications Environment

The following ICAO Air-Ground data networks are expected to be used to support the ATN:

1. The Aeronautical Mobile Satellite Service (AMSS)

2. The VHF Data Link (VDL)

3. The Mode S Data Network

In each case, ITU recommendation X.25 provides the data network access procedures, and the responsible ICAO Panel's have required that:

a) AMSS communications are "air initiated", that is the aircraft is responsible for initiating communication with the ground

b) VDL communications are similarly air initiated.

c) Mode S communications are "ground initiated" that is a ground ATN Router attached to a Mode S data network is responsible for initiating communications with an aircraft.

2.9.3.2 Summary of Procedures

The Air-Ground Route Initiation procedures are illustrated in Figure 2-17, and summarised below. They are discussed in greater depth in the following sections. This figure illustrates the case where a Join Event is generated by the air-ground subnetwork. If the subnetwork cannot generate a Join Event then the procedures start with the Call Request, as part of a polling procedure. System "A" is the initiator and System "B" is the responder. If the air-ground subnetwork is air-initiated then System "A" represents the Airborne Router, and System "B" the Ground Router. If the air-ground subnetwork is ground-initiated, then System "A" represents the Ground Router, and System "B" the Airborne Router.

The Route Initiation Procedures are:

1) When an aircraft attaches to an air-ground subnetwork, a Join Event is generated, potentially to both Airborne and Ground Routers. If received by System "B", the Join Event is ignored; System "B is ready to receive incoming calls as soon as it attaches to the Mobile Subnetwork.

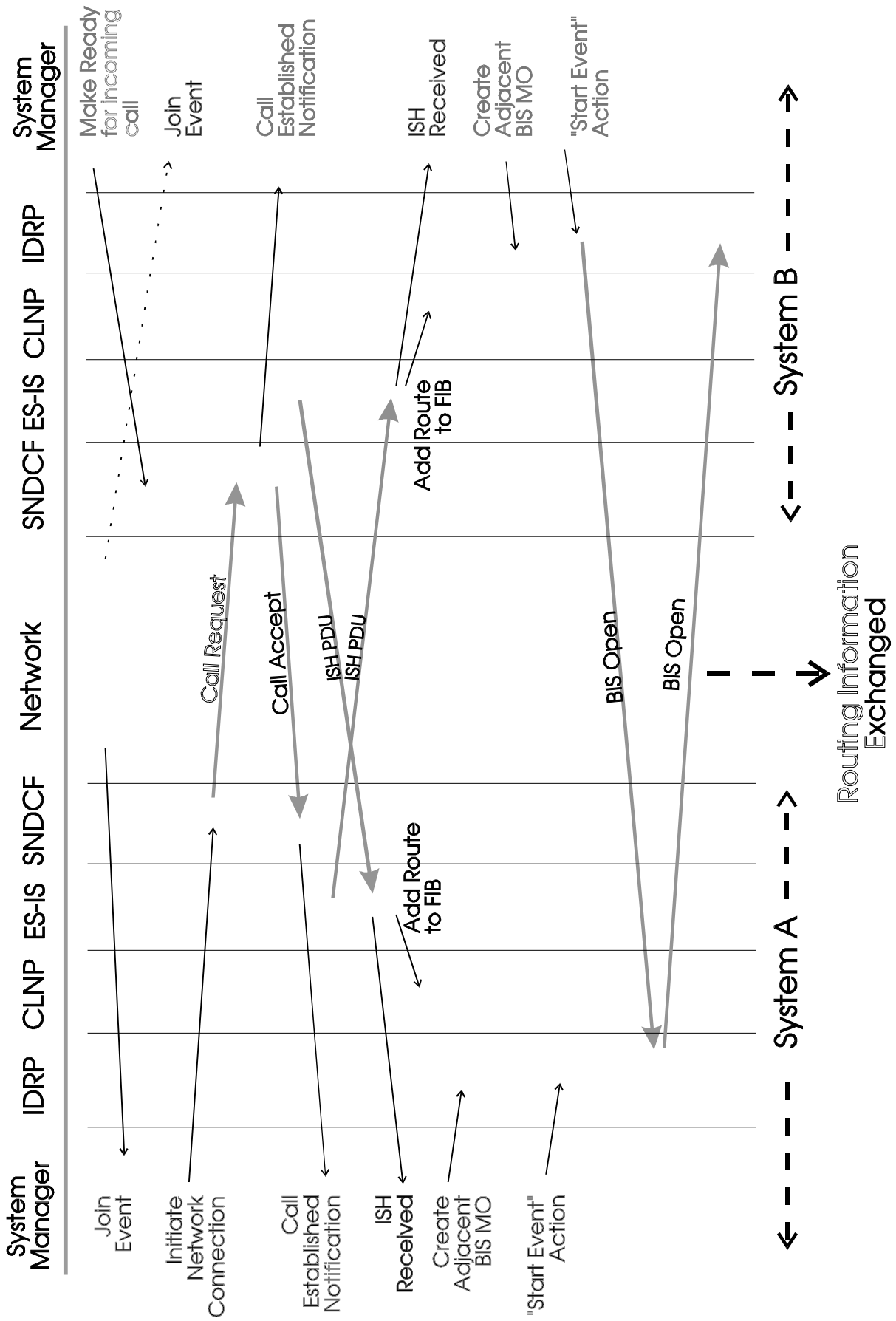

Figure 2-17 Air-Ground Route Initiation Procedures

2) System “A” acts on a Join Event by initiating the establishment of a virtual circuit to the address given by the Join Event, provided such a connection is permitted by local policy, or

3) if polling, System “A” issues a Call Request to the next address on its poll list.

4) When an incoming call is received by System “B”, it accepts the call if permitted to do so by local policy, and generates and sends an ISH PDU to System “A” over the newly established virtual circuit. This ISH PDU includes the NET of the System “B” Network Entity.

5) When System “A” receives a Call Accept, it too generates an ISH PDU, and sends it to System “B” over the newly established virtual circuit. This ISH PDU includes the NET of the System “A” Network Entity.

6) On receipt of the ISH PDU, both systems update their local FIB to include the routing information received on the PDU, and

7) if one does not already exist, the local IS-SME creates an Adjacent BIS MO for the remote system identified by the ISH PDU, and issues a “Start Event” action to that MO. The Adjacent BIS MO created in System “A” identifies the system as being in the passive role, while the System “B” MO identifies the system as being in the active role. Hence on receiving the start event, System “A” simply listens for an incoming BIS OPEN PDU, while System “B” generates one and sends it to System “A”. System “A” responds to the OPEN PDU, with its own OPEN PDU.

8) Alternatively, if a BIS-BIS connection already exists with the remote system, then the IDRP Decision Process is re-run.

9) Once the BIS Open PDUs have been exchanged, the Route Initiation procedures have been completed.

2.9.3.3 Initial Route Initiation

In the air-ground environment, Route Initiation starts with the notification that an aircraft has come into contact with an air-ground subnetwork, and that a BIS-BIS connection should be established, so that dynamic routing information may be exchanged. In order to ensure the automatic and timely execution of these procedures, a management entity is required by the ATN SARPs to be implemented in each airborne Router and each ground Router with air-ground connectivity. This known as the “Intermediate System - Systems Management Entity” (IS-SME).

Note: The IS-SME is part of the Systems Management Agent for that Router and may also implement other functions outside of the scope of Routing Initiation.

The IS-SME may have to handle two different classes of air-ground subnetwork:

1) Air-Ground subnetworks that can recognise when an aircraft has come into contact with the subnetwork (e.g. logged on to a satellite, or captured by a Mode S Interrogator) and hence that a communications path may be established with that aircraft, and which report this event.

2) Air-Ground Subnetworks which have no mechanism for recognising the above event and/or reporting it.

In the former case, Route Initiation procedures commence when the air-ground subnetwork reports this event - known as the “join” event. In the latter case, Route Initiation additionally includes procedures to allow support Route Initiation in the absence of such an indication.

Note: Only when air-ground communications are air-initiated is it possible to establish communications without a join event.

2.9.3.3.1 The Join Event

Ideally, the Join Event should be a Systems Management Notification sent to the IS-SME from a Management Entity in the subnetwork itself. This notification should provide the following information:

1) A subnetwork identifier allowing the Boundary Router to associate the event with an air-ground subnetwork to which the Router is connected.

2) The address on that subnetwork of the remote airborne or ground Router.

3) The expected lifetime of the adjacency i.e. how long a communications path is expected to be available.

A Ground Router will typically receive a join event for each aircraft that joins each air-ground subnetwork to which the ground Router is attached. The receipt of such join events will therefore be a regular activity. An airborne Router will typically receive a join event for each ground Router on an air-ground network at the time it comes into contact with that air-ground subnetwork.

On receipt of a Join Event, an ATN Ground Router will, if communication is ground initiated, issue a call request to the subnetwork Address reported by the Join Event and thence establish a virtual circuit with the corresponding Airborne Router. An ATN Ground Router will ignore any Join Events received from air-initiated Air-Ground subnetworks.

Likewise, on receipt of a Join Event, an ATN Airborne Router will, if communication is air initiated, issue a call request to the subnetwork Address reported by the Join Event and thence establish a virtual circuit with the corresponding Ground Router. An ATN Airborne Router will ignore any Join Events received from ground-initiated Air-Ground subnetworks.

In each case, the QoS, Security and Priority requested on the call request should be satisfactory for the exchange of routing information. A local policy decision may also be taken to ignore a Join Event from certain sources.

2.9.3.3.2 The Join Event for Subnetworks that do not support ATN Systems Management

It is anticipated that not all ICAO air-ground subnetworks will support the ATN Systems Management protocols. In order to provide the equivalent of the join event, this Guidance Material provides the following guidance describing an alternative procedure for passing a join event to an air-ground Router. Future ICAO SARPs for air-ground subnetworks which do not specify support of ATN Systems Management should specify the following procedures or an equivalent procedure.

1) A communications path (e.g. a virtual circuit) is established between the ATN Router and a subnetwork processor (e.g. Mode S GDLP) by a Systems Manager and kept open as long as both Router and subnetwork are active.

2) Join events are passed from subnetwork processor to Router over this subnetwork connection and as discrete items of data (e.g. as a single packet), and passed to the IS-SME.

3) The Join Event packet is formatted as a sequence of fields according to Table 1.

2.9.3.3.3 Procedures for Air-Ground Subnetworks that do not Provide a Join Event

With this class of subnetwork, it is necessary to adopt a polling strategy in order to establish air/ground communications, and an Airborne Router must "poll" a list of Ground Routers that has been configured by the System Manager.

A suitable "poll" is a periodically repeated Call Request packet addressed to the DTE Address of a Ground Router. Such call requests are regularly repeated until they are answered with a Call Accept from the addressed Ground Router, and an Airborne Router may cycle through a list of Ground Router DTE Addresses until a connection is established. The QoS, Security and Priority requested on this Call Request should be satisfactory for the exchange of routing information.

Once a virtual circuit has been established, the Router may cease to cycle through its poll list, until the connection terminates (e.g, because the aircraft goes out of range of the mobile subnetwork), when it must resume polling for another connection. However, this may lead to unnecessary gaps in communications availability. Furthermore, not all ground Routers will support all security types required by the aircraft. The airborne Router is thus recommended to continue to cycle through its poll list, even when subnetwork connections exist, and to poll the remaining DTE Addresses on the poll list. Polling need only stop when the Router has made sufficient air/ground connections to satisfy its requirements for each supported traffic type, QoS and availability. Polling may resume when these requirements cease to be met

Note: Typically, there will be many more Airborne Routers on a mobile subnetwork than there are Ground Routers, regardless of the subnetwork's coverage area. Hence, while an Airborne Router can be expected to be configured with a complete list of Ground Router DTE Addresses, it is unlikely to be practicable for a Ground Router to be configured with a complete list of Airborne Router DTE Addresses. This is why subnetworks which do not provide information to DTEs on the connectivity status of other DTEs are only considered suitable for air-initiated BIS-BIS connections.

2.9.3.4 Route Initiation in CLNP

As a result of the handling of the Join Event or the "polling" procedure described above, a virtual circuit will have been established between Airborne and Ground Routers. The Mobile SNDCF specified in the ATN SARPs should also have been assigned to support the use of this virtual circuit by CLNP. As with ground-ground Route Initiation, it is now necessary for the IS-SME to add to each Router's FIB, a route to the NET of the remote Router's Network Entity, using the newly established virtual Circuit.

Field	Size, octets	Format	Status	Contents
Message ID	1	binary	required	’1’
Length	1	binary	required	Total message length, in octets
Version	1	binary	required	’1’
Lifetime	2	binary	required	Lifetime of link, in seconds
SNPA	var	type/len/value	optional	Remote ATN Router DTE address(es) now available

Notes:

1. The length field defines the length of the entire message, including the message identifier field

2. The value of the lifetime field is determined by the subnetwork processor. This value should be set to the expected time (in seconds) that connectivity over the mobile subnetwork is expected. A typical value would be on the order of 600 - 1200 seconds (10 - 20 minutes). Note that if air/ground connectivity is still possible shortly before expiration of the lifetime, the SP should re-issue the routing initiation event.

3. The SNPA field contains the subnetwork address of the remote Router. For example, the routing initiation event delivered to the aircraft Router contains the SNPA of the ground Router(s). The actual SNPA may have a different format or length for each subnetwork (for an 8208 subnetwork, the SNPA is the equivalent to the DTE address). The three subfields, type, length, and value are set as follows:

   a) a one-octet type field is set to ’1’, indicating the field as type "SNPA"

   b) a one-octet length is set to the length of the remote Router SNPA address

4. the variable-length value contains the actual DTE address of the remote Router

5. Multiple SNPA fields may be included within a single routing initiation event to report the reachability of several Routers simultaneously .

6. The VER field should be set to ’1’.

7. The value of the type field identifying the following data to be of type "SNPA" should be set to ’1’

Table 1 Join Event Format

However, all each Router knows at this point is the DTE Address of the other Router. In order to avoid the maintenance problem inherent in managing lookup tables that would enable a correspondence to be made between a DTE Address and a NET, a dynamic procedure has been specified by the ATN SARPs.

An ISO 9542 IS Hello (ISH) PDU is used for this purpose. This is sent either as data, once the connection has been established, or as part of the Call Request/Call Confirm dialogue when "Fast Select" is supported by the air-ground subnetwork. Both Airborne and Ground Routers generate an ISH PDU that reports their NET to the other Router. On receipt of an ISH PDU, each Router updates its FIB with a route to the remote Router, using the NET supplied by the ISH PDU and associating this NET with the subnetwork connection over which the ISH was received, as the forwarding path.

Note: this procedure is also used to negotiate the interim procedures used when IDRP is not supported by the Airborne Router.

2.9.3.5 Route Initiation in IDRP

Route Initiation in IDRP in the air-ground case is then almost identical to the ground-ground case, except that the SARPs require that one Router is in the passive mode and the other in the active mode. This is because the efficiency improvement gained by this approach is worthwhile in the air-ground environment, and the active and passive roles can be unambiguously identified when ICAO air-ground data networks are used.

The SARPs specify that for air-initiated air-ground subnetworks (i.e. AMSS and VDL), that the Ground Router takes on the active role and the Airborne Router takes on the passive role. For ground-initiated air-ground subnetworks (i.e. Mode S), the SARPs specify that the Airborne Router takes on the active role and that the Ground Router takes on the passive role. This approach will permit the exchange of route initiation data to take place in the shortest timeframe.

The Adjacent BIS MO, if it does not already exist, must be created in response to a notification that an ISH PDU has been received over a new subnetwork connection. It is necessary to create this MO in response to receipt of the ISH PDU, because it is not realistic to pre-configure an Adjacent BIS MO for every aircraft or Ground Router that could be connected to.

An IDRP "Start Event" is then invoked by the IS-SME, provided that a BIS-BIS connection does not already exists with the remote system. If a BIS-BIS connection does already exist then, as in the ground-ground case, and for the same reasons, the IS-SME must cause the IDRP Decision Process to be re-run.

2.9.4 Air-Ground Route Initiation without IDRP

Due to avionics limitations, the ATN SARPs permit, as an interim measure, the existence of ATN Airborne Routers which do not support IDRP. Modified Route Initiation procedures are specified to identify such Airborne Routers and thence to infer the routes that would have been distributed had IDRP been implemented.

Note 1: The identification of routes by inference is only possible because aircraft are required by the ATN SARPs to be End Routing Domains. That is they do not relay data between ground stations or to other aircraft, and hence only provide routes to their local Routing Domain.

Note 2: The consequence of this procedure is that aircraft cannot be dynamically informed about ground route availability. Therefore, until this interim measure has been withdrawn, the ground ATN environment must be constructed to ensure a higher level of availability than would have been necessary had dynamic information been available to all aircraft. This

is because, when aircraft make assumptions about ground route availability, those ground routes must exist within the margins of tolerance necessary for air safety.

2.9.4.1 Summary of Procedures

The procedures for Air-Ground Route Initiation without IDRP are illustrated in Figure 2-18, and summarised below. They are discussed in greater depth in the following sections. The figure illustrates the case where Air-Ground Routing is ground-initiated. The Route Initiation Procedures are:

1) When an aircraft attaches to an air-ground subnetwork, a Join Event is generated, potentially to both Airborne and Ground Routers. If received by System “B” (the Airborne Router), the Join Event is ignored. System “B is ready to receive incoming calls as soon as it attaches to the Mobile Subnetwork.

2) System “A” (the Ground Router) acts on a Join Event by initiating the establishment of a virtual circuit to the address given by the Join Event, provided such a connection is permitted by local policy, or

3) if polling, System “A” issues a Call Request to the next address on its poll list.

4) When an incoming call is received by System “B”, it accepts the call if permitted to do so by local policy, and generates and sends an ISH PDU to System “A” over the newly established virtual circuit. This ISH PDU includes the NET of the System “B” Network Entity, with the NSEL set to the conventional value of hexadecimal **FE**.

5) When System “A” receives a Call Accept, it too generates an ISH PDU, and sends it to System “B” over the newly established virtual circuit. This ISH PDU includes the NET of the System “A” Network Entity.

6) On receipt of the ISH PDU, both systems update their local FIB to include the routing information received on the PDU, and

7) System “A” generates the derived routes using the NET of System “B”, inserts them into the IDRP RIB, and invokes the IDRP Decision Process.

8) System “B”, generates the derived routes from its local “look up” table and inserts them into its local FIB. If for any derived route, an alternative route exists via a different Ground Router to the same destination then only that with the highest degree of preference as indicated by the look up table is inserted in the FIB.

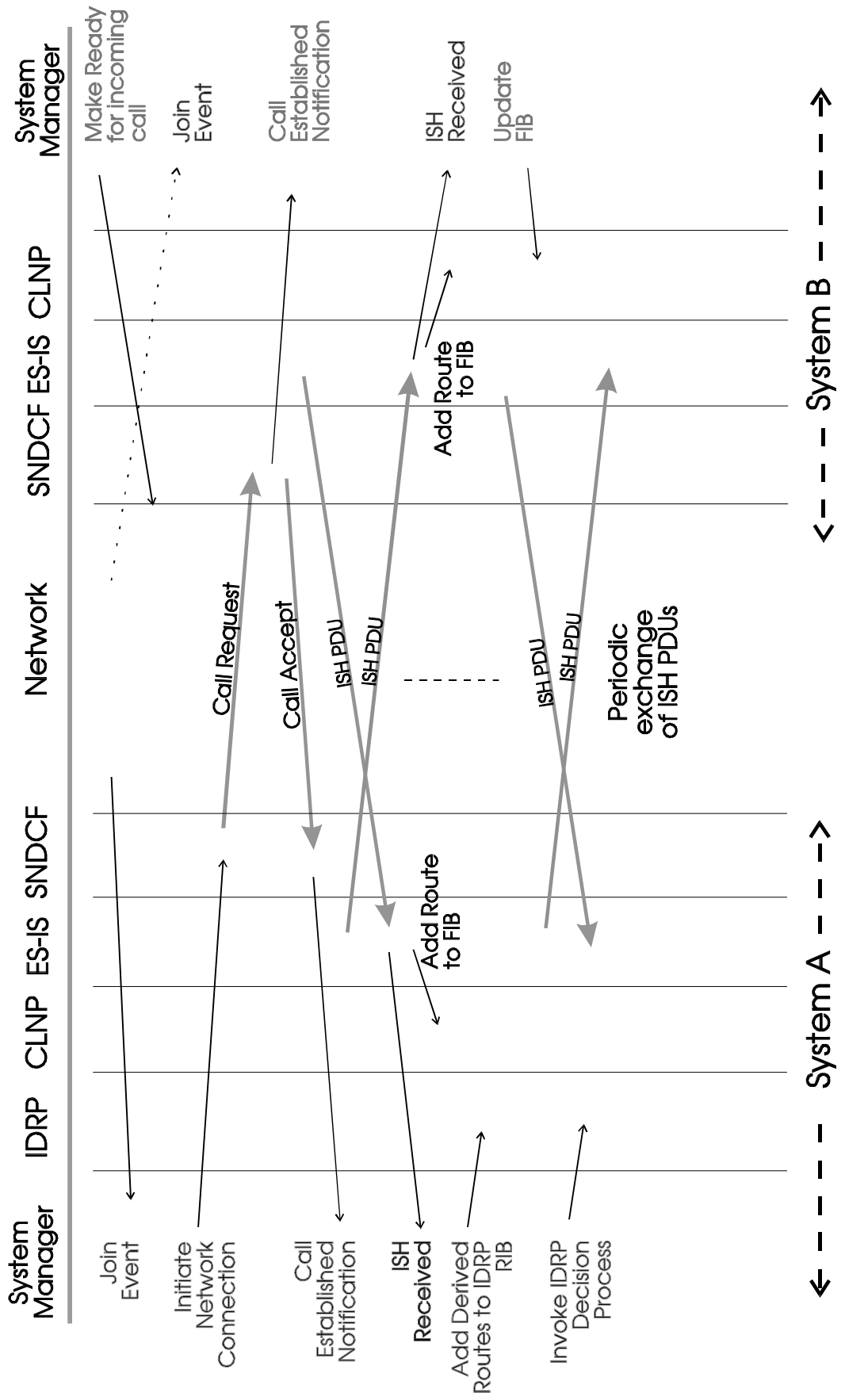

Figure 2-18 Air-Ground Route Initiation without IDRP

2.9.4.2 Initial Route Initiation

There is no difference in the initial Route Initiation procedures when IDRP is not used over the air-ground data link.

2.9.4.3 Route Initiation in CLNP

The ATN SARPs require that the NET of an ATN Router's Network Entity has a Network Selector (NSEL) of zero. This is in accordance with ISO 10589. The SARPs further specify that Airborne Router's that do not support IDRP over the air-ground data link, have an alias NET with an NSEL value of hexadecimal '**FE**', and that this NET is used in the ISH PDU passed over the air-ground data link.

Note: that support of an NET with an NSEL of zero is necessary in such Airborne Routers when, for example, they also support ISO 10589 within the aircraft.

Receipt of an ISH PDU with an NET that has an NSEL of hexadecimal '**FE**' indicates to the receiving Ground Router that the sending Airborne Router does not support IDRP. The IS-SME must then apply the special procedures discussed below.

2.9.4.4 IS-SME Procedures without the use of IDRP

2.9.4.4.1 In the Ground Router

When the IS-SME receives a notification that an ISH PDU has been received from an Airborne Router that does not support IDRP, it must derive the routes that are available via the Airborne Router and add these routes to the local IDRP Routing Information Base (RIB). IDRP may then update the FIB and distribute these routes in the normal fashion.

The derivation of routes is possible because the aircraft is known to comprise an End Routing Domain, and from knowledge of the ATN Addressing Plan it is possible to determine an NSAP Address Prefix common to all systems in the aircraft from the NET of the Airborne Router. Further, from *a priori* knowledge of ITU restrictions that may apply to each air-ground data network and the Quality of Service offered by each such data network, the distinguishing path attributes appropriate to the routes may also be determined.

The number of routes derived by the Ground Router in respect of a specific Airborne Router will be determined by the number of different Application Security Types permitted by ITU restrictions to pass over the air-ground subnetwork multiplied by the number of QoS metrics appropriate to the network. Each such route will have as its Network Layer Reachability Information (NLRI), an NSAP Address Prefix constructed from the first eleven octets of the received NET. That is because the ATN Addressing Plan results in a common eleven octet prefix for all NSAP Addresses and NETs in one aircraft's Routing Domain, which may therefore be determined by inspection of any NSAP Address or NET from any system in that Routing Domain.

The IS-SME must then add those routes to the IDRP RIB and run the IDRP Decision Process, which then disseminates those routes and adds them to the FIB in line with the existing Routing Policy, and provided that they are a preferred route to the Airborne Router.

The actual strategy for doing this is implementation specific. However, a likely strategy is for the IDRP implementation to allocate special "adj-RIB-ins" (one per RIB-ATT) for holding routes received by mechanisms outside of the scope of IDRP. The Decision Process will then consider such routes along with those in "normal" adj-RIB-ins. The only distinguishing aspect of such routes is that they will include the "EXT_INFO" path attribute. This is a flag that enables Routing Policy to differentiate between routes that have been advertised by IDRP throughout and those which have been learnt through some other mechanism, perhaps less reliable. As in the general case, the Decision Process must be able to

associate this special Adj-RIB-in with the connections to the Airborne Router, and the QoS provided by these connections . This is so that when computing the degree of preference for each such route, or when copying them to the loc-RIB, the Decision Process can update their QoS to reflect the current communications paths that exist to the Airborne Router.

If additional subnetwork connections are opened up (or lost) to an Airborne Router then, instead of generating the derived routes, as before, the IS-SME must cause the IDRP Decision Process to be re-run.

Finally, in this interim role, the IS-SME must also determine when the assumed routes are no longer valid. This event occurs when either the air-ground subnetwork connection is lost or when the periodic exchange of ISH PDUs ceases. On the occurrence of either such event, the routes generated above must be withdrawn.

Note: that in contrast with the use of IDRP over an air-ground data link, when the ATN SARPs recommend that for reasons of efficient bandwidth utilisation, ISH PDUs are not periodically transmitted, in this case they must be periodically transmitted in order to maintain the "liveness" of the routes.

2.9.4.4.2 In the Airborne Router

The IS-SME procedures are in this case, similar to the ground case, except that:

a) the NLRI of the generated routes cannot be simply derived from the Ground Router's NET. This is because the Ground Router is typically part of a Transit Routing Domain, and the destinations of the onward routes that it offers will not have any known relationship to its NET.

b) The generated routes must be directly added to the FIB as IDRP is not present to do this on behalf of the IS-SME, or

c) if ISO 10589 is implemented, the generated Routes are used to generate Reachable Address MOs and the ISO 10589 entity is used to update the FIB.

In order to determine the NSAP Address Prefixes for the generated routes, lookup tables will have to be provided so that given the NET of a Ground Router, the Airborne Router can identify the NSAP Address Prefixes for destinations reachable via that Ground Router. Furthermore, such look up tables will have to provide:

i) restrictions on Security Types for such destinations that are additional to ITU restrictions imposed by the Air-Ground Subnetwork;

ii) The Capacity, Hop Count and QoS information for such destinations in a manner sufficient to enable alternative routes to be discriminated between. i.e. an indication of relative preference for each supported metric.

Operationally, there will be a need to ensure that such tables are up-to-date with information appropriate to the Flight Region(s) through which the aircraft will fly, prior to each flight. The actual implementation of this procedure is dependent on the systems involved.

The IS-SME will have to keep dynamic information on which routes are available via each Ground Router with which it is in contact. This information is derived from the look up table and *a priori* information for each Air-Ground Subnetwork supported. When multiple subnetwork connections exists to a given Ground Router then the routing information will be determined taking into account the characteristics of each such subnetwork.

When routes to the same destination are available via different Ground Routers, then the IS-SME will have to choose between them based on the degree of preference given by the look up tables.

The IS-SME is also responsible for maintaining the FIB with an up-to-date set of available preferred routes determined as above. It must add such routes to the FIB when they become available, and remove them when the reverse is true, Alternatively, if ISO 10589 is implemented, then the IS-SME may make such routes available to 10589 by creating a Reachable Address MO for each such route, and removing the MO when the route ceases to be available. The ISO 10589 implementation may be relied upon to maintain the FIB with this routing information.

2.10 Quality of Service Maintenance

In response to User Requirements from Air Traffic Services Communications (ATSC) users, the ATN provides a classification mechanism for ATN Routes. The classifications reflect the Quality of Service available over the route taking into account availability, capacity and transit delay. Class “A” is the best while Class “H” is the worst.

These classifications do not reflect dynamic conditions but are assigned statically by network managers and reflect the result of capacity planning work.

In the CLNP header of each user data packet, the sender may then identify the minimum route class that the packet should follow; this reflects the application requirements. The ATN Routers will then choose the lowest classification route available that meets the user requirement and, if one cannot be found, then the route with the highest classification albeit lower than that required by the application.

2.11 Priority

2.12 Security

As an operational network, ATN Security has to be taken seriously. There are three aspects to ATN Security:

1. Maintaining Regulatory and National Restrictions on the use Air/Ground Data links.

2. Maintaining Restrictive Routing Policy Requirements

3. Protecting the ATN Against mis-use.

The first two aspects are dealt with procedurally. Information is included with each use on the type of Air/Ground data link over which it is available and any restrictions that apply to each such data link. When packets are then forwarded a route, if any, is chosen that is permissible for the packet’s application data to pass over and which is in line with any routing controls that the sender has specified in the packet header.

The final aspect of ATN Security requires specific security mechanisms to be effective. Security Mechanisms in this area are currently *tba*.

The IDRP protocol supports a range of authentication mechanisms (referred to as authentication type 1, 2 and 3). Authentication type 1 provides an unencrypted checksum, and so is not secure, although it gives protection against arbitrary errors. Type 2 provides protection against masquerade and modification by use of a checksum which is encrypted using a mutually agreed encryption algorithm. Authentication type 3 uses a “validation field”

in each routing protocol exchange to carry a Message Authentication Check (MAC), generated from an agreed password.

3. Guidance for ATN Administrators

3.1 Areas of Responsibility

3.2 Interconnection Strategies

3.3 Address Allocation Strategies

3.4 Systems Management Strategies

3.5 Capacity Planning

3.6 Route Planning

3.7 Intra-Administrative Domain Communications

4. Guidance for ATN System Implementors

4.1 Transport Protocol Considerations

4.1.1 General

The OSI Transport Layer supports the end-to-end exchange of data between end systems, and serves as an interface between the application and upper layers, dealing with the exchange of information, and the lower layers, which provide the necessary transmission and routing capabilities (see Figure 8.1). The applications and OSI upper layers that directly use transport layer services for the exchange of data are known as Transport Service users (TS-users).

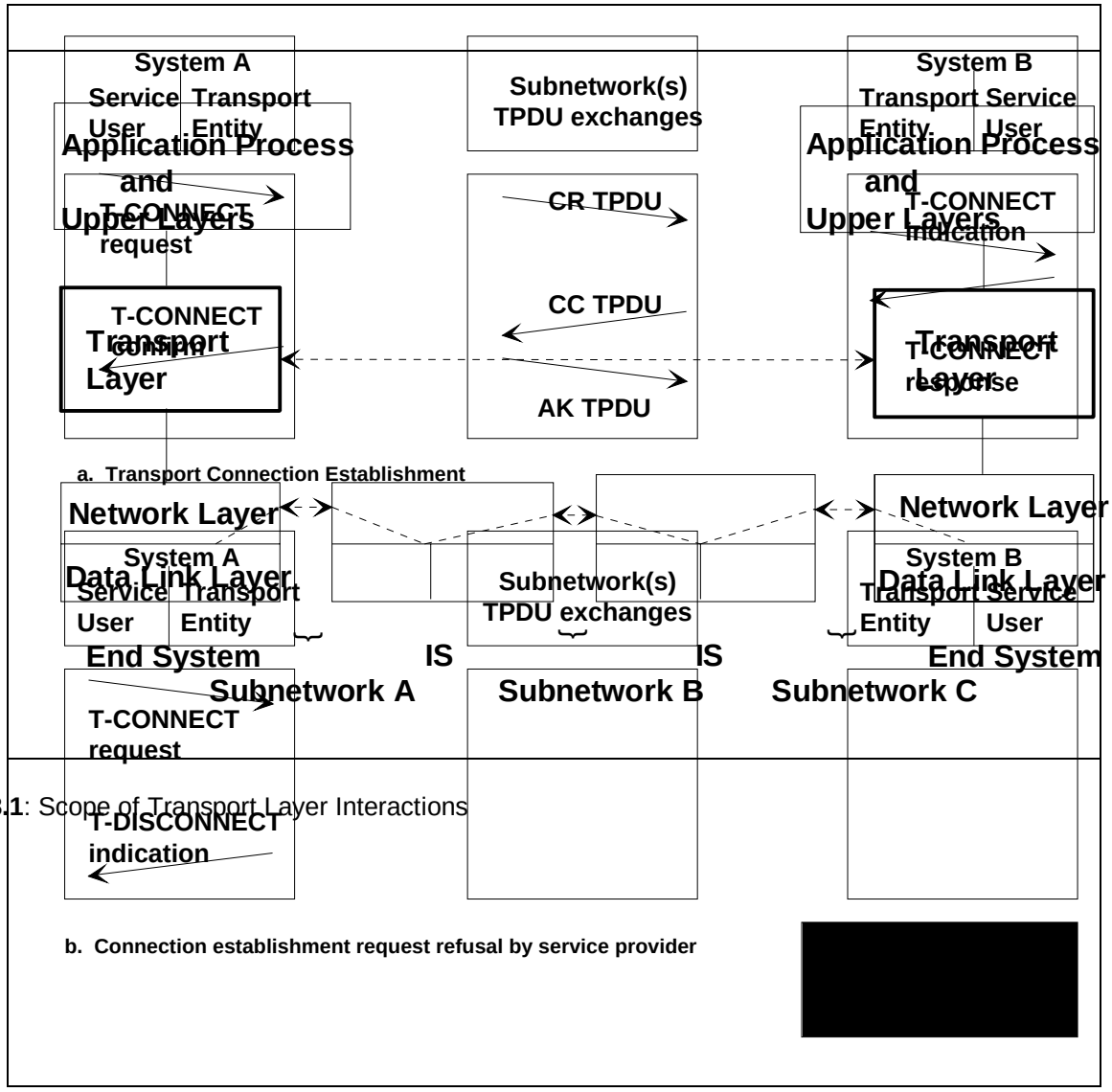

Figure 8.1: Scope of Transport Layer Interactions

Figure 8.2: TPDU Exchanges for Connection Establishment and Connection Refusal by Transport Provider

TS-users receive a service which conceals the details in which reliable and cost effective transfer of data is achieved. This must be done by the transport layer in an economical manner which is independent of the implementation specifics of the various subnetworks used, and of end system hardware and software implementation details.

The Transport Layer may consist of one or several transport entities. There are two transport protocol entity types in the ATN: the COTP and the CLTP. A given ES may implement one or both of these, depending upon the requirements of the applications it contains. For example, if all of the applications in a given ES require the COTP, then that ES does not need to implement the CLTP.

4.1.1.1 Transport Addresses

A transport address, or TSAP address, identifies a specific TS-user.

A TSAP address comprises two elements, a NSAP address and a TSAP-selector. The NSAP address provides the address of the transport protocol entity for a particular ES, such as the connection mode transport layer. The TSAP Selector then identifies one of the users of the transport protocol entity

Note.— Refer to Section 7.6 for more information on transport addressing.

4.1.1.2 Network Service Assumptions

The ATN Transport Layer operates using the connectionless network service provided by the ATN network layer. All TPDUs are transmitted and received as NSDUs using the N-UNITDATA service of the network layer. Each NSDU is considered independent of the others, and may arrive in a different order than was sent, in duplicate, or not at all. Although it is possible for NSDUs to be lost, the ATN is expected to have a low loss rate, based on the intrinsic reliability of the subnetworks supporting communications.

4.1.1.3 Use of Transport Layer Services

4.1.1.3.1 Selection of Transport Service Mode

The selection of the transport service to be used by an application is influenced by the communications characteristics and the quality of service requirements of that application. Two basic modes of service can be requested: the COTS, now called the connection mode transport service or the CLTS, now called the connectionless mode transport service. Either the COTS or the CLTS can be employed to support the exchange of transport service data units (TSDUs) between two TS-users.

4.1.1.3.2 Service Selection Guidance

Connection Mode is appropriate when users need to maintain an association, either because they need to transfer a lengthy data stream, or because the applications need to maintain a close binding (e.g. as a test of liveness). COTS is appropriate for applications that place a higher importance on data integrity than on time of delivery. The connection mode transport service is supported by the ISO 8073 protocol. The characteristics of the service provided by the connection mode protocol include the following:

- TS-users negotiate the establishment of a transport connection; this connection enables reliable data transfer between the two. An initial delay is associated with the establishment of a transport connection. During this phase, data cannot be exchanged.

- Maintenance of a transport connection will generally incur some additional costs associated with the transfer of TPDUs not associated with user data, such as acknowledgements. Acknowledgements are utilized for both data acknowledgements and keep-alive indicators.

- The order of submission of TSDUs is preserved on delivery.

- The transport protocol can employ facilities to detect and recover from end-to-end transmission errors within a TSDU.

- The protocol is capable of segmenting TSDUs, allowing TSDU sizes larger than the recommended maximum allowable NSDU size of 1024 octets. This has the potential for improving network performance, because network level (that is, the connectionless network protocol) segmentation is less efficient than transport segmentation.

- The protocol has the capability to control the flow of TSDUs. This allows the receiver of information to adjust the rate of incoming TSDUs to meet local processing capabilities. In addition, this flow control can be exercised by a transport entity to react to varying network congestion problems, applying and relieving constraints to match resource limitations.

  Note.— Since no complete congestion management strategy could be fully analysed within the time limit available for the definition of these SARPs, no such strategy is required in the CNS/ATM-1 internet.

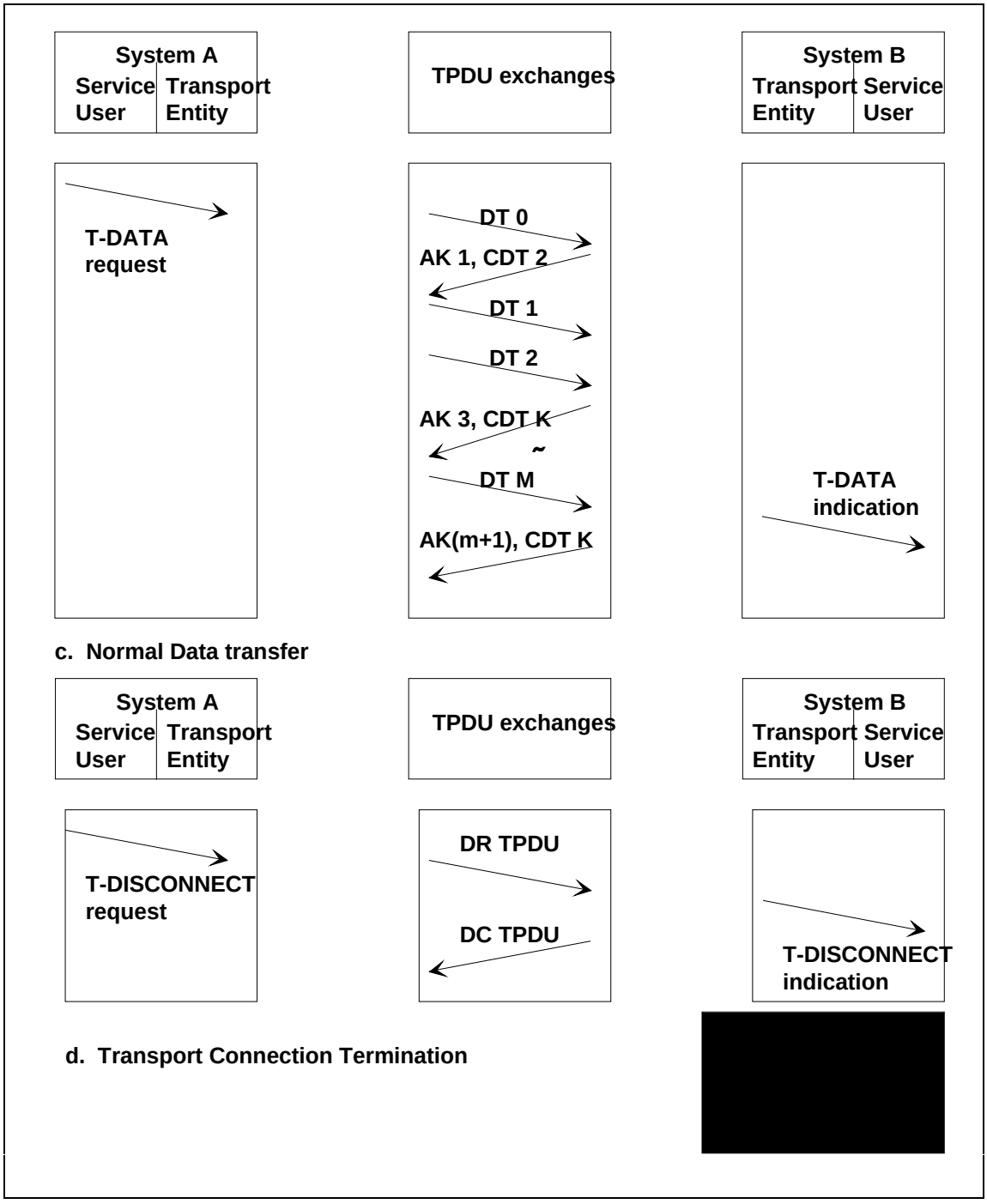

Figure 8.3: TPDU Exchanges for Data Transfer and Connection Termination

- Operation of the COTP requires processing resources to maintain shared state and to monitor connection status.

  The CLTS is valuable when there is a requirement for time-critical data transfer, i.e. it is more desirable to discard data rather than apply flow control or retransmission techniques. The connectionless mode transport service is supported using the ISO 8602 protocol. The characteristics of the service provided by the CLTP include the following:

- No negotiation takes place before a TSDU is transmitted from one user to another. This mode does not have the delay associated with establishing a transport connection before data can be exchanged.

- There are no TPDUs transmitted other than those carrying user data.
- Each TSDU is transmitted independently from all others; TSDU delivery and TSDU delivery sequence are not guaranteed. There is no transport-layer recovery on detected errors.
- The transport protocol can employ facilities to detect end-to-end transmission errors within a TSDU. TSDUs containing detected errors are discarded.
- TSDU sizes are limited to the maximum NSDU size on each end system; no segmentation is performed by the connectionless mode transport protocol.
- Because there is no negotiated relationship between TS-users, the protocol does not have the capability to control the flow of TSDUs.
- The processing requirements for the connectionless transport protocol are minimal, since the transport protocol does not perform any TSDU sequencing or TSDU guarantee functions.

4.1.2 The Connection Mode Transport Service

4.1.2.1 Overview

The COTS has three phases of operation: connection establishment, data transfer, and connection release. It is able to operate over a CLNS, such as provided by the ATN network service. The Transport Protocol reacts to network status information and hides any problems from the TS-user.

A pair of users of the COTS can transfer information once a transport connection is established between them. The information unit transferred between TS-users is the TSDU. For the transfer of TSDUs, the transport layer provides a known set of characteristics, as noted below.

TSDU Sequencing. The ATN COTS guarantees that TSDUs will be delivered to the destination TS-user in the order they have been submitted by the source TS-user to the TS-provider. The only exception is expedited data which, being subject to a different flow control scheme, may overtake normal data.

TSDU Delivery Support. The transport layer supports the delivery of a submitted TSDU to the destination TS-user. The only case where data may be lost is if the connection release phase has been entered by the local or remote TS-user and/or provider.

End-to-End Detection and Recovery of Error. Class 4 of the connection mode transport protocol provides mechanisms that support the detection and recovery of errors such as TPDU loss, duplication, or corruption. The error detection and recovery is done transparently to the user.

4.1.2.1.1 Transport Protocol Classes

The ATN operates the transport protocol class 4, as this is the only class allowed over a connectionless network.

4.1.2.1.2 Transport Connection Management

Connection management involves connection establishment, data transfer, and connection release. Although some type of connection management is handled by almost every layer, it is especially complex at the transport layer due to the unpredictability of network errors or delay. There are two basic mechanisms used for transport connection management: the handshake-based mechanism and the timer-based mechanism. Handshake-based mechanisms use explicit exchanges in response to a given packet initiating an action, such

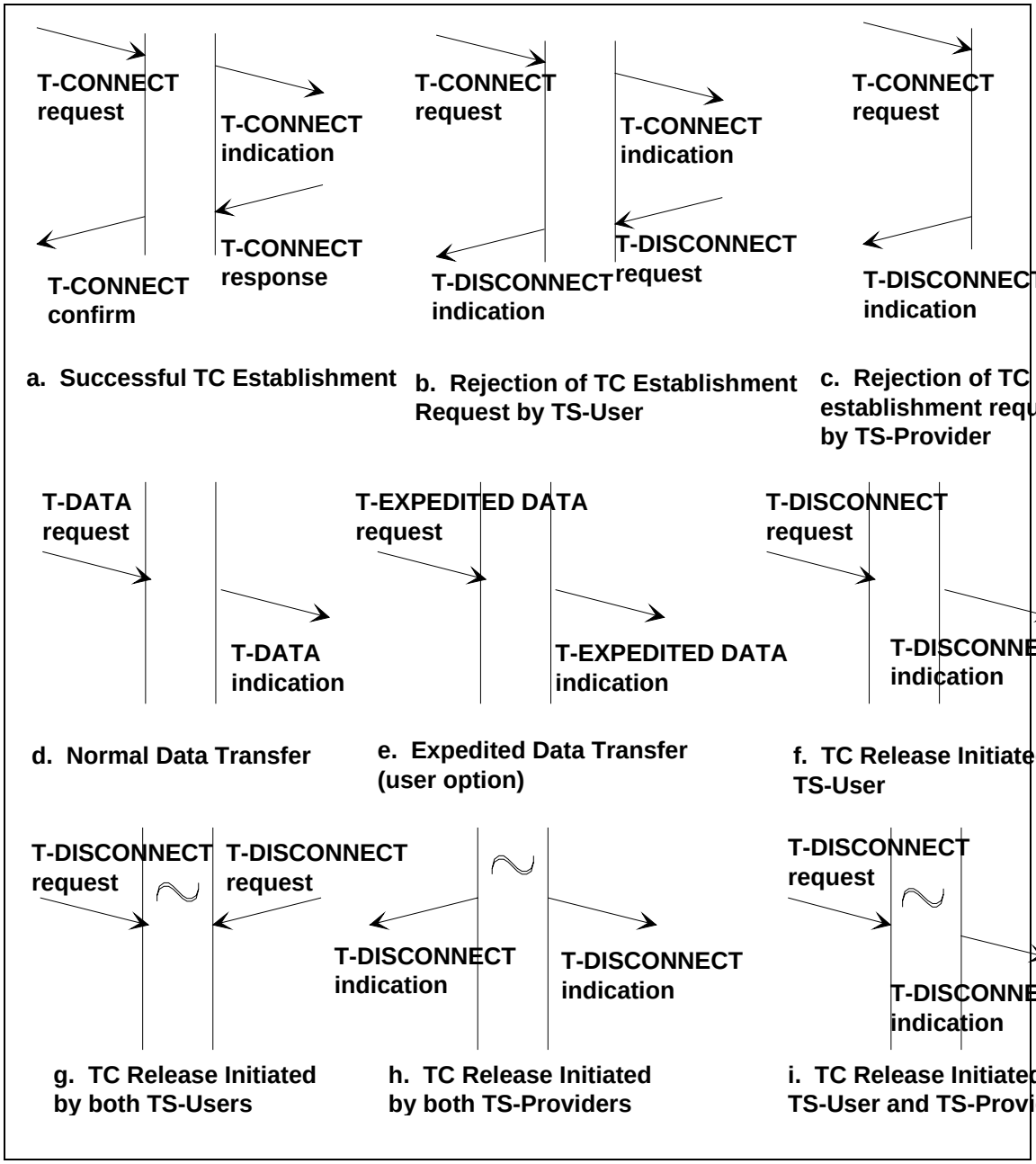

Figure 8.4: Transport Service Time Sequence Diagrams

as is done in connection establishment. Timer-based mechanisms are based on the sender and receiver keeping track of the system state long enough to ensure that all PDUs from closed connections have left the system. Several of these exchanges are illustrated in Figure 8.2 and Figure 8.3.

The handshake- and timer-based mechanisms are combined to ensure that connection identifiers are unique during the maximum time packets may remain in the system.

4.1.2.1.2.1 Connection Establishment

The OSI Transport layer protocol uses a three-way handshake mechanism in combination with a timer-based mechanism to ensure connection establishment in class 4. Figure 8.2 (a) illustrates a typical transport connection establishment procedure. The service user, either the session layer or a specific application at system A, passes a T-CONNECT

request primitive to its service provider (the transport layer) with appropriate parameters for setting up the connection. The transport layer entity of A then generates a connection request TPDU containing the parameter values and sends it to its peer transport layer entity at B. The transport entity at B generates a T-CONNECT indication primitive and passes it to its user.

If the user B accepts the connection establishment request, it generates a T-CONNECT response. The transport entity at B then transmits a connection confirm TPDU to the transport entity at A. Finally the transport entity at A informs its user that its connection establishment request has been accepted by invoking a T-CONNECT confirm primitive.

The transport entity at A also generates an acknowledgement (AK), or a data (DT), or expedited data (ED) TPDU (if there are data to be transferred), and sends it back to the transport entity at B. The connection is considered established only after the transport entity at B has received this acknowledgement or data TPDU.

If the connection request is initially refused by the TS-provider at A, a T-DISCONNECT indication is sent back to the TS-user at A as illustrated in Figure 8.2 (b).

4.1.2.1.2.2 Data Transfer

TP4 implements a sliding window flow control mechanism enabling AKs to be returned while data are still being sent. An AK is returned when the acknowledgment timer set or reset after receipt of data expires. The acknowledgment timer mechanism enables multiple TPDUs to be acknowledged with the same AK TPDU. An example of normal data transfer is shown in Figure 8.3 (c), which illustrates the transmission of a single transport service data unit via multiple TPDUs. After the establishment of the transport connection, the initial DT TPDU number is 0 (DT 0). An initial credit of 1 is assumed and transport entity A waits for an acknowledgement with more credit. Transport entity B returns AK 1, with a credit (CDT) of 2, allowing the transmission of two more TPDUs. When the EOT (end of TSDU) bit is set to 1 in the final DT TPDU, the sequence ends and the whole TSDU is delivered to user B. At the expiration of the acknowledgment timer, an AK is returned. This AK acknowledges up through the final TPDU.

4.1.2.1.2.3 Connection Termination

Connection release can be performed at the initiative of either TS-user or TS-provider at any point in the lifetime of the transport connection. This is an abrupt release because the transport protocol does not have functions that support prior negotiation of termination and so data may be lost. Typical scenarios of connection release are demonstrated in Figure 8.4 (f) through (i). In the first scenario (f), User A sends a disconnect request (DR), the Transport entity at B sends a T-DISCONNECT indication to user B and the connection ends. A disconnect confirm (DC) TPDU is sent back from system B to system A. In the second case (g), the two users send a DR at the same time. In the third case (h), the transport layer itself (either the entity at B or at A) generates the DR. In the fourth case (i), user A sends a DR after the transport layer has initiated termination of the connection.

4.1.2.1.3 ATN Connection Mode Transport Service Model

The operation of a Transport Connection (TC) is modelled as a pair of queues linking the two TSAPs to which the communicating TS-users are attached. For each potential TC, a pair of queues is considered to be available: one queue for the information flow from user A to user B, and one queue for the information flow from user B to user A.

4.1.2.2 Connection Mode Transport Service Primitives

There are ten connection mode transport service primitives. In the connection establishment phase, the TS-user issues the T-CONNECT Request and the T-CONNECT Response; the TS-provider issues the T-CONNECT Indication and the T-CONNECT Confirmation. In the data transfer phase, the TS-user issues the T-DATA Request and the T-EXPEDITED DATA Request; the TS-provider issues the T-DATA Indication and the T-EXPEDITED DATA Indication. In the disconnect phase, the TS-user issues the T-DISCONNECT request; the TS-provider issues the T-DISCONNECT indication.

A TS primitive issued by one TS-user will, in general, result in receipt of an indication by the other TS-user. Figure 8.4 gives a summary of TS-primitive time-sequence diagrams for some typical scenarios.

Each of the Connection Mode TS primitives has one or more associated parameters. They will be discussed in detail in subsequent sections.

Note.— In Figure 8.4 the flow of time is represented by the downward direction in individual figures. The sequential relation between two points of interaction is shown by a horizontal line which is discontinuous between the two vertical lines representing the flow of time (e.g. the T-CONNECT request primitive in (a) invoked by a TS-user at moment t1, is necessarily followed by a T-CONNECT indication primitive invoked by the remote TS-provider at moment t2). The absence of relationship is indicated by using a tilde (~).

Figure 8.4 is derived from a state transition diagram which defines the allowed sequences of TS primitives at a TC endpoint. This state transition diagram pertains to the Transport Protocol Machine.

4.1.2.2.1 Connection Establishment Primitives

4.1.2.2.1.1 Connection Establishment Overview

To initiate communication with a peer, a TS-user invokes the T-CONNECT request primitive (see Figure 8.4). Upon arrival at the destination TSAP, a T-CONNECT indication is delivered to the destination ATN TS-user. The peer TS-user accepts the connection request by issuing a T-CONNECT response primitive. Finally, the calling TS-user receives a T-CONNECT confirm primitive and the connection is established. Simultaneous T-CONNECT requests typically result in a corresponding number of TCs. The parameters associated with the connection establishment primitives are listed in Table 8-1.

As part of the TC establishment phase, TS-users can negotiate the QOS parameters to be associated with a transport connection. Use of expedited data is also negotiated. QOS parameters are used to describe the desired characteristics of the data flow over the TC, rather than to provide mechanisms for the transport protocol to enforce specific characteristics. The use or non-use of expedited data is negotiated between TS-users, and will be selected based on TS-user requirements. Furthermore, some negotiations take place between TS-providers which are transparent to the TS-users. All the choices made during the connection establishment phase remain valid for the whole TC lifetime. The TC establishment procedure may fail due to:

Table 8-1 TC Establishment Primitives and Parameters

Parameters	**Transport Service Primitive**			
	T-CONNECT Request	**T-CONNECT Indication**	**T-CONNECT Response**	**T-CONNECT Confirm**
Called Address	M	M(=)		
Calling Address	M	M(=)		
Responding Address			M	M(=)
Expedited Data Option	M	M(=)	M	M(=)
Quality of Service	M	M	M	M(=)
TS User Data	M	M(=)	M	M(=)
Security	O	O(=)	O	O(=)

M The parameter is mandatory
(=) The value of the parameter in the T-CONNECT Indication/Confirm is identical to the value of the corresponding parameter in the T-CONNECT Request/Response TS primitive
O Use of this parameter is a TS-user option

- timeout procedures, such as when a TS-user does not respond to a connection request

- rejection by the TS-provider of an attempt to establish a TC (part c of Figure 8.4), for reasons such as invalid or unknown called TSAP address, lack of local or remote resources of the TS-provider etc., or,

- unwillingness of the called TS-user to accept the TC establishment request (part b of Figure 8.4).

The TC establishment may also fail due to either of the TS-users releasing the TC before the T-CONNECT confirm has been delivered to the calling TS-user.

4.1.2.2.1.2 Connection Request

A calling TS-user, when invoking a T-CONNECT request primitive, specifies the following parameters :

Called Transport Address: The called transport address contains the addressing information necessary to reach the desired destination TS-user. An ATN called transport address comprises an ATN NSAP address and a TSAP Selector (also called TSAP-ID in ISO 8073). See chapter 7 for further details on ATN transport layer addressing.

Calling Transport Address: The calling transport address contains the addressing information that identifies the TS-user invoking the T-CONNECT request. An ATN calling transport address comprises an ATN NSAP address and a TSAP selector.

Expedited data option: By means of this parameter the communicating TS-users negotiate the use or non-use of the expedited data service for the TC in question. The calling TS-user initially specifies the use or non-use of expedited data. If non-use is initially proposed, the called TS-user cannot further negotiate its use. If its use is initially proposed, the called TS-user can either confirm use or can select non-use of the expedited data option.

Requested Quality of service: QOS parameters are used to describe the desired characteristics of the data flow over the transport connection. The parameters which may be negotiated are transit delay, residual error rate, and priority.

TS-user-data: A user can specify data from 1 to 32 octets in the connection establishment request. These data can be used by the TS-user in a manner agreed with the peer TS-user. For example, the information could be used to communicate authentication and access control information. It should be noted that the delivery of TS-user-data is not guaranteed. TS-user-data are not recommended for direct use by applications.

Security: The security parameter may be used by the service user to indicate the value of the security label. The syntax and semantics of the ATN Security Label are specified in 5.9.1.

Note 1.— Negotiation of options only proceeds in a "mandatory" direction. That is, the called TS-user can always negotiate to the mandatory aspect of any option.

Note 2.— In practice, not all of the parameters in a connection request must be explicitly specified, even though they exist in the service interface. For example, the invoking TS-user may only be required to specify the called transport address if the transport entity knows the calling address a priori*. Other parameters, if not specified, may take on default values. For example, most implementations today do not require explicit specification of QOS values. If not specified, one of two things may occur: QOS parameters may not be conveyed in the CR TPDU or the TE may select a standard set of parameters.*

4.1.2.2.1.3 Connection Indication

A T-CONNECT request issued by a TS-user results in a corresponding T-CONNECT indication to the destination ATN TS-user. The TS-provider, when issuing the T-CONNECT indication, specifies the following parameters:

Calling and called address

Expedited data option

TS-user-data

Indicated QOS

The values of the first three parameters are delivered unchanged by the TS-provider to the destination TS-user. The values of the indicated QOS parameters can be equal to or poorer than the requested QOS parameters selected by the calling user in the T-CONNECT request primitive. The value of a QOS parameter can be downgraded by either the transport entity serving the calling TS-user or the transport entity serving the called TS-user. This will happen if the transport entity has additional provisions implemented which monitor the ability to provide the requested QOS.

4.1.2.2.1.4 Connection Response

To accept the TC establishment, the called TS-user issues a T-CONNECT response primitive (otherwise, it invokes a T-DISCONNECT primitive and the connection is not established; see 8.2.2.4). The associated parameters and their corresponding values are the same as in the T-CONNECT request.

4.1.2.2.1.5 Connection Confirm

A T-CONNECT response primitive at one TC endpoint starts the delivery of a T-CONNECT confirm primitive at the other TC endpoint. This primitive has exactly the same associated parameters as those of the T-CONNECT response primitive. The values of these parameters are also equal, that is, the TS-provider delivers these values unchanged to the calling TS-user. Once this primitive has been received by the calling TS-user, the connection is considered to be established.

4.1.2.2.2 Data Transfer Primitives

The transport service provides for bidirectional exchange of TSDUs while preserving the integrity, sequence and boundaries of TSDUs. Two kinds of transfer service are offered by the ATN COTS provider: the normal data transfer service and the expedited data transfer service. Part (d) of Figure 8.4 describes the primitive sequences in a successful transfer of normal data.

4.1.2.2.2.1 Data Request

A TS-user requests the transfer of a TSDU by invoking a T-DATA request primitive. This primitive has only one associated parameter: the TS-user-data parameter (i.e. the TSDU to be transmitted). A TSDU consists of an integral number of octets greater than zero; the length of a submitted TSDU is limited by implementation constraints only.

4.1.2.2.2.2 Data Indication

Upon arrival of the TSDU at the other TC endpoint, the TS-provider invokes a T-DATA indication primitive to the destination TS-user. The TS-user-data parameter of the T-DATA request primitive is delivered unchanged by the TS-provider to the destination TS-user.

4.1.2.2.3 Expedited Data Transfer Primitives

This service is available on a given TC only if its use has been requested by the calling TS-user and agreed to by the called TS-user during the TC establishment phase. The TS-

provider guarantees that an expedited TSDU will not be delivered after any subsequently submitted normal TSDU or expedited TSDU on the same TC. The transfer of expedited TSDUs is subject to separate flow control from that applied to the data of the normal transfer service. Part (e) of Figure 8.4 shows the sequence of primitives in a successful transfer of expedited data.

4.1.2.2.3.1 Expedited Data Request

A TS-user desiring to transmit an expedited TSDU invokes the T-EXPEDITED DATA request primitive. This primitive has only one associated parameter: the TS-user-data parameter (i.e. the TSDU to be transmitted).

An expedited TSDU consists of an integral number of octets between 1 and 16 inclusive .

4.1.2.2.3.2 Expedited Data Indication

Upon arrival at the destination, the TS-provider invokes a T-EXPEDITED DATA indication primitive which delivers the submitted TSDU (TS-user-data parameter) unchanged to the destination TS-user.

4.1.2.2.4 Connection Termination Primitives

TC release is permitted at any time. A TS-user may issue a connection termination primitive to refuse TC establishment or to release the established TC. The TS-provider never guarantees delivery of submitted data - it just guarantees order preservation - if it delivers a TSDU it guarantees to have delivered all previously submitted TSDUs. There is always an uncertainty over how much data has been lost once the release phase is entered and includes TSDUs submitted well before the release phase was entered. The degree of data loss is independent of the credit window, and depends on the length of the queue between TS-provider and TS-user. In particular, all data received after a transport entity has entered the release phase are discarded. The parameters associated with the connection termination primitives are summarized in Table 8-2.

Table 8-2 TC Release Primitives and Parameters

Parameters	**Transport Service Primitive**	
	T-DISCONNECT Request	**T-DISCONNECT Indication**
Reason		M
TS User Data	M	M(=)

M The parameter is mandatory

(=) The value of the parameter is identical to the value of the corresponding parameter in the preceding TS primitive

4.1.2.2.4.1 Disconnect Request

A TS-user releases an established TC by invoking the T-DISCONNECT request primitive. This primitive has only one optional parameter: the TS-user-data parameter. The TS-user-data parameter is an integral number of octets in length between 1 and 64 inclusive. The content of this parameter may provide additional information on the reasons for the TC release request.

4.1.2.2.4.2 Disconnect Indication

The T-DISCONNECT indication primitive has different parameters, according to the originator of this primitive. If the T-DISCONNECT indication is invoked by the TS-provider as a result of a T-DISCONNECT request invoked by a TS-user at the other TC endpoint, this primitive has the following associated parameters:

TS-user-data: This parameter is present only if it was also present in the T-DISCONNECT request primitive. These data are normally delivered unchanged by the TS-provider, except if the TS-provider initiates TC release before the T-DISCONNECT indication is delivered (see part (i) of Figure 8.4), or if TS-users initiate a T-DISCONNECT request simultaneously (see part (g) of Figure 8.4). In these cases these data may be lost.

Reason: This parameter will take the value "remote TS-user invoked".

If the T-DISCONNECT indication is invoked by the TS-provider itself, the only associated parameter is the "Reason" parameter which takes the value "TS-provider-invoked" (in this case no TS-user-data parameter is present). Examples of reasons for a TS-provider-initiated release include: lack of local or remote resources of the TS-provider, misbehavior of the TS-provider, called TS-user unknown, or called TS-user unavailable (if the release occurs during the connection establishment phase).

4.1.2.3 ATN Connection Mode Transport Layer Quality of Service

QOS parameters are used to indicate the required characteristics of the underlying communications service supporting application information exchange. The transport layer may interpret the QOS parameters which are provided by a TS-user; these parameters may then affect the interactions of the transport layer with the network layer providing service.

QOS is of special importance to the aviation community because of the wide variation in service provided by the ATN network service. For some applications, there may be requirements for minimum transit delay, or cost constraints that need to be accommodated. For these applications, users will want to have some influence over the selection of network resources. Within an ES, the way of affecting the selection of network resources is by the use of network QOS parameters. The selection of transport and the associated network QOS parameters can be done in several ways. For example:

a. the transport entity can be statically configured to use a given set of parameters;

b. the TS-user can use a separate interface to indicate the desired QOS parameters; or

c. the transport layer can dynamically select network QOS parameters based on the transport QOS parameters selected by the TS-user.

These, or other techniques, can also be combined. For an end system with only one application or a group of applications with very similar requirements, a single set of configuration parameters can be used to determine the appropriate transport and network layer QOS parameters (option a). Dynamic selection of QOS parameters (option b or c) is needed when there are two or more applications in an end system with very different or

varying requirements or usage characteristics. The dynamic selection of QOS parameters based on the user QOS requirements (option c) has the further advantage of maintaining the recommended ISO 8072 interface.

Note.— Refer also to 5.7.1 on the QOS management framework; refer to 8.2.5.1.2.4 for guidance on dynamic determination of network QOS parameters based on TS-user-specified QOS parameters.

The use of checksums for a given TC or TS-user can also be determined using one of the methods described above. Although checksum use is not explicitly indicated by a TS-user, its use can be defined either through configuration techniques or it can be inferred based on the QOS requirements of the TS-user.

Since checksums are contained in the TPDU header, implementation of checksums is a protocol performance issue.

4.1.2.3.1 Use of Transport Layer Quality of Service

QOS parameters are specified by a user to request certain characteristics; they are provided to a user to provide information about service characteristics. QOS parameters are defined, thus, as the requested transport layer QOS or the indicated transport layer QOS. A user of the COTS provides the requested transport layer QOS parameters in the invocation of the T-CONNECT request or the T-CONNECT response. A user is provided with the indicated transport layer QOS in the T-CONNECT indication or the T-CONNECT confirmation.

At the invocation of the T-CONNECT request primitive, the TS-user provides the requested transport layer QOS parameters. The role of the requested parameters is two-fold; 1, to influence the behavior of the transport layer and 2, to relay to the destination TS-user the characteristics that must be mutually accepted, or negotiated. In the first case, for example, the user QOS parameters may affect the use of checksum. Since the ATN transport layer operates over a CLNS, class 4 is always required and so the QOS interpretation by the transport layer has no effect on the class of protocol operated. These parameters are received by the transport layer but no action or effect is guaranteed. Further, based on transport layer knowledge of the expected QOS (information either known *a priori* or received from the systems management interface), the transport layer may choose to downgrade the set of QOS parameters that is forwarded to the destination. The user parameters may also influence the selection of the requested network QOS parameters in the invocation of network services by the transport layer. When there is negotiation of QOS parameters, the following steps are performed:

a. The transport layer receives the TS-user-specified QOS parameters provided in the T-CONNECT request and encodes those values or downgraded values in the corresponding CR TPDU.

b. The transport layer provides the destination TS-user, via the T-CONNECT indication, the proposed QOS values or downgraded values of parameters contained in the CR TPDU.

c. The transport layer uses the QOS values provided in the T-CONNECT response issued by the destination TS-user to determine the QOS values in the corresponding CC TPDU. The destination TS-user may also issue a DR TPDU based on unacceptable QOS.

d. If a TC is established, the transport layer reports to the originating TS-user the final negotiated values of QOS parameters in the T-CONNECT confirm primitive.

Note 1.— Modification of user parameters will happen if the ATN Transport Entity has additional provisions implemented that estimate the ability to provide the requested QOS. If there are no system management monitoring or estimation functions implemented, the QOS parameters will be passed unchanged.

Note 2.— As there is no requirement for the ATN Transport Layer to provide QOS monitoring functionality, the agreed QOS values are not guaranteed by the TS-provider.

Note 3.— As part of the interpretation of QOS parameters, the transport layer must have some method to determine the relative importance of cost. While relative importance of cost is not a parameter provided by the TS-user, it is a parameter that the transport layer must specify as a network service user (NS-user). The importance of cost can be determined by configuration or it may be determined based on rules which take into account the other parameters specified by a TS-user.

4.1.2.3.2 Connection Mode Transport Layer QOS Parameters

The QOS parameters are set to agreed values based on a combination of *a priori* knowledge and negotiation. In respect to this distinction, QOS parameters can be divided into two classes :

- the *non-negotiated* QOS parameters, i.e. those QOS parameters which cannot be changed during the connection establishment phase. Most of these parameters are communicated to the local TS-provider only.

- the *negotiated* QOS parameters, i.e. those QOS parameters which can be negotiated with both the TS-users and the remote TS-provider.

According to ISO 8072, the set of possible values and the default parameter values should be specified at the initial installation of the TS-provider. These values can also be fixed (for one or more QOS parameters) for a given TS-provider, in which case there is no negotiation when the connection is established. Subsequent paragraphs explain a simple method of specification and interpretation of transport layer interface QOS parameter values.

4.1.2.3.2.1 Non-Negotiated QOS Parameters

QOS non-negotiated parameters are TC establishment delay, TC release delay, TC establishment failure probability, transfer failure probability, resilience of the TC, TC release failure probability, and protection. Even if ATN provisions do not impose any restrictions on the range of values which can be specified, users must be aware that the ATN transport layer has no means to enforce the requested QOS characteristics. Thus, in practice, the TS-users should have *a priori* knowledge of the QOS parameters values available from the given TS-provider. The requested non-negotiated QOS values can then refer to the prior agreed non-negotiated QOS values in all TC establishment attempts. ATN TS-users with strict QOS requirements are responsible for determination of whether the required non-negotiated QOS parameters values can be satisfied.

4.1.2.3.2.1.1 Transport Connection Establishment Delay.

This is the maximum acceptable time between a connection request (T-CONNECT request primitive) and the corresponding confirmation (T-CONNECT confirm primitive). This time includes any delays due to the called user.

4.1.2.3.2.1.2 Transport Connection Release Delay.

This is the maximum acceptable delay between a TS-user-initiated disconnect request and the delivery of the corresponding indication to the destination TS-user (this time limit does not apply to TS-provider-initiated releases). This delay is specified independently for each TS-user; issuance of a disconnect request by either TS-user starts the counting of TC release delay for the other user.

4.1.2.3.2.1.3 Transport Connection Establishment Failure Probability.

This is the ratio of total TC establishment failures to total TC establishment attempts in a measurement sample. A connection establishment attempt is considered to have failed when a requested connection is not established within the specified maximum acceptable TC establishment delay. This may occur as a result of misconnection, TC refusal or excessive delay on the part of the TS-provider (the reason can be congestion or other internal problems on the network). This parameter includes only failures due to TS-provider faults (failures due to TS-user faults are excluded in calculating this parameter).

4.1.2.3.2.1.4 Transfer Failure Probability.

A transfer failure is defined as demonstrated in a transfer sample in which the observed performance as measured by the transport entity is worse than the minimum acceptable thresholds for one or more of the following QOS parameters: residual error rate (RER) and transit time. A transfer sample begins on input of a selected TSDU at the sending TS-user boundary and continues until the outcome of a given number of TSDU transfer attempts has been determined. This is a discrete observation of TS-provider performance in transferring TSDUs between a specified sending and receiving TS-user. It normally corresponds to the duration of an individual TC. Transfer failure probability is the ratio of total transfer failures to total transfer samples observed during a performance measurement. If reliable QOS monitoring is available, this probability can be estimated by the resilience of the TC parameter (i.e. the probability of a TS-provider-initiated release during a transfer sample). It indicates the part of the time for which the agreed QOS values were not reached during an observation period.

4.1.2.3.2.1.5 Resilience of the Transport Connection.

This is the probability of a TS-provider-initiated connection release (i.e. issuance of a T-DISCONNECT indication with no prior T-DISCONNECT request) during a specified time interval. It expresses the reliability of the connection.

4.1.2.3.2.1.6 Transport Connection Release Failure Probability.

A TC release failure occurs, for a receiving TS-user, if that user does not receive a T-DISCONNECT indication within the maximum TC release delay of the originating TS-user issuing the T-DISCONNECT request, given that the receiving TS-user has not itself issued a T-DISCONNECT request. The TC release failure probability is defined as the ratio of total TC release requests resulting in release failure to total release requests during a measurement sample.

4.1.2.3.2.1.7 Protection.

This is a qualitative parameter indicating security-related protection of the data carried on the connection. Four options are available:

- no protection features,
- protection against passive monitoring,
- protection against active measures (i.e. modification, replay, addition or deletion),
- protection against both passive and active monitoring

The protection parameter takes one of four logical values corresponding to the four options defined in ISO 8073.

4.1.2.3.2.2 Negotiated QOS Parameters

QOS negotiated parameters are transit delay, residual error rate, and priority. In specifying the quantitative parameters, a TS-user can:

- omit, or indicate a "DEFAULT" value for those parameters which are not of interest for its communication needs,

- indicate a scalar value for parameters of interest.

If all of these parameters are set to "DEFAULT" values, this is equivalent to the case of fixed values. In this case, according to ISO 8073, no QOS negotiation takes place at the transport layer; the most important network layer QOS factor to optimize for the TS-provider would then be a default set of network QOS values set by configuration, usually the cost factor.

If the TS-user specifies scalar values for one or more QOS parameters, some rules (see 8.2.5.1.2.4) apply on the interpretation of those values by the ATN COTS provider. A straightforward way to interpret the TS-user-requested QOS values is to define threshold values for each one of the quantitative parameters. If the TS-user specifies, for a given QOS parameter, a scalar value higher than the specified threshold, this parameter is considered more important than the others.

4.1.2.3.2.2.1 Transit Delay.

This is the elapsed time between a data transfer request submitted by a TS-user and the delivery of the corresponding indication to the peer TS-user. A maximum and an average value are defined. Each of these specifications is based on an average TSDU size fixed beforehand. The delays due to any interface flow control exercised by the receiving TS-user are not included in the transit time. The transit delay is only calculated for those TSDUs whose transfer is correct (i.e. without error and in the proper sequence). In summary, this parameter consists of four values :

- Maximum transit delay calling-called user direction

- Average transit delay calling-called user direction

- Maximum transit delay called-calling user direction

- Average transit delay called-calling user direction

4.1.2.3.2.2.2 Residual Error Rate.

This is the ratio of the sum of lost, incorrect and duplicate TSDUs to total TSDUs transferred across the transport interface during a measurement period.

4.1.2.3.2.2.3 Priority.

This is the relative priority of a TC (with respect to other TCs) and specifies the order in which the TCs are to have their QOS downgraded as necessary, or the order in which the connections should be broken in the event of a shortage of resources

The use of the Transport priority is optional in the CNS/ATM-1 package.

When specified, transport priority values should be integers in the range from 0 to 14, with priority level 0 as the highest priority. In such a case, there is a one-to-one correspondence with the CLNP priority values (see Table A5-1 for further details on the mapping of Transport priority values to CLNP priority values).

4.1.2.4 Transport Layer Protocol Conformance

This section provides background information on the provisions for the connection mode transport protocol and the encoding of TPDUs. The requirements for the connection mode transport protocol are defined using the APRL for the ISO 8073 protocol. The numbering of this section has been patterned after the numbering of the APRL in Appendix 8 for ease of reference. Chapter 4 explains APRL usage and symbology.

4.1.2.4.1 Mandatory and Optional Functions

This section defines the mandatory and optional functions of the ATN implementation of ISO 8073.

4.1.2.4.1.1 Index of Indices

The Provisions contain an index of all indices used in the APRL.

4.1.2.4.1.2 Protocol Implementation

The base standard which applies to the ATN Transport Layer protocol is the 1992 version of ISO 8073.

Efforts were expended for backwards compatibility to encompass the following features of the 1992 version which do not exist in the 1988 version:

1. A new parameter, "preferred maximum TPDU size", was added to accommodate a larger set of sizes than was possible with the present parameter, "maximum TPDU size".

2. The Selective Acknowledgement option was added, which allows a transport entity to acknowledge a non-contiguous set of TPDUs.

3. The Request Acknowledgement option was added, which allows a transport entity to request that the remote entity acknowledge received TPDUs.

4. The inactivity time is specified as two times, a "local" inactivity time and a "remote" inactivity time.

5. The values of the inactivity times can now be passed as parameters in the connection establishment phase.

Note.— The PICS (D.6.2) identifies C4L as ISO:C2:0 reflecting that Class 4 over connectionless networks requires the implementation of class 2 for conformance purposes. However, ISO 8073 6.5.5.i indicates that Class 4 is the only valid class over the CLNS. There is no purpose for requiring Class 2 in the ATN environment.

4.1.2.4.1.2.1 Protocol Classes Implemented.

This statement is used to indicate which classes of ISO 8073 are implemented. For operation over the ATN network service, only the last class, *Class Four over Connectionless Network Service*, is applicable.

4.1.2.4.1.2.2 Specific ATN Recommendations.

This statement is used to indicate the specific recommendations made by Appendix 8 in selection of optional features of ISO 8073.

4.1.2.4.1.3 Initiator/Responder Capability for Protocol Classes 0-4

Predicates "IR1" and "IR2" are defined as an option set in the ISO PICS, which means that a conforming implementation of the transport protocol must be able to initiate a connection or respond to a connection request. The ATN Transport profile recommends that both capabilities be present. This capability will support the long-term utility of transport layer implementations in the ATN.

4.1.2.4.1.4 Supported Functions

4.1.2.4.1.4.1 Supported Functions for Class 4 (C4 or C4L::).

8.2.4.1.4.1.1 Mandatory Functions for Class 4. All Class 4 features of the ISO transport layer defined as mandatory by ISO must be part of the ATN transport protocol.

8.2.4.1.4.1.2 Mandatory Functions for Operation over Connectionless-mode Network Service. All features of the ISO transport layer for operating over a CLNS that are defined as mandatory by ISO must be part of the ATN transport protocol.

8.2.4.1.4.1.3 ISO 8073 Optional Functions. All of the functions of the transport protocol defined as optional by ISO are either required or recommended for the ATN transport protocol

Note.— Refer to 8.2.4.1.10 on negotiation of transport layer options.

Support of extended TPDU numbering is recommended to allow support of ATS applications with high data rates or those operating over links with long delays. Normally, the transport protocol uses 7 bits for the TPDU number, resulting in a range of [0 - 127]. Extended TPDU numbering uses 31 bits for the TPDU number and expands this range to [0 - 2 147 483 647]. The extended numbering option is useful when there are a large number of TPDUs that may be unacknowledged at a time. This may occur, for example, when a large amount of data is transferred over a link which has long delays, or for the case when information transfer is primarily unidirectional. The other reason extended numbering is used is to support a high rate of TPDU transfer. TPDU numbers may not be re-used during the maximum period to receive an acknowledgement, L (see 8.2.4.1.12). If a large number of TPDUs (i.e. more than seven) is expected to be transmitted during the period L, and flow control is not acceptable, extended numbering is required to guarantee unique TPDU numbers. The cost of using extended TPDU numbering is an increased header on every TPDU that is transmitted for a given connection. Thus, this option should not be exercised when the window sizes for normal TPDU numbering are sufficient.

Support of the non-use of checksum feature is required to allow applications that can tolerate some level of error to operate without the added cost of transmitting checksums with every TPDU. Checksums are used to verify the end-to-end integrity of data within a TPDU. By default, checksums are present in all TPDUs; non-use must be mutually agreed by both TS-users.

Note.— The transport layer provisions do not specify the conditions for an initiating transport layer entity to specify non-use of checksums. The use or non-use of checksums is dependent on the characteristics of the TS-user-data flow. Refer to 8.2.3 on methods to select this option.

Support of the selective acknowledgement feature is recommended to improve the management of air-ground resources and to reduce unnecessary retransmissions of data. Selective acknowledgement allows the transport layer to acknowledge receipt of multiple TPDUs, even if there is one or more missing in a given sequence. For example, if the transport layer received TPDU numbers 4, 5, 6, 8, and 9, it can use the selective acknowledgement function to indicate receipt of all of these TPDUs, indicating that number

7 is not yet received. This provides the remote transport layer the information to retransmit only TPDU number seven, without having to retransmit 8 and 9.

Support of the request of acknowledgement (ROA) function is recommended for ATN implementations. The ROA function allows a transport layer to request that the remote transport layer acknowledge all currently received TPDUs. This is especially useful in the case that either a transmit window is closing up, or the sending transport layer is having buffer limitations and needs to free up additional space.

Support of the reduction of credit window feature is recommended to support congestion avoidance mechanisms in the transport layer.

Support of the concatenation function is recommended to improve use of air-ground resources. Concatenation of TPDUs may be performed when a number of TPDUs is to be sent to the same transport entity (for example, a DT TPDU and an AK TPDU). Multiple TPDUs may be concatenated and sent together in the same NSDU to the remote transport entity; the remote entity then separates the two TPDUs. Note, however, that concatenation of TPDUs may not be suitable with TS-users requiring minimal delays, since some TPDUs may be held until several are concatenated.

4.1.2.4.1.5 Supported TPDUs

4.1.2.4.1.5.1 Mandatory TPDUs.

All of the TPDUs defined by ISO for Class 4 operation over the connectionless network service are mandatory for the ATN transport layer.

4.1.2.4.1.5.2 Error TPDU Support.

The Error (ER) TPDU may be sent by a transport layer in response to an error condition, such as receiving a legal TPDU with illegal values. Transmission of the ER TPDU is not required by the transport protocol; the conditions which cause an entity to transmit one are a local matter.

4.1.2.4.1.6 Supported Parameters of Issued TPDUs

4.1.2.4.1.6.1 Parameter Values for CR TPDU.

The additional option selection parameter shall be included in a CR TPDU in order for the initiator to inform the destination of intentions for the following protocol options:

Use of request of acknowledgement

Use of selective acknowledgement

Non-use of checksum

Use of transport expedited data transfer service

Note.— Refer to Table 8-3 for the encoding of the additional option parameter.

Table 8-3 Encoding of the Additional Option Field

Bit	Option	Class
6	Use of request acknowledgement	1,3,4
5	Use of selective acknowledgement	4
4	Use of network expedited data	1 (N/A)
3	Use of receipt confirmation	1 (N/A)
2	Non-use of checksum	4
1	Use of transport expedited data	1,2,3,4

4.1.2.4.1.6.2 Supported Parameters for Class 4 TPDUs (C4 or C4L::).

8.2.4.1.6.2.1 Optional Parameters for a Connection Request TPDU. This section describes the ATN recommendations for support of the optional parameters which may be included with a CR TPDU. Note that no parameters are recommended that cannot be supported in both the 1992 and the 1988 versions of ISO 8073.

Support of the called and calling TSAP-ID parameters is required to allow applications to be identified through the use of upper-layer selectors, rather than using *a priori* knowledge of the user based on the NSAP. The called TSAP-ID parameter contains the TSAP Selector portion of the called user's TSAP, and ensures unambiguous identification of the destination TS-user. The calling TSAP-ID allows the destination user to identify the calling TS-user, and initiate a call to the other user in the case that the transport connection is terminated.

The ability to use the TPDU size parameter is recommended. There are two different parameters which may be used to propose a TPDU size, the TPDU Size parameter (index I4CR9) and the Preferred Maximum TPDU Size parameter (index I4CR18). Either parameter may be used to negotiate a maximum TPDU size. The latter was added to the latest version of ISO 8073 to allow a larger range of TPDU sizes. Invocation of the Preferred Maximum TPDU Size parameter should only be done if the peer transport entity is known to implement the parameter. Otherwise, if the preferred maximum TPDU size parameter is not recognized, the maximum TPDU size will be the default value, 128 octets.

Support of the version number parameter is not recommended. No specific use is seen for this parameter, and implementations should not expect that other ATN transport entities will use this optional parameter.

Support of the protection parameter is not currently recommended as no security mechanisms have been defined for the ATN besides the network layer IDRP traffic type parameter. Use of this feature may be specified in later versions of the CNS/ATM SARPs, when an ATN-wide solution to the security problem has been specified.

The additional option selection parameter must be supported in a transport layer implementation, to allow negotiation of several transport layer optional functions.

Support of the residual error rate parameter and the transit delay parameter is not recommended for transport layer implementations.

Support of the priority parameter is recommended. In addition, the priority parameter should be present in a CR TPDU. Priority is an especially important feature in the ATN air-to-ground environment. There are long-standing priority mappings (e.g. ITU) used to

separate traffic by criticality. Flight safety TSDUs must never be interspersed with routine communications. Priority is non-negotiable in the ATN. TS-users should issue a DR TPDU if a different priority level is returned in the CC TPDU. There is a further ICAO recommendation that the responding transport layer should respond with the same priority as was proposed. For transport implementations unable to specify priority, a default priority may be used. This default priority is the lowest transport priority (level 14), and is mapped to the lowest network priority level. Priority is used to separate classes of application traffic, and to ensure that in conditions of limited resources certain classes of traffic receive service over others. Thus implementations unable to state priority will have their traffic discarded first in an ATN global congestion avoidance scheme. These priority mappings are also enforced by certain NS-providers.

Support of the acknowledgement timer parameter and the inactivity time parameter is recommended. These two parameters allow transport entities to better manage transport resources.

8.2.4.1.6.2.2 Optional Parameters for a Connection Confirm TPDU. Requirements and recommendations on the support of parameters for the CC TPDU follow those for the CR TPDU parameters. It is recommended that if both the preferred maximum TPDU size parameter and the Maximum TPDU size parameters are present in a CR TPDU, then the CC TPDU should respond using the Preferred Maximum TPDU size parameter only.

8.2.4.1.6.2.3 Optional Parameters for a Disconnect Request TPDU. The Additional Information parameter (index I4DR4) in a DR TPDU is not recommended for ATN implementations of the transport layer.

8.2.4.1.6.2.4 Mandatory Parameter for a Data TPDU. If the Request of Acknowledgement feature has been selected during the connection establishment phase, then the Request of Acknowledgement (ROA) parameter (index I4DT4) is mandatory in the DT TPDU.

8.2.4.1.6.2.5 Optional Parameters for an Acknowledgement TPDU. The flow control confirmation parameter (index I4AK4) is recommended for ATN implementations of the transport layer.

8.2.4.1.6.2.6 Use of the Subsequence Number Parameter in the Acknowledgement TPDU. If the reduction of credit window capability is implemented, support of this parameter is required. Even if it is not implemented, support of the flow control confirmation parameter is recommended for use in congestion avoidance mechanisms.

8.2.4.1.6.2.7 Use of the Selective Acknowledgement Parameter in the AK TPDU. Support of this parameter is recommended for transport layer implementations. If selective acknowledgment has been selected for a given TC, then this parameter is optional in an AK TPDU.

8.2.4.1.6.2.8 Optional Parameters for an Error TPDU. The Invalid TPDU parameter (index I4ER3) in an ER TPDU is not recommended for ATN implementations of the transport layer.

4.1.2.4.1.7 Supported Parameters for Received TPDUs

The following sections describe the requirements for supporting parameters in received TPDUs. Implementors should be aware that a transport layer should be capable of receiving and processing all possible parameters for all possible TPDUs, depending upon the class and optional functions implemented.

4.1.2.4.1.7.1 TPDUs in Class 4 (C4 or C4L::).

If use of checksums has been selected during connection establishment (either explicitly by the responder or by default), the transport layer must process the checksum parameter in the listed TPDUs. If the computed checksum for a TPDU does not match the checksum included in the TPDU, the transport layer must discard the TPDU.

4.1.2.4.1.8 User Data in Issued TPDUs (C4L::)

These requirements refer to the presence of user-data in a connection request, connection response, or disconnect request TPDU.

4.1.2.4.1.8.1 User Data in Class 4 TPDUs (C4 or C4L::).

A TS-user may optionally include data in the CR, the CC, or the DR TPDUs. The ability to include data in the CR, CC, and DR TPDU is required for ATN implementations.

4.1.2.4.1.9 User Data in Received TPDUs

As defined by ISO, all transport layer implementations capable of initiating a CR must be able to receive user-data in the two possible responses: a CC TPDU or a DR TPDU. These data are passed on to the TS-user. Similarly, all transport layers capable of responding to a CR must be able to receive user-data within a CR TPDU.

Since both capabilities are recommended, transport layer implementations should be able to receive data in the appropriate TPDU.

4.1.2.4.1.10 Negotiation

The ISO transport layer allows areas of negotiation in the connection establishment phase. One of the negotiated features is the class of operation. Depending on the class selected, other features are also negotiated.

Negotiation in the transport layer is based on the following assumptions:

a. If a feature is not negotiated, the "default" option, or "mandatory" implementation of the option, is selected.

b. To suggest anything other than the default, the proposed value must be explicitly proposed in a connection request.

c. The responder has the choice of explicitly accepting the proposed value or possibly selecting a "lesser", or "mandatory" value. If the responder does not explicitly indicate the desired value, the default is in effect.

For example, one option for class four operation is the use of checksums. The default is use of checksums, and all implementations must be able to support use of checksums on a connection. To operate a connection without checksums, the requester must explicitly propose "non-use of checksums". If the responder does not explicitly reply with "non-use of checksums", then the checksum procedures are in effect for that connection.

Table 8-4 indicates the items that can be negotiated and their default, or mandatory, values in Class 4 operation.

Table 8-4 Negotiable and Default Values for Class 4 Operation

Feature	Allowed Values	Default
Preferred TPDU Size, octets	Multiple of 128	128
Maximum TPDU Size, octets	128, 256, 512, 1024, 2048, 4096, 8192	128
TPDU Numbering Format	normal, extended	normal
Expedited Data	use, non-use	non-use
Checksum	use, non-use	use
Selective Acknowledgement	use, non-use	non-use
Request Acknowledgement	use, non-use	non-use

4.1.2.4.1.10.1 Class Negotiation - Initiator.

The first ISO requirement for class negotiation states that "the preferred class in the CR TPDU may contain any of the classes supported by the implementation". This requirement is further constrained by connectionless network operation - for ATN implementations, the preferred class *must* be class 4.

In addition, a CR TPDU may contain an alternative class parameter. Since the only acceptable mode is class 4, there are no alternative classes allowed.

4.1.2.4.1.10.2 Class Negotiation - Responder.

There is only one appropriate class for operation in the connectionless network environment - class 4. An implementation of the ATN transport layer must respond with class 4 as the negotiated class.

4.1.2.4.1.10.3 TPDU Size Negotiation.

All transport entities must be able to support a TPDU size of 128 octets, the default required by ISO 8073. Larger sizes may also be supported, such as the recommended 1024-octet capability. 1024 octets is the minimum maximum-size value recommended for ATN usage. The actual TPDU size negotiated for a TC, however, may be smaller than the maximum size supported or the initial size proposed.

The larger TPDU size is recommended for application data exchanges involving large TSDUs. The optimum TPDU size may vary anywhere from 128 octets up to the maximum TSDU size required by a TS-user. The selection of a 1024-octet TPDU size ensures that no additional network segmentation will be performed on any TPDUs transmitted as NSDUs.

8.2.4.1.10.3.1 TPDU Size Support. Indices TS1 and TS2 require that if a size for TPDUs is proposed, that the initiator must be capable of supporting all legal TPDU sizes smaller than the proposed size. For example, if the Preferred Maximum TPDU Size parameter was included in a CR to propose a TPDU size of 1,280 octets (128 octets times ten), the initiator must be prepared to use a negotiated TPDU size of (n*128) octets, where ($1 \leq n \leq 10$). If the Maximum TPDU size parameter is used, the negotiated size may be in the set [128, 256, 512, 1024, 2048, 4096, or 8192], as long as it is equal to or smaller than the proposed size.

8.2.4.1.10.3.2 Preferred Maximum TPDU Size Support. The maximum preferred TPDU size that an initiator proposes may be any multiple of 128 octets.

For operation over the ATN, it is recommended that a size of 1024 octets be negotiated for the preferred maximum TPDU size. This value is derived from the requirements for the minimum subnetwork service data unit (SNSDU) size.

8.2.4.1.10.3.3 Maximum TPDU Size Support. The maximum preferred TPDU size that an initiator proposes may be from the set [128, 256, 512, 1024, 2048, 4096, 8192].

For operation over the ATN, it is recommended that a size of 1024 octets be negotiated for the maximum TPDU size. This value is derived from the requirements for the minimum SNSDU size. It eliminates the need for segmenting by the CLNP.

4.1.2.4.1.10.4 Use of Extended Format.

The default format for TPDU numbering is the "normal" format, which involves the use of a seven-bit field. Extended format uses a 31-bit field. If there is no proposal in a connection request, the normal format is used. If the initiator proposes extended format, the responder may reply indicating use of normal format.

Generally, the extended format is used when an extremely large window of outstanding TSDUs is expected. This would occur, for example, on large data transfers with very little interaction between end users (e.g. reception of acknowledgements only after an extended interval). Large windows may also occur in the situation where a link has high capacity but long transit delays.

Thus, the use of normal formats is recommended for operation in the ATN because of the smaller resulting size of transport protocol headers. Note that as defined by ISO 8073, the ability to support normal formats is mandatory.

4.1.2.4.1.10.5 Expedited Data Transport Service.

Support of the expedited data transport service is required by ISO 8073. Thus, all ATN implementations must have the capability to send and receive expedited data. Actual use of the feature is optional. Negotiation of the expedited data service is performed using the additional options selection parameter (bit 1) as shown in Table 8-3.

4.1.2.4.1.10.6 Non-use of Checksum ((C4 or C4L::) and T4F29::).

The default operation for a connection is to use checksums. If non-use is desired, the initiator must propose non-use of checksums and the responder must agree. Checksums are a valuable tool because they verify the end-to-end integrity of TPDUs, and thus all TSDUs.

Non-use of checksums may be selected, for example, to support transmission of low-fidelity graphical data. The initiator of a transport connection being used for this purpose may propose non-use of checksums if the cost of using checksums (both in terms of cost and transmission efficiency) is considered too high. It is recommended in such cases that the responding transport layer accept the non-use of checksums so that the efficiency gains can be realized.

There may be situations, however, when the responding transport entity would not agree to non-use of checksums. For example, if the responding entity has knowledge that the available QOS between the two end systems is not sufficient to support the needs of the TS-user, it may respond indicating that checksums are to be used.

Note.—The method of acquiring knowledge of available QOS is a local matter. For some applications, dynamic knowledge may be required. Other applications may have less stringent needs and will not require any dynamic information.

All ATN transport layer implementations must be able to propose either use or non-use of checksums in a CR TPDU. If non-use is proposed, all ATN transport layer implementations must be able to accept non-use. Mechanisms for determining when not to accept the non-use of checksums are not required.

4.1.2.4.1.10.7 Use of selective acknowledgement.

The default for selective acknowledgement is non-use. That is, selective acknowledgement must be explicitly proposed in a CR TPDU and accepted in the CC TPDU.

Because the selective acknowledgement feature reduces the need for retransmitting TPDUs, it is recommended that transport layer implementations propose the use of selective acknowledgement in a CR TPDU. If a transport layer receives a CR TPDU proposing this option, it is recommended that the proposal be accepted in the CC TPDU.

Note.— Refer also to 8.2.4.1.4.1.3 for a description of the selective acknowledgement feature.

4.1.2.4.1.10.8 Use of Request of Acknowledgement.

The default for ROA is non-use, that is, ROA must be explicitly proposed in a CR TPDU and accepted in the CC TPDU. The ROA function allows a transport layer to request, on a per-TPDU basis, that the remote transport layer immediately acknowledge all TPDUs currently awaiting acknowledgement. This is especially useful in the case that a window is closing up, or if the sending transport layer is having buffer limitations, and needs to free up additional space. Thus, it is recommended that this option be proposed in a CR TPDU, and that it be accepted, if proposed, in the CC TPDU.

4.1.2.4.1.11 Error Handling

In some cases, the action upon certain types of error is mandatory (see also 8.2.4.1.7).

4.1.2.4.1.11.1 Action on Receipt of a Protocol Error

There are three possible actions of a transport implementation upon detection of a protocol error:

- The transport layer can issue an ER TPDU
- The transport layer can terminate the transport connection (that is, issue a DR TPDU)
- The transport layer can discard the TPDU (that is, ignore the error).

Events which qualify as a protocol error are defined in the following sections (for example, see index RR2). It is recommended that in event of a protocol error, that the transport layer issue an ER TPDU, discard the TPDU, or respond with a DR TPDU

4.1.2.4.1.11.2 Actions on Receipt of an Invalid or Undefined Parameter in a CR TPDU.

The actions upon receipt of an invalid parameter are defined as mandatory by ISO, and so must be performed by all ATN implementations of the transport layer.

Index RR1, which is concerned with receipt of an undefined parameter, requires that the parameter be ignored. This action, in combination with the general rules for negotiation

allows compatibility between versions of the transport layer. For example, if a transport layer issues a CR proposing the selective acknowledgement option to a remote transport layer built to ISO 8073 (1988), the remote transport entity will not recognize the new option. Rather than declaring a protocol error, the remote entity would simply pass over the option and would continue to process the rest of the TPDU. A transport connection could then be

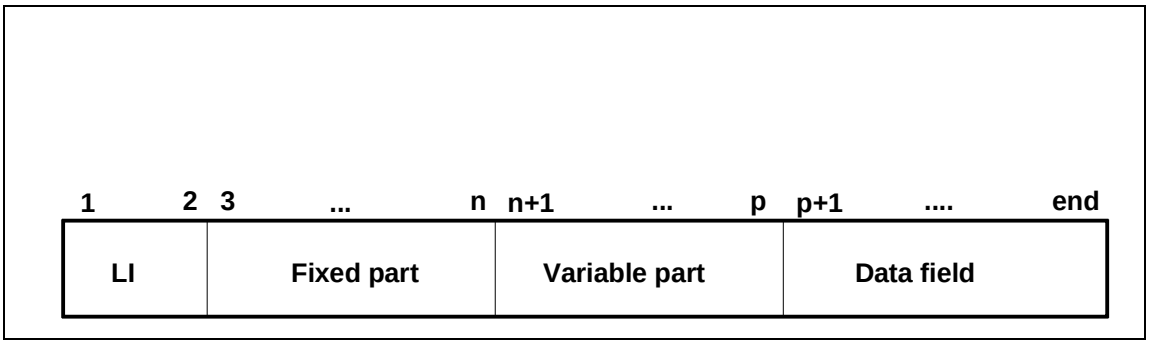

Figure 8.5: TPDU General Structure

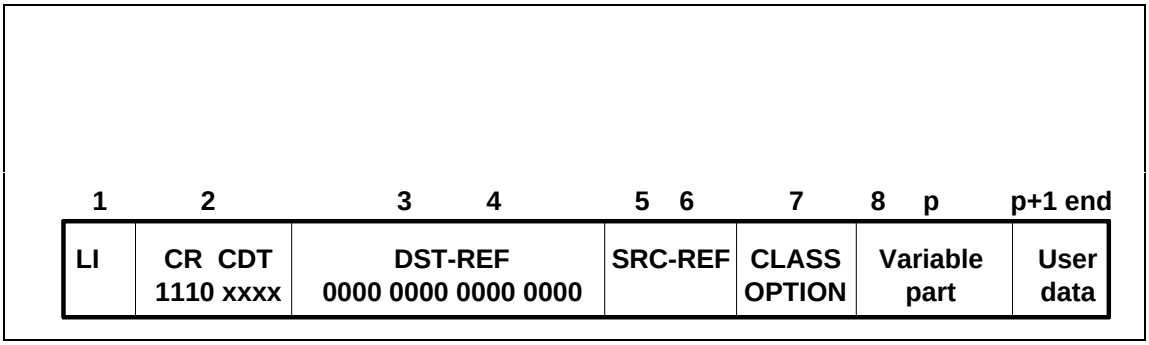

Figure 8.6: Connection Request TPDU

established which operates without using selective acknowledgement.

For index RR7, an implementor may specify the action upon receipt of a valid parameter with an invalid value. Note that for class 4 over CLNS operation, if the parameter in question is the checksum, the transport layer is required to discard the TPDU (see index U13).

4.1.2.4.1.11.3 Actions on Receipt of an Invalid or Undefined Parameter in a TPDU other than a CR TPDU.

The interpretation of certain events is defined as mandatory by ISO. The decision of whether to treat an undefined parameter as a protocol error or to ignore it is a local matter. In the case that a protocol error is defined, the implementation should either discard the TPDU, issue an ER TPDU, or issue a DR TPDU.

4.1.2.4.1.12 Timers and Protocol Parameters

Although the implementation of most of the timers and protocol parameters is mandatory, there are no mandatory values for them, other than the maximum values which may be defined for each.

It is recommended for ground systems that timers be configurable on a per TC basis.

In general, the assignment of values for timers and parameters must be optimized based on operational testing of the applications. In such testing, incompatible timer values and optimum combinations can be identified. Implementations of the transport protocol should support configurable values for all timers and protocol parameters on a TC or TSAP basis, rather than having fixed values. This allows modification as operational experience is gained.

Note 1.— Refer to Table 8.5 for the complete listing of timers and parameters.

Note 2.— Refer also to 12.2.1.1 of ISO 8073 for more details on the timers.

Note 3.— The subscripts "R" and "L" refer to "remote" and "local", respectively. The variable E_{RL}, for example, refers to the maximum transit delay from the remote entity to the local entity. The variable E_{LR} is the maximum transit delay from the local entity to the remote entity. It is assumed that these values may be different.

Table 8-5 Example Timer and Parameter Values and Ranges

Symbol	**Name**	**Minimum**	**Example**	**Maximum**
M_{RL}, M_{LR}	NSDU Lifetime, seconds	5	40	135
E_{RL} + E_{LR}	Maximum Roundtrip Transit Delay, seconds	0	35	150
A_L, A_R	Acknowledgement Time, seconds	0	2	20
T1	Local Retransmission Time, seconds	12	37	300
R	Persistence Time, seconds	0	75	2710
N	Maximum Number of Transmissions	1	3	10
L	Time bound on reference and/or sequence numbers, seconds	160	160	3000
I	Inactivity Time, seconds	300	960	3000
W	Window Time, seconds	160	160	400

Note. - This table is subject to validation during ATN operational testing.

Several of the timers and variables are not directly configurable, but may be determined based on the values of other timers and variables.

- The NSDU lifetime variables, M_{RL} and M_{LR}, may have a general estimate, based on the lifetime values used for NPDUs. The NSDU lifetime value is the value used to delete aged packets from the ATN. It should be over three times the expected end-to-end time. The expected air-to-ground end-to-end time can be up to 30-40 seconds.

- The end-to-end delay variables, E_{RL} and E_{LR}, may be estimated only, or some mechanism may be available to determine these dynamically.

- The value for the local acknowledgement timer, A_L, may be determined based on application requirements. For example, applications supporting ATC may require immediate acknowledgement of TPDUs so that the uncertainty about delivery is minimized. The remote acknowledgement time variable A_R, for example, may not be known or it may be provided by the remote transport entity explicitly during the connection establishment phase. The value for A_L should be dynamically configurable.

- The local retransmission time, T1, is defined by ISO as:

  $T1 = E_{LR} + E_{RL} + A_R + x$, where x is the local processing time for a TPDU.

- The persistence time, R, is the maximum time a transport entity will attempt to retransmit a TPDU. The persistence time is larger, in general, than the maximum number of retransmissions, N-1, times the local retransmission time, T1.

- The maximum number of transmissions, N, is related to the expected transmission reliability of the end-to-end path, since exceeding N results in the termination of a transport connection. Too high a value, however, may result in wasted retransmissions if end-to-end communication is no longer possible.

- The maximum time to receive an acknowledgement of a given TPDU, L, is bounded by ISO as:

  $L = M_{LR} + M_{RL} + R + A_R$

- In general, a reference or sequence number should not be re-used for the time period L. The value of L, in combination with the expected traffic, may be used to determine if extended TPDU numbering is required.

- The inactivity timer, I, is set based on network delays and the expected QOS. Specification of this parameter is related to the use of the maximum number of transmissions parameter, N, since it is used to terminate transport connections.

- The window timer, W, determines when acknowledgements are sent in the case of no activity. Up-to-date window information is sent when W expires. It should be set smaller than the expected value of the remote value of I.

Table 8-5 provides an example of some transport timers and parameters specified by one State to support initial ATC services.

4.1.2.5 Use of the Network Service

The transport layer uses the connectionless network service to exchange TPDUs with remote transport entities. This involves two network service primitives: the N-UNITDATA request, to send TPDUs, and the N-UNITDATA indication, to receive TPDUs.

Note.— Guidance on the dynamic determination of network QOS parameters based on TS-user-specified QOS parameters is provided in 8.2.5.1.2.4.2 .

4.1.2.5.1 Use of the N-UNITDATA Request

4.1.2.5.1.1 Scope and Applicability

All TPDUs are transmitted using the N-UNITDATA request primitive. In general, the transmission of a single TPDU corresponds to an invocation of the N-UNITDATA request. If the transport layer performs TPDU concatenation, the combined set of TPDUs is sent via a single request.

4.1.2.5.1.2 Procedure

4.1.2.5.1.2.1 NS-user-data.

The transport layer sends the TPDU (or the concatenated set of TPDUs) as a NSDU.

4.1.2.5.1.2.2 Network Service Access Point Addresses.

Transport addresses are passed between the TS-user and the transport protocol entity. With the connection mode transport layer, transport addresses are passed during the connection establishment phase. The TS-user issuing a CR must provide the destination transport address and the source transport address. These addresses are interpreted by the transport layer when the user's connection request is translated into a CR TPDU and transmitted. The TSAP selectors of the source and destination transport addresses are transmitted within the CR TPDU. The NSAP addresses of the source and destination are used in the transport layer's invocation of the N-UNITDATA request that is used to transmit the CR TPDU.

4.1.2.5.1.2.3 Security.

The value of the security parameter specified by the connection indicator is used as the value of the NS security parameter for the N-UNITDATA that contains the CR TPDU. The same value is used for all subsequent N-UNITDATA requests used to convey TPDUs sent by both the connection initiator and the connection responder on that transport connection.

4.1.2.5.1.2.4 Network Quality of Service.

8.2.5.1.2.4.1 Network Layer Protection. The possible actions that can occur when the user specifies a protection parameter are:

a. the transport layer can use protection techniques peer-to-peer

b. the transport layer can use network protection techniques by setting the network layer protection parameter

c. the transport layer can use a combination of the above actions

d. the transport layer can pass protection parameters but not interpret them.

The ATN implements option (b) by passing the ATN Security Label to the network layer.

ES security techniques can also be performed at any of the other protocol layers, including the application layer for a given application. At the application layer, the security mechanisms can be directly selected to best fit the needs of the particular application.

8.2.5.1.2.4.2 Network Layer Transit Delay, Cost, and Residual Error Probability. The ATN network layer QOS parameters include the relative ranking of cost, transit delay, and error. The TS-user interface supports the specification of transit delay and residual error

rate. The cost parameter, however, is not one of the QOS parameters that are supported by the TS-user interface. The selection of the requested NL QOS parameters can be done by configuration or dynamically.

This section provides suggested mappings between user QOS values and network QOS rankings, using threshold values fixed in an ES. Requested QOS values from the TS-user are compared to the threshold and, based on these results, NL QOS encoding can be proposed.

Table 8-11 Dynamic Selection of ATN Network QOS Rankings

Transit Delay	**Error**	**QOS Ranking**	**QOS Encoding**
-	-	C/T/E	000
-	> T_{RE}	C/E/T	010
-	< T_{RE}	E/C/T	011
> T_{TD}	-	C/T/E	000
> T_{TD}	> T_{RE}	C/T/E	000
> T_{TD}	< T_{RE}	E/T/C	111
< T_{TD}	-	T/C/E	100
< T_{TD}	> T_{RE}	T/C/E	100
< T_{TD}	< T_{RE}	T/E/C	101

Notes.

1. The symbol "-" indicates that the value is not specified

2. The ranking "C/T/E" indicates that "Cost" is most important, followed by transmit delay, with residual error as the least important factor.

3. The symbol "< T_{RE}" means that the residual error parameter specified by the TS user is less than the threshold value.

   For consistent operation of ESs, standard values and interpretations for the thresholds are desirable, although not required. It is expected that operational evaluation of these thresholds would result in determination of optimal values for each threshold. In Table 8-11, these thresholds are defined as T_{TD} for transit delay, T_{RE} for residual error.

   For transit delay, a user can specify both target and maximum acceptable values, in both the calling-called user direction and called-calling user direction. To determine whether transit delay has crossed the threshold, the appropriate direction should be compared with the threshold value. For example, if the user is the originator of a TC, the calling-called user direction is used. For transit delay, a reasonable value for the threshold can be set at 30 seconds for air-ground communications. The maximum possible transit delay that can

be specified is 65 seconds. The threshold value of 30 assumes that of the specifiable range, anything under 30 seconds is relatively unimportant.

For residual error rate, a user can specify a target and minimum acceptable value. To determine whether residual error rate is below the threshold, the target value should be compared with the threshold. For the residual error rate, a reasonable value for the residual error threshold would be 10^{-6}. This is approximately the rate achieved when using checksums. Specification of a lower rate indicates that a residual error beyond the typical rate is desired.

8.2.5.1.2.4.3 Network Layer Priority. When specified, the transport priority parameter shall have a one-to-one correspondence with network priority. Note that for the transport layer, priority level 0 is highest, while for the network layer, priority level 14 is highest. Table 5-1 in the Provisions provides the priority mapping.

The selection of the network priority may be done either on a dynamic basis or on a static configuration basis, depending on the application categories on the ES. If the transport layer supports levels of priority higher than 14, these should be assigned a network priority level of zero.

4.1.2.5.2 Use of the N-UNITDATA Indication

The transport layer receives all TPDUs via the N-UNITDATA indication. TPDUs are contained within the NS-user-data parameter of the N-UNITDATA indication. Note that if the remote transport layer is performing concatenation, there may be multiple TPDUs within a single NSDU.

4.1.2.5.2.1 Scope and Applicability

These procedures apply to all TPDUs that may be received by the transport layer.

4.1.2.5.2.2 Procedure

4.1.2.5.2.2.1 NS-user-data.

The transport layer assumes that the first TPDU begins at the first octet of the NS-user-data. If the length of the TPDU is less than the length of the NSDU, the transport layer should assume that there are one or more TPDUs following the first one.

4.1.2.5.2.2.2 Network Service Access Point Addresses.

The source and destination NSAP addresses are used to determine the source and destination transport addresses associated with a TPDU. In general, this is only required during the connection establishment phase, before a TC identifier has been assigned. The transport addresses are determined by combining the NSAP addresses with the appropriate TSAP selectors. The selectors are contained in a CR or CC TPDU.

4.1.2.5.2.2.3 Network Quality of Service.

The connection mode transport layer does not need to interpret most of the indicated network layer QOS parameters associated with an N-UNITDATA indication. The network layer priority is not interpreted, because, when its use has been specified by the TS-User, the transport priority is set explicitly. The network layer protection parameter is not used. The relative rankings of transit delay, residual error, and cost are after the fact, and do not have any effect on the transport protocol.

As no congestion management strategy has been defined for the CNS/ATM-1 internet, the Congestion Experienced flag will not be interpreted by the transport layer.

4.1.2.5.2.2.4 Security.

The value of the security parameter received in an N-UNITDATA indication is saved by the TS-provider and used with all subsequent N-UNITDATA requests on that transport connection.

4.1.3 The Connectionless Mode Transport Layer

The ATN CLTS is identical to the ISO 8072/AD1 Standard Service Definition. Consequently, the ATN CLTS offers the necessary means for transferring TSDUs of limited size without prior transport connection establishment. The ATN CLTS offers transmission with no protection against losses, duplication or misordering of a TSDU. It is well suited to ATN applications requiring a one-time, one-way transfer of data, thus taking advantage of simpler mechanisms than those employed by the connection mode protocol.

4.1.3.1 Overview of the Connectionless Mode Transport Layer

The defining characteristic of CLTS transmission is the independent nature of each invocation of the Service. Each TSDU is independent in the sense that it bears no relationship to any other TSDU transmitted through the invocation of the connectionless mode service. It is also self-contained in that all of the information required to deliver the TSDU (destination address, quality of service selection options, etc.) is presented to the TS-provider, together with the user-data to be transmitted, in a single service access. Each unit of data transmitted is routed independently by the layer providing the connectionless mode service.

Certain elements of QOS associated with each instance of connectionless mode transmission, are requested from the TS-provider by the sending TS-user. The TS-provider does not guarantee any of the characteristics the user may set.

The connectionless mode transmission is the transmission of a single data unit from a source service access point to one or more destination access points without establishing a connection. In order to speed up the data exchanges and reduce transit delays of short TSDUs, the connection mechanism is not used and the Transport machine has been simplified. The functions in the Transport Layer are those necessary to interface between the service available from the Network Layer and the service to be offered to the TS-users. The functions provided by the Transport Layer in connectionless mode are:

1 - network service selection,

2 - mapping of Transport address onto Network address,

3 - TSDU delimiting (determine the beginning and end of a TSDU),

4 - end-to-end error detection (implying the use of a specific mechanism) and the necessary monitoring of the QOS.

These functions will operate according to the type of subnetwork and the related network services. Only a pre-arranged association between the entities which determine the characteristics of the data to be transferred is required. No dynamic agreement is involved in an instance of the use of service.

4.1.3.1.1 Service Characteristics

The CLTP operates using the ATN connectionless mode network service. The procedure of data transfer is used for one-time, one-way transfer of a TSDU between TS-users. The protocol does not provide confirmation of receipt, TC establishment and release, or network connection establishment and release.

4.1.3.1.2 Data Transfer

The data transfer procedure is used for one-time, one-way transfer of a TSDU between TS-users without confirmation of receipt, without transport connection establishment and release, and without network connection establishment and release.

The QOS parameter in the T-UNITDATA request is used to determine if a checksum mechanism should be used (including a checksum parameter). If a checksum is used, it is generated at the transmitter and verified at the receiver. TPDUs failing verification are discarded.

Receipt verification is unavailable, so any recovery is by a higher layer. Note that no segmenting of a TSDU into smaller TPDUs is permitted and large user-submitted data units (over 63 488 octets) are discarded.

As the ATN transport layer operates over a CLNS, only the following network service primitives are used : N-UNITDATA request and indication. There is no indication given to transport entities of the ability of the network entity (NE) to fulfill the service requirements given in the N-UNITDATA primitive. However, it can be a local matter to make TEs aware of the availability and characteristics (QOS) of the CLNS (e.g. through the use of the N-FACILITY management primitives set).

4.1.3.1.3 ATN Connectionless Mode Transport Service Model

The CLTS can be modelled in the abstract as a permanent association between the two TSAPs. Only one type of object, the unitdata object, can be passed to the TS-provider. The TS-provider may perform any or all of the following actions :

- discard objects,

- duplicate objects,

- change any order of independent service requests into a different order of service indications.

The existence of the association does not depend on the behavior of the TS-users. The set of actions which are performed by the TS-provider on a particular association may depend on the TS-users' behavior. However, these actions are taken by the TS-provider without notification to the TS-user. Awareness of the characteristics of an association is part of the TS-users' *a priori* knowledge of the ATN environment.

4.1.3.2 ATN Connectionless Mode Transport Layer Quality of Service

4.1.3.2.1 Use of Transport Layer QOS

The use of transport layer QOS parameters for the CLTS is similar to that of the connection-mode service (see 8.2.3.1). Unlike the COTS, there is no concept of negotiation of requested transport layer QOS parameters. Each invocation of the T-UNITDATA service involves a set of requested transport layer QOS parameters by the source TS-user; the corresponding T-UNITDATA indication to the destination TS-user contains the indicated transport layer QOS parameters.

The TS-user can specify the requested transport layer QOS parameters, but there is no guarantee that the TSDU will have the requested level of service. Upon delivery of a TSDU, the transport layer provides the indicated transport layer QOS parameters. The indicated parameters are only an estimate of what may have been provided for that TSDU. The transport layer can determine the indicated transport layer QOS parameters by either *a priori* information or through a systems management interface which provides information on the expected QOS between two ESs.

4.1.3.2.2 Connectionless Mode Transport Layer QOS Parameters

Four QOS parameters are identified for the connectionless mode transport service: transit delay, residual error probability, priority, and protection.

In specifying the transit delay and the residual error rate parameters a TS-user can either specify a "DEFAULT" value for those of the parameters which are not important for its communication needs, not specify them at all, or specify a scalar value for the other parameters.

If all of these parameters are set to "DEFAULT" values, the most important factor to optimize for the TS-provider can be a default value, such as cost.

If the TS-user specifies scalar values for one or more QOS parameters, some rules apply on the interpretation of those values by the ATN CLTS provider. A straightforward method to interpret the TS-user-requested QOS value is to define threshold values for each one of these parameters. If the TS-user specifies, for a given QOS parameter, a scalar value higher than the specified threshold, this parameter is considered more important than the others. See for further information on how these parameter values can be mapped onto the network QOS parameters.

4.1.3.2.2.1 Transit Delay

This is the elapsed time between a T-UNITDATA request and the corresponding T-UNITDATA indication. This time defines the maximum value expected during the transmission of the TSDU and does not include any flow control delays, if flow control is exercised by the receiving TS-user. It is based on a TSDU size of 128 octets.

4.1.3.2.2.2 Residual Error Probability

This is the probability that a given TSDU is lost, duplicated or corrupted. This parameter is defined as being the ratio of the total number of lost, duplicated and corrupted TSDUs to the total number of TSDUs transmitted during a measurement period.

4.1.3.2.2.3 Priority

This parameter enables the TS-user to specify the relative priority of a TSDU in relation to every other TSDU handled. A TSDU of higher priority is processed before a TSDU of lower priority by the TS-provider. This parameter specifies the order in which TSDUs should have their associated QOS downgraded, and the order in which they should be discarded in order to retrieve resources.

The use of the transport priority is optional in the CNS/ATM-1 internet.

When specified, priority values should be integers in the range from 0 to 14, with priority level 0 as the highest priority. In such a case, there is a one-to-one correspondence with the CLNP priority values (see 8.3.5). Table A5-1 defines the mapping of transport layer priority values to network layer priority values.

4.1.3.2.2.4 Security

The security parameter is used by the service user to indicate the value of the security label to be associated with the TSDU. The syntax and semantics of the ATN Security Label are specified in 5.9.1.

4.1.3.3 Connectionless Mode Transport Layer Service Primitives

Two TS primitives are used to provide the CLTS: the T-UNITDATA request primitive and the

T-UNITDATA indication primitive. The parameters associated with these primitives are summarized in Table 8-12. The sequence of primitives in a successful CLTS transmission is defined in Figure 8.15.

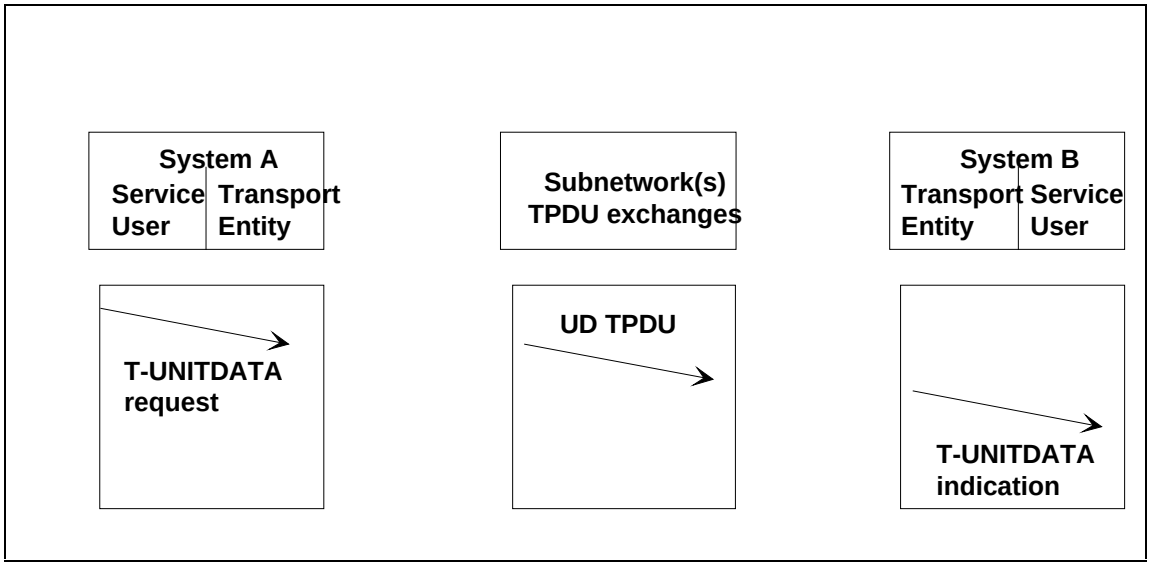

Figure 8.15: Sequence of Primitives and TPDU Exchange for Connectionless Data Transfer

4.1.3.3.1 T-UNITDATA Request

An ATN TS user requests the transfer of a TSDU by invoking a T-UNITDATA request primitive. This primitive has the following associated parameters:

Source and Destination Address: These are TSAP addresses and they are unique within the scope of TSAP addresses. The ATN transport addressing scheme is the same for COTS and CLTS providers i.e. each transport address is composed of an NSAP address and a TSAP Selector (see chapter 7 for further information on Transport Layer addressing).

Quality of service: The value of the QOS is a list of subparameters. The subparameters composing the CLTS QOS are presented in 8.3.2. The TS-provider does not guarantee that it can offer the requested QOS.

TS-user-data: These are the user-data (i.e. the TSDU) to be transmitted between TS-users. The ATN TS-user can transmit an integral number of octets greater than zero up to a limit of 63 488 octets (this amount is 1 K less than the maximum allowed ATN NSDU size). Using a TSDU size of more than 1024 octets may lead to CLNP segmentation and so, to more overhead on the mobile subnetworks.

Security: The security parameter is used by the service user to indicate the value of the security label to be associated with the TSDU. The syntax and semantics of the ATN Security Label are specified in 5.9.1.

With the connectionless mode transport layer, transport addresses are passed with each invocation of the T-UNITDATA primitive. The TS-user sending data must provide the destination transport address and the source transport address. The TSAP selectors of the source and destination transport addresses are transmitted within the header of the UD TPDU; the NSAPs of the source and destination are used in the transport layer's invocation of the N-UNITDATA request that is used to transmit the UD TPDU.

4.1.3.3.2 T-UNITDATA Indication

Upon arrival at the other TC endpoint, a T-UNITDATA indication is delivered by the TS-provider to the destination TS-user. This primitive has exactly the same associated parameters as the T-UNITDATA request primitive. Their values are unchanged by the TS-provider, except for the QOS parameter which may have a different value from the value specified in the request primitive.

The QOS parameter value associated with the T-UNITDATA indication primitive, is based on the NS QOS indication and on the use of the checksum mechanism; it may be different from the value requested, if the TS- or NS-provider has the means to verify that the requested QOS has not been reached. Note that the TS-user-data parameter value is expected to be equal to the TSDU transmitted only if a checksum mechanism has been used for this TSDU.

4.1.3.4 Use of the Network Service

Note.— Refer to 8.2.5 for more background on selection of requested network layer QOS parameters.

4.1.3.4.1 Use of the N-UNITDATA Request

4.1.3.4.1.1 Scope and Applicability

Each UD TPDU is transmitted using the N-UNITDATA request primitive. The transmission of a single TPDU corresponds to an invocation of the N-UNITDATA request.

4.1.3.4.1.2 Procedure

4.1.3.4.1.2.1 NS-user-data.

The transport layer sends the UD TPDU as an NSDU.

4.1.3.4.1.2.2 Network Service Access Point Addresses.

Transport addresses are passed between the TS-user and the transport protocol entity. With the connectionless mode transport layer, transport addresses are allocated into two elements: the TSAP selector and the NSAP. The source and destination TSAPs are sent within the UD TPDU; the NSAPs of the source and destination TS-users are passed as the source and destination NSAPs within the invocation of the N-UNITDATA primitive.

4.1.3.4.1.2.3 Network Quality of Service.

QOS parameters are used to indicate the needed characteristics of the underlying communications service supporting application information exchange. The transport layer must interpret the QOS parameters which are provided by a TS-user; these parameters

may then affect the interactions of the transport layer with the network layer providing service.

4.1.3.4.1.2.3.1 Network Layer Transit Delay, Cost, and Residual Error Probability.

The determination of the network QOS parameters for transit delay, cost, and residual error probability can be done in a manner similar to that of the COTS. See 8.2.5.1.2.4.2.

4.1.3.4.1.2.3.2 Network Layer Priority.

There is no explicit priority parameter in a CLTP TPDU. To meet the ISO 8072 Service Specification, the CLTP entity translates the TS-user priority to network priority upon transmission of a TPDU and perform the inverse upon receipt. For example, to send a TSDU, the CLTP entity maps the TS-user Priority parameter to the network priority parameter, which is passed to the NE in the N-UNITDATA request. This passed parameter is used by the Network entity to set the Network NPDU priority parameter. This mapping ensures that the TS-user requested priority is used for transmission of the TSDU.

Once the TSDU is received by the destination CLTS entity, the datagram transaction is complete. There are no requirements for the receiving TE to make any distinctions based on the received priority of a TPDU. The received priority value is not negotiated, so the receiving TS-user may or may not choose to modify its processing based on the indicated value of priority for a TSDU.

4.1.3.4.1.2.4 Security.

The value of the security parameter specified by the service user is used as the value of the NS security parameter for the N-UNITDATA that contains the UD TPDU.

4.1.3.4.2 Use of the N-UNITDATA Indication

The transport layer receives all UD TPDUs via the N-UNITDATA indication. TPDUs are contained within the NS-user-data parameter of the N-UNITDATA indication.

4.1.3.4.2.1 Scope and Applicability

These procedures apply to UD TPDUs that may be received by the transport layer.

4.1.3.4.2.2 Procedure

4.1.3.4.2.2.1 NS-user-data.

The transport layer assumes that the UD TPDU begins at the first octet of the NS-user-data.

4.1.3.4.2.2.2 Network Service Access Point Addresses.

The source and destination NSAPs are used to determine the source and destination transport addresses associated with a TPDU. With the CLTS, transport addresses are determined by combining the NSAPs with the appropriate TSAP selectors, which are contained in the header of the UD TPDU.

4.1.3.4.2.2.3 Network Quality of Service.

The connectionless mode transport layer does not need to interpret most of the indicated network QOS parameters associated with an N-UNITDATA indication, except for the network priority parameter. The network layer protection parameter is not used. The

relative rankings of transit delay, residual error, and cost are after the fact, and do not have any effect on the transport protocol.

The CLTP must interpret the indicated network layer priority to determine the associated transport layer priority, since priority is not passed. See Table A5-1 to map NL priority to TL priority.

Another parameter passed in the indicated network layer QOS is the flag for the presence of congestion. For each NSDU delivered to the transport layer, the network layer must indicate whether the CE flag was set for any NPDUs associated with the NSDU. The presence of this condition indicates that there is congestion between the source and destination ESs. Because the CLTP does not implement flow control mechanisms, there is little that can be done to treat the congestion. Some metering function could be implemented to reduce the rate of TSDUs submission by a local TS-user.

4.1.3.4.2.2.4 Security.

The value of the security parameter received in an N-UNITDATA indication is provided to the TS-user with the received TSDU.

4.2 CLNP Implementation Considerations

4.3 IDRP Implementation Considerations

4.4 ES-IS Implementation Considerations

4.4.1 Protocol Selection

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 11.2).

4.4.1.1 Protocol Overview

ISO 9542 operates among the systems attached to a single SN, independently from the routing organization. It is used to allow systems on the SN 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 11-1, Table 11-2, Table 11-3 and Table 11-4 respectively indicate:

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 SN destination addresses are possible:

I. "All ESs network entities", or

II. "All ISs network entities".

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 SN, and all the ISO 9542 PDUs generated by each IS are sent to all the ESs on the same SN.

Table 11-1: ISO 9542 PDU Types

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 SN 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 SN) to which the redirected PDUs will be sent for the first hop from the ES (better path to destination)

Table 11-2: Generation of ISO 9542 PDUs

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 11-3: Propagation of ISO 9542 PDUs

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 SN
ISH	Transmitted on each SNPA the IS is attached to Transmitted to all the ESs on each SN 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 11-4: Role 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 SN, along with the NSAPs this ES supports Allows the ESs to discover the existence and reachability of another ES on the same SN, 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 SN 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 SN along with the NET of this IS
RD	**ROUTE REDIRECTION** Allows an IS to inform the source ES (on the SN) of a better path to reach a destination NSAP (by indicating another IS corresponding to a better first hop on the same SN, or directly the destination ES if it is on the same SN) It may also relate to a "class" of NSAPs (using Address Masks)

4.4.1.2 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.

4.4.1.2.1 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.

4.4.1.2.2 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.

4.4.1.2.3 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-initialization).

4.4.1.2.4 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.

4.4.1.2.5 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.

4.4.1.2.6 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.

4.4.1.2.7 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.

4.4.1.2.8 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.

4.4.1.2.9 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.

4.4.1.2.10 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-initialization).

4.4.1.2.11 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.

4.4.1.2.11.1 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.

4.4.1.3 ISO 9542 Operation Among ESs

When ISO 9542 is used among the ESs of a single SN, the ESH PDUs are transmitted with the same destination SN 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 optimization, namely by anticipating the information contained in the RD PDUs, when the destination NSAP is supported by an ES on the same SN.

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

4.4.1.4 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 SN, the ISs validate the reception of the ISHs normally destined for the ESs, by validating the corresponding SN address ("All ESs").

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

4.4.2 ISO 9542 Operation over Fixed Ground Subnetworks

4.4.2.1 Generalities

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 fulfill the following requirements :

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

2. the NSAP and SNPA addresses of neighbor ESs and the NET and SNPA addresses of neighbor 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 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.

4.4.2.3 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.

4.4.2.4 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.

4.4.3 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 initialization phase is triggered so that communication can be established between peer ground and airborne routers.

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

As already discussed in Chapter 6, this action is performed via the exchange of an ISO 9542 ISH PDU.

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 4-1 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

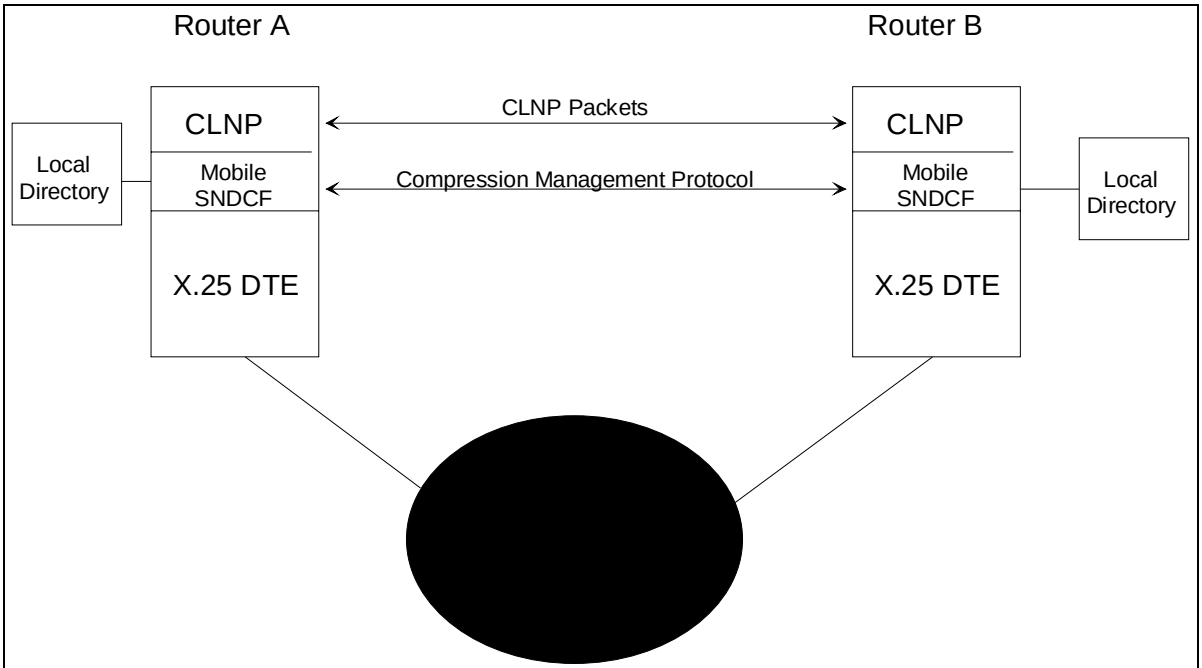

Figure 4-1 Implementation Model of the Mobile SNDCF

mode data link.

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.

4.5.2.3 Congestion Management

4.5.2.4 Priority Mapping

5. Guidance for ATN Service Providers

5.1 The Role of an ATN Service Provider

5.2 Interconnection with other ATN Service Providers

5.3 Interconnection with Ground Based Service Users

5.4 Interconnection with Mobile Users

5.5 Allocation of Addresses to Service Users

5.6 Provision of Default Routes to Mobile Systems

6. Guidance for ATM Application Designers

6.1 The ATN Transport Service

6.2 The Quality of Service Available

6.3 Using Security, QoS Maintenance and Priority Parameters