ATNP/WG2/
WP/234
31 January 1996

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Brisbane 5.2.96-9.2.96

Proposed Guidance Material for Section Four of the ATN Internet SARPs Guidance Material (Part 1 - Transport Layer)

Presented By Henk Hof

Prepared by Tony Whyman

SUMMARY

Action 6/32 required the author to edit the proposed section four guidance material and to present the result to the next meeting. This paper completes part of that action, and provides the guidance material specific to the transport layer. This has been based upon chapter eight of the ATN Manual, and includes new material to bring it up-to-date with recent changes to the SARPs.

DOCUMENT CONTROL LOG

SECTION	DATE	REV. NO.	REASON FOR CHANGE OR REFERENCE TO CHANGE
	31-Jan 1996	Issue 1.0	

TABLE OF CONTENTS

4. Guidance for ATN System Implementors

4.1 Types of ATN Systems

There are two types of ATN System: the End Systems, which host the ATN Applications; and the Intermediate Systems that are the ATN Routers. Within these two basic types there are many variations. For example, there are some End Systems that are located on board aircraft and are part of the aircraft's avionics. There are also End Systems that are located in ATC Centres or are part of an airline's operational ground systems, and are the computers that host operational ATC and Airline applications. An End System is essentially any computer system that is connected to the ATN and implements the communications protocols necessary to access the ATN.

There are also many different types of ATN Router. In aircraft, airborne routers will also be part of an aircraft's avionics, and on the ground, ATN Routers will support both ground-ground and air-ground data communications. The various types of ATN Routers are classified in chapter two of the ATN Internet SARPs.

An ATN End System is required to support the ATN Transport Protocol, and the End System provisions for the Connectionless Network Protocol. In addition, the End System must implement the access protocol required for the subnetwork through which it accesses the ATN, and may also need to support the ISO 9542 ES-IS protocol. Support of ISO 9542 will be necessary if this is required by the ATN Router(s) through which the End System accesses the ATN, is a local matter as far as the ATN Internet SARPs are concerned.

An ATN Router is required to support the Intermediate System provisions for the Connectionless Network Protocol and most classes of ATN Router also require support of IDRP, although the support requirements for IDRP do differ depending on the role of the Router. Local considerations may also require support of the ISO 9542 EI-IS protocol and/or the ISO 10589 IS-IS protocol. ATN Routers must also implement the access protocol required for each subnetwork to which they are attached, and those attached to air-ground subnetworks are, additionally, required to implement the Route Initiation procedure specified in chapter 3 of the ATN Internet SARPs.

The remainder of this chapter is concerned with providing guidance for ATN Systems Implementors on the:

- Implementation of the Transport Protocol;
- Implementation of the Connectionless Network Protocol (CLNP);
- Implementation of the Inter-Domain Routing Protocol (IDRP); and
- implementation of the routing protocols that are outside of the scope of the ATN Internet SARPs, but which are nevertheless often required to meet local requirements.

4.2 Transport Layer Considerations

4.2.1 The ATN Transport Layer

4.2.1.1 Transport Layer Model

The OSI Transport Layer supports the end-to-end exchange of data between end systems, and serves as an interface between the application and the upper layers, which deal with the exchange of

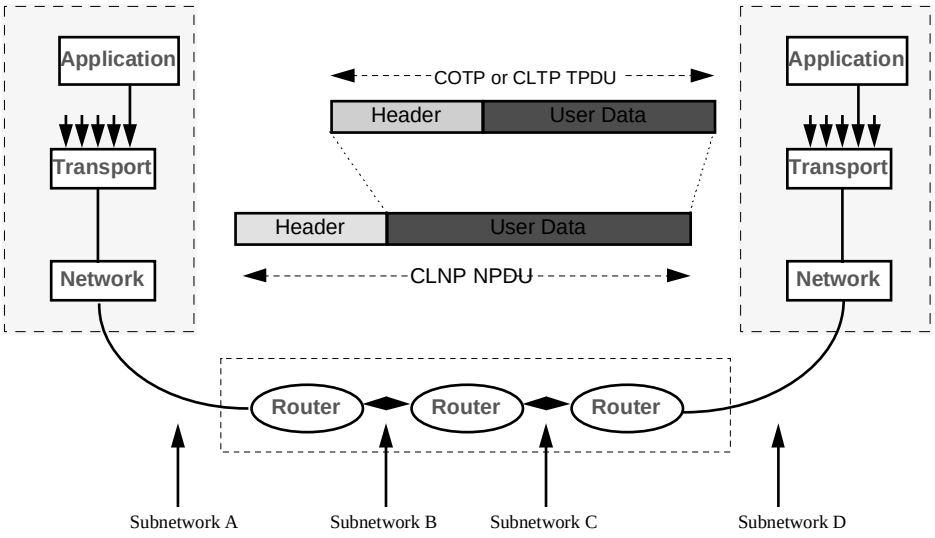

Figure 4-1 Scope of Transport Layer Interactions

application messages, and the lower layers, which provide the necessary transmission and routing capabilities (see Figure 4-1). 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).

TS-users receive a service which conceals the details in which reliable and cost effective transfer of data is achieved. This is achieved 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. TS-users may choose to use either of two modes of transport service:

- The Connection Mode Transport Service (COTS), or
- The Connectionless Mode Transport Service (CLTS).

4.2.1.2 Transport Layer Protocols

The Transport Layer may consist of one or several transport entities, each implementing a different transport protocol. Two transport protocols are specified for use in ATN End Systems,: the Connection Oriented Transport Protocol (COTP) and the Connectionless Transport Protocol (CLTP). The COTS is support by the COTP and the CLTS by 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 only the COTS, then that ES does not need to implement the CLTP.

Both protocols support the exchange of application messages, henceforth referred to as Transport Service Data Units (TSDUs), while transferring each TSDU as one or more Transport Protocol Data Units (TPDUs), using the service provider by the ATN Network Layer.

- The **COTP** provides to its users an end-to-end connection mode service (i.e. the COTS), and is a conformant subset of the Class 4 Transport Protocol (TP4) specified in ISO 8073. This

enables the reliable sequenced data transfer, where the user is guaranteed the byte order to data is preserved and that if a given TSDU is delivered then all previous messages will have been delivered. Both data integrity and data sequence integrity are supported by the COTP, together with end-to-end flow control.

- The **CLTP** provides a connectionless transport service (i.e. the CLTS), where no service guarantees are offered, other than preservation of the data integrity of each TSDU. Each CLTP TSDU is transferred as an event unrelated to the transfer of any other message and there is no guarantee either of delivery or that a TSDU may not overtake an earlier TSDU. The CLTP is conformant with ISO 8602.

4.2.1.3 Service Provided by the ATN Transport Layer

ATN Applications may choose to use either the COTS or the CLTS. The selection of the transport service used by an application is influenced by the communications characteristics and the quality of service requirements of that application. However, the choice of which mode to use cannot usually be left to the implementor. This must be specified by the application specification. It is the implementor's responsibility to implement the transport protocol necessary to support an End System's applications' requirements.

4.2.1.3.1 Service Provided by the COTS

As far as application designer's are concerned, the COTS 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 also appropriate for applications that place a higher importance on data sequence integrity than transit delay. The characteristics of the service provided by the connection mode protocol include the following:

- TS-users negotiate the establishment of a transport connection, prior to actual data transfer; 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 utilised for data acknowledgements, flow control purposes and keep-alive indicators.

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

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

- The underlying protocol is capable of segmenting TSDUs, allowing TSDU sizes larger than the maximum NSDU size. 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 underlying 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.

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

4.2.1.3.2 Service Provided by the CLTS

The CLTS is appropriate 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.

4.2.1.4 Transport Addresses

Users of the Transport Service are uniquely identified by their Transport Address (TSAP Address).

A TSAP address comprises two elements, an 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 that it is possible for the COTP and CLTP to share a common NSAP Address. However, if the End System supports other Transport Protocols (e.g. TCP), then these must use different NSAP Addresses.

4.2.1.5 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. NSDU loss is only expected during times of network congestion, when NPDUs are discarded by congested routers.

4.2.1.6 ATN Security and Priority

The ATN SARPs specify the use of an ATN Security Label and the prioritisation of data. In the COTP an ATN Security Label applies to a transport connection rather than an individual TSDU, and all TSDU sent over a given transport connection must have the same ATN Security Label. On the other hand, in the CLTP, each TSDU may be assigned a separate ATN Security Label.

Similarly, in the COTP, a transport connection is given a priority, and all TSDUs sent over that transport connection have the same priority, while, in the CLTP, each TSDU may have a different priority.

The ATN Security Label and priority applicable to each TPDU are parameters of the N_UNITDATA service and are therefore encoded in the NDPU header, rather than each TPDU, and are referenced by the network layer forwarding function. For such reasons, TPDUs from transport connections with different ATN Security Labels, and/or priorities, cannot be concatentated.

4.2.2 Provision of the Connection Mode Transport Service

4.2.2.1 Overview

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 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. Each user of a TC is provided with the COTS.

The COTS may exist in four possible states: idle, connection establishment, data transfer, and connection release. In the idle state, there is no connection and data transfer cannot take place. In order to transfer data, a transport service user must request that a transport connection is established with the required remote transport service user, identified by its Transport Address. While an attempt is made to establish a transport connection, the COTS enters the connection establishment state.

During the connection establishment state, the transport entity attempts to establish contact with the remote transport service user. If it is successful, and the remote user agrees to the connection, then a transport connection is established, the data transfer state is entered, and data transfer may take place. If it is not successful then the COTS returns to the idle state.

Either user of a transport connection may, at any time, request that the transport connection is released. The COTS then enters the connection release state. This is only a transitory state as the connection is always released immediately the request is made with any in-transit data lost - it is the responsibility of the transport service users not to release the connection before all data has been transferred. The idle state is then re-entered.

The COTS is realised through the implementation of the COTP.

The ATN COTP uses the ISO 8073 class 4 procedures and is therefore 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.

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.

4.2.2.2 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 4-2 gives a summary of TS-primitive time-sequence diagrams for some typical scenarios.

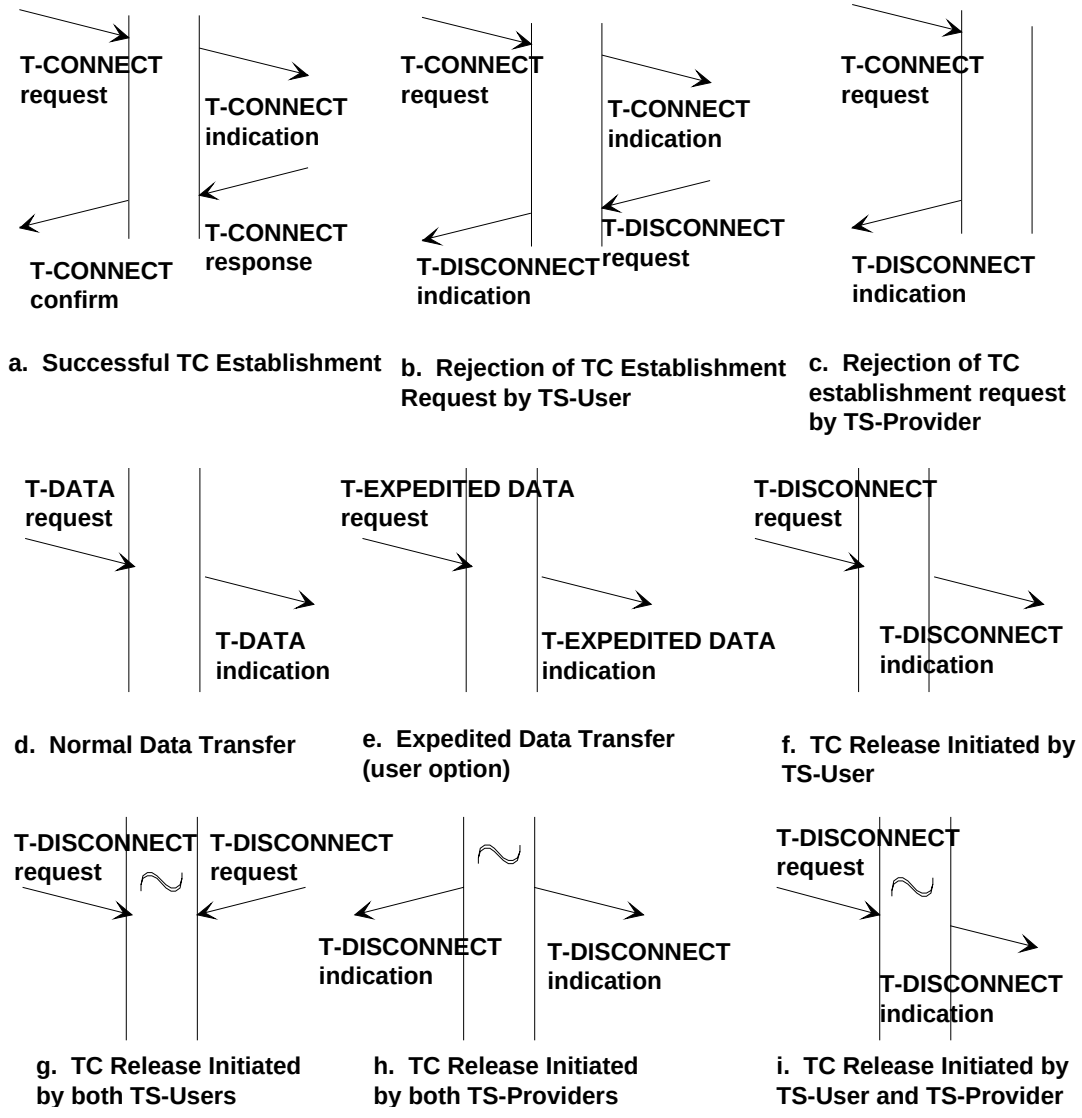

Figure 4-2 Transport Service Time Sequence Diagrams

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 4-2, *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 4-2 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.

4.2.2.3 The Connection Mode Transport Protocol (COTP)

4.2.2.3.1 Overview

COTP procedures support 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 as connection establishment. Timer-based mechanisms are, for example, used by the sender and receiver keeping track of the system state long enough to ensure that all PDUs from closed connections have left the system.

The handshake and timer-based mechanisms are combined to ensure that connection identifiers are

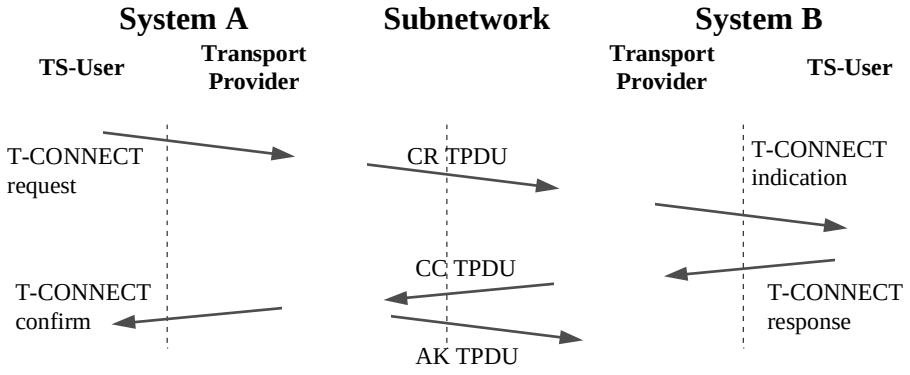

Figure 4-3 TPDU Exchanges for Connection Establishment

unique during the maximum time packets may remain in the system.

4.2.2.3.2 Connection Establishment

The COTP uses a three-way handshake mechanism in combination with a timer-based mechanism to ensure connection establishment in class 4. Figure 4-3 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 (CC) 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 4-4.

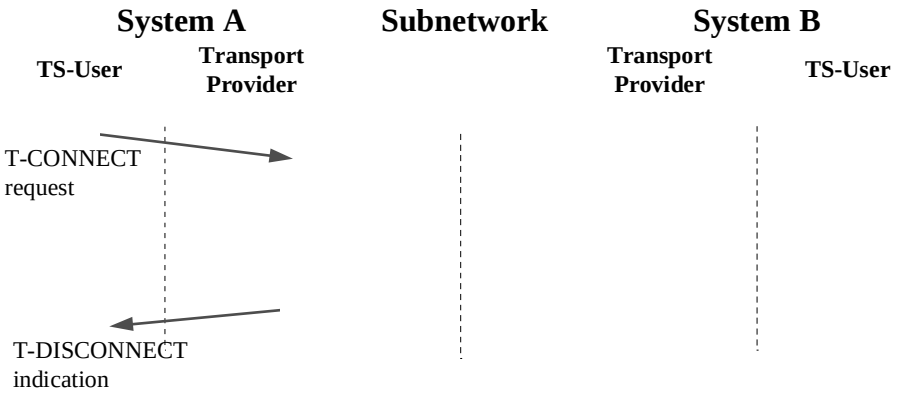

Figure 4-4 Connection Refusal by the TS Provider

To initiate communication with a peer, a TS-user invokes the T-CONNECT request primitive (see Figure 4-2). 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 4-1.

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:

- 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 4-2), 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 4-2).

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.

4.2.2.3.2.1 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).

- **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

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(=)

Note: in the above table:

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*

Table 4-1 TC Establishment Primitives and Parameters

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 the ATN Internet SARPs..

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.*

4.2.2.3.2.2 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.

4.2.2.3.2.3 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 Figure 4-4). The associated parameters and their corresponding values are the same as in the T-CONNECT request.

4.2.2.3.2.4 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.

4.2.2.3.3 Data Transfer

Once a connection has been successfully opened data transfe may take place. Normal data transfer is always full duplex with independent flow control in each direction. The Quality of Service is assumed to be the same in each direction.

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 acknowledgement timer set or reset after receipt of data expires. The acknowledgement timer mechanism enables multiple TPDUs to be acknowledged with the same AK TPDU. An example of normal data transfer is shown in Figure 4-5, 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 acknowledgement timer, an AK is returned. This AK acknowledges up through the final TPDU.

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. Figure 4-2(d) describes the primitive sequences in a successful transfer of normal data.

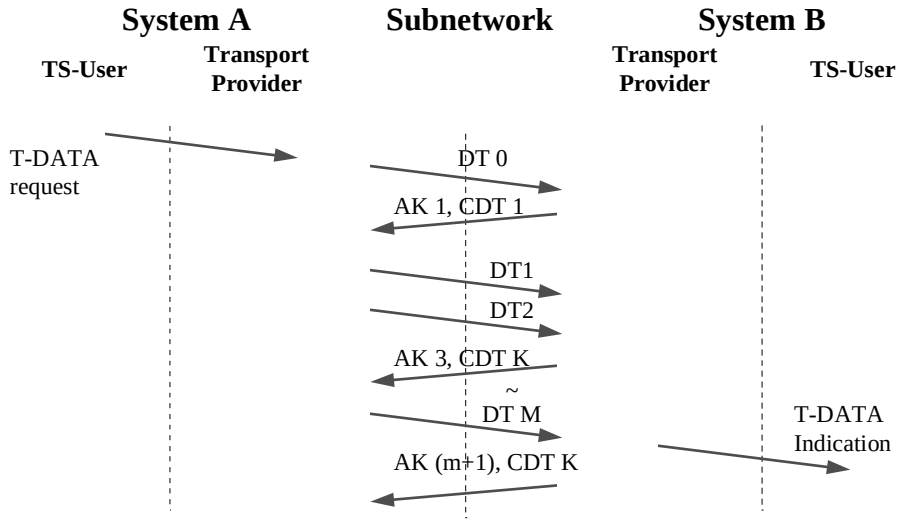

Figure 4-5 Normal Data Transfer

4.2.2.3.3.1 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.

4.2.2.3.3.2 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.

4.2.2.3.4 Expedited Data Transfer

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. Figure 4-2 (e) shows the sequence of primitives in a successful transfer of expedited data.

4.2.2.3.4.1 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 .

4.2.2.3.4.2 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.

4.2.2.3.5 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 4-2 (f) through (i).

The first scenario (f), is shown in more detail in Figure 4-6. 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 Figure 4-2 (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.

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 summarised in Table 4-2.

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

Note: in the above table:

M *The parameter is mandatory*

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

Table 4-2 TC Release Primitives and Parameters

4.2.2.3.5.1 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.

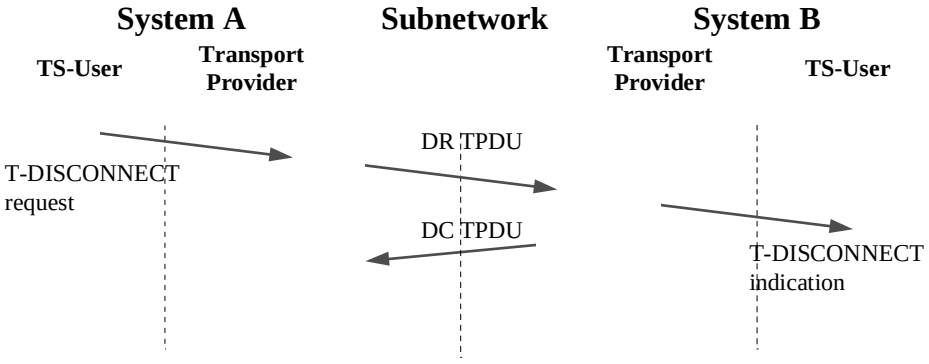

Figure 4-6 Transport Connection Termination

4.2.2.3.5.2 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 4-2), or if TS-users initiate a T-DISCONNECT request simultaneously (see part (g) of Figure 4-2). 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, misbehaviour of the TS-provider, called TS-user unknown, or called TS-user unavailable (if the release occurs during the connection establishment phase).

4.2.2.4 The ATN Security Label

ATN Security Functions are concerned with:

a) Protecting CNS/ATM applications from internal and external threats;

b) Ensuring that application Quality of Service and Routing Policy Requirements are maintained, including service availability; and,

c) Ensuring that air-ground subnetworks are used in accordance with ITU requirements.

The ATN Internet provides mechanisms to support items (b) and (c) above only. These mechanisms are defined to take place in a common domain of trust, and use a Security Label in the header of each CLNP Data PDU to convey information identifying the “traffic type” of the data and the application’s routing policy and/or strong QoS Requirements. Strong QoS Requirements may only be expressed by ATSC Applications, and they are expressed as an ATC Class identifier, encoded as part of the ATN Security Label.

Except when a transport connection is used to convey general communications data, each transport connection is associated with a single ATN Security Label. The value of this label is determined when the connection is initiated, and by the initiating TS-User. A responding TS-user may refuse to accept a transport connection associated with a given ATN Security, but cannot propose an alternative. It is also not possible to change an ATN Security Label during the lifetime of a transport connection.

The ATN Security Label is never actually encoded into a TPDU header. Instead, every NSDU passed to the Network Layer that contains a TPDU from a transport connection associated with an ATN Security Label is associated with the same ATN Security Label. This is passed as a parameter to the N-UNITDATA request, and then encoded into the NPDU header.

TPDUs from transport connections associated with different ATN Security Labels cannot be concatenated into the same NSDU.

Note. The mechanism by which the connection initiator specifies the appropriate ATN Security Label for a given transport connection is a local matter. For example, it may be identified by an extension to the transport service interface, be implicit in the choice of a given TSAP, or be identified using a Systems Management function. Similarly, the mechanism for determining the ATN Security Label associated with an incoming transport connection is a local matter.

4.2.2.5 ATN 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. However, there are practical difficulties in a connectionless internet, as regards dynamic route selection based on differential QoS requirements. While dynamic route selection is still a long term goal, in the near to medium term, application QoS requirements will be met through the following principles:

a) The capacity requirements of CNS/ATM-1 Applications will be met through a combination of network design and capacity planning, in order to ensure that network capacity both exists and is usable by CNS/ATM-1 Applications, and that their QoS Requirements will be met to the required availability.

b) The strong QoS Requirements of certain ATSC Applications will be met, without having to design the whole ATN to meet their QoS requirements, by reserving certain subnetwork paths for applications data of at least a given ATSC Class, as identified by the ATN Security Label associated with the data.

c) The strong QoS Requirements of certain AISC Applications will be met by respecting routing policy requirements, restricting their data to travel over only certain air/ground data links, expressed in the ATN Security Label associated with the data.

The only exception to this is *Residual Error Rate*. The ATN Internet provides an expected residual error rate of 1 in 10^8. This may be improved upon through use of the transport protocol checksum mechanism, and it is believed that with this additional mechanism, an undetected error rate of 1 in 10^{13} is achievable. 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. However, the checksum is essential for ensuring protection against undetected errors.

4.2.2.6 Priority

Although priority is defined by ISO 8072 to be part of QoS, it is important enough in the ATN to be treated separately.

The purpose of priority is to signal the relative importance and/or precedence of data, such that when a decision has to be made as to which data to action first, or when contention for access to shared resources has to be resolved, the decision or outcome can be determined unambiguously and in line with user requirements both within and between applications. In the ATN, priority is signalled separately by the application in the transport layer and network layer, and in ATN subnetworks. In each case, the semantics and use of priority may differ.

In the ATN Internet, priority has the essential role of ensuring that high priority safety related data is not delayed by low priority non-safety data, even when the network is overloaded with low priority data.

In the ATN Transport Layer, priority is concerned with the relationship between transport connections and determines the relative importance of a transport connection with respect to (a) the order in which TCs are to have their QoS degraded, if necessary, and (b) the order in which TCs are

to be broken in order to recover resources. The transport connection priority is specified by the initiating TS-user either explicitly or implicitly, when the transport connection is established. As with the ATN Security Label, priority is not negotiable, and a responding TS-user must either accept the proposed priority or reject the connect request. TPDUs belonging to transport connections with different priorities cannot be concatenated.

When an ATN Transport Layer entity is unable to satisfy a request for a transport connection from either a local or remote TSAP, and which is due to insufficient local resources available to the transport layer entity, then it is required to terminate a lower priority transport connection, if any, in order to permit the establishment of a new higher priority transport connection.

Transaport Layer implementations may also use transport priority to arbitrate access to other resources (e.g. buffers). For example, this may be achieved by flow control applied to local users, by discarding received but unacknowledged TPDUs, by reducing credit windows, etc.

All TPDUs sent by an ATN Transport Layer Entity are transferred by the ATN Internet Layer, using the Network Priority that corresponds to the transport connection’s priority according to Table 2-3 of the ATN Internet SARPs. The network priority is signalled by a parameter to the N-UNITDATA request, and the priority of an incoming NSDU is signalled by a parameter to the N-UNITDATA indication.

Transport Priority may be encoded into the CR TPDU. However, this is not essential and, if present must be equivalent to the network priority of the NSDU that conveys the CR TPDU. The priority of this NSDU determines the priority of the transport connection.

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 chapter 2 of the ATN Internet SARPs for further details on the mapping of Transport priority values to CLNP priority values).

4.2.2.7 Negotiation of Connection Parameters

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 4-3 indicates the items that can be negotiated and their default, or mandatory, values in 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

Table 4-3 Negotiable and Default Values for Class 4 Operation

4.2.2.7.1 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.

4.2.2.7.2 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.

4.2.2.7.3 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.

4.2.2.7.4 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.

4.2.2.7.5 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 4-3.

4.2.2.7.6 Non-use of Checksum

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 realised.

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.

4.2.2.7.7 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 retranslating 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 4.2.2.10.4.3 for a description of the selective acknowledgement feature.

4.2.2.7.8 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.

4.2.2.8 Error Handling

4.2.2.8.1 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); or,
- The transport layer can discard the TPDU (that is, ignore the error).

Events which qualify as a protocol error are defined in ISO 8073. It is recommended that in event of a protocol error, that the transport layer issue an ER TPDU, and either discard the TPDU, or respond with a DR TPDU. This action ensures that the cause of a protocol error can be more readily identified.

4.2.2.8.2 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.

ISO 8073 requires that, on receipt of an undefined parameter, 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 recognise 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 established which operates without using selective acknowledgement.

If a recognised parameter has an invalid value, then an implementor may either ignore the error or declare a protocol error, at their own discretion. However, 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.

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

For all other TPDUs, the decision s to 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 may either:

a) discard the TPDU silently;

b) issue an ER TPDU and either discard the TPDU or issue a DR TPDU; or,

c) immediately issue a DR TPDU.

4.2.2.9 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 optimised 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 4-4 *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.— In Table 4-4, 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.

Note 4- The example values in Table 4-4 have not been subject to validation and are for illustrative purposes only.

Several of the timers and variables listed in Table 4-4 are not directly configurable, but may be determined based on the values of other timers and variables. That is:

- 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

Symbol	Name	Minimum	Example	Maximum
M_{RL}, M_{LR}	NSDU Lifetime, seconds	5	40	135
E_{RL} + E_{LR}	Maximum Round-trip 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

Table 4-4 Example Timer and Parameter Values and Ranges

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 minimised. 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.

4.2.2.10 Transport Layer Protocol Conformance

This section provides background information and notes on the APRLs 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 specified in the ATN Internet SARPs, which is derived from the PICS Proforma provided with ISO 8073. ATN specific extensions are also included in the APRL.

4.2.2.10.1 Base Standard

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

During the development of the APRL, an important objective was to ensure backwards compatibility with ISO 8073: 1988, whilst permitting the use of the following features of the 1992 version which do not exist in the 1988 version:

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

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

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

4. The inactivity time is now specified as two values, 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.

4.2.2.10.2 Caveat to Conformance with Base Standard

The ISO 8073 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 as a connection mode network service is not provided. In respect of this item, ATN conformant implementations of ISO 8073 are therefore not necessarily in conformance with ISO 8073.

4.2.2.10.3 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.

4.2.2.10.4 Notes on Required and Recommended Optional Functions

4.2.2.10.4.1 Extended TPDU Numbering

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 4.2.2.9). 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.

4.2.2.10.4.2 Non-use of Checksum

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. These are a local metter. The use or non-use of checksums is dependent on the characteristics of the TS-user-data flow.

4.2.2.10.4.3 Selective Acknowledgement

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.

4.2.2.10.4.4 Request of Acknowledgement

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.

4.2.2.10.4.5 Reduction of Credit Window

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

4.2.2.10.4.6 Concatenation

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.

4.2.2.10.5 Notes on TPDU Support

4.2.2.10.5.1 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.

4.2.2.10.5.2 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 left as a local matter.

However, it can be very useful in providing diagnostic information, and has the added advantage that it makes clear which side of the transport connection detected the error and hence which implementation is the probable source of the error.

4.2.2.10.6 Notes on TPDU Parameter Support

4.2.2.10.6.1 Optional Parameters for the CR 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. The optional parameters for which ATN specific recommendation have been made are:

- **The called and calling TSAP-ID** parameters: Support is required in order 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.

- **TPDU size parameter**: 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 recognised, the maximum TPDU size will be the default value, 128 octets. Furthermore, 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. 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.

- **Preferred Maximum TPDU Size:** Support is recommended. 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

- **Version Number Parameter**: Support 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.

- **Protection Parameter:** Support is not currently recommended as no security mechanisms have been defined for the ATN besides use of the ATN Security Label, which is outside of the scope of this parameter. Use of this feature may be specified in later versions of the CNS/ATM SARPs, if a need for lower layer protection mechanisms had been identified.

- **Additional Option Selection Parameter:** The additional option selection parameter must be supported in a transport layer implementation, in order to allow negotiation of several transport layer optional functions.

- **Residual Error Rate And Transit Delay Parameters**: Support is not recommended for transport layer implementations, as these are design parameters of connectionless networks and cannot readily be selected dynamically.

- **Priority Parameter:** Support 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, as it is used to ensure that high priority (i.e. flight safety related data) is never impeded by lower priority, 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 recommendation in the ATN SARPs 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 in preference to 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 ATN Subnetwork Service Providers.

- **Acknowledgement Timer and Inactivity Time Parameters:** Support is recommended for both. These two parameters allow transport entities to better manage transport resources, and may be implicitly required in order to support applications (e.g. ADS) that demand well defined bounds on either data delivery, or an indication of transport connection less.

4.2.2.10.6.2 Optional Parameters for the CC 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.

4.2.2.10.6.3 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.

4.2.2.10.6.4 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.

4.2.2.10.6.5 Optional Parameters for an Acknowledgement TPDU.

The flow control confirmation parameter (index I4AK4) is recommended for ATN implementations of the transport layer.

4.2.2.10.6.6 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.

4.2.2.10.6.7 Use of the Selective Acknowledgement Parameter in the AK TPDU

Support of this parameter is recommended for transport layer implementations. If selective acknowledgement has been selected for a given TC, then this parameter is optional in an AK TPDU.

4.2.2.10.6.8 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.

4.2.2.10.6.9 User Data in Class 4 TPDUs

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.

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.

4.2.2.11 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.

4.2.2.11.1 Use of the N-UNITDATA Request

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.

The N-UNITDATA parameters are used as follows:

4.2.2.11.1.1 NS-user-data.

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

4.2.2.11.1.2 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.

4.2.2.11.1.3 Network Quality of Service.

4.2.2.11.1.3.1 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; or,

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

The ATN effectively implements option (b) by passing the ATN Security Label to the network layer, as the protection parameter.

The value of the ATN Security Label specified by the connection initiator on the connect request, is used as the value of the NS protection parameter for the N-UNITDATA that contains the CR TPDU. The same value is then 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.

4.2.2.11.1.3.2 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 Network Layer QoS parameters can be done by configuration or dynamically.

However, general support of the network layer QoS parameters is not expected in the near to medium term. They may be specified by the sending transport layer, but are ignored by the network layer.

4.2.2.11.1.4 Network Layer Priority

When specified, the transport priority parameter has 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. The relationship between transport priority and network priority is specified in chapter 2 of the ATN Internet SARPs.

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.

4.2.2.11.2 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.

The parameters of an incoming N-UNITDATA indication are interpreted as follows.

4.2.2.11.2.1 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 assumes that there are one or more TPDUs following the first one.

4.2.2.11.2.2 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.

4.2.2.11.2.3 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, expect for the protection parameter conveying the ATN Security Label. 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 need not be interpreted by the transport layer.

The value of the protection parameter received in an N-UNITDATA indication is interpreted as the ATN Security Label, and saved by the TS-provider and used with all subsequent N-UNITDATA requests on that transport connection.

4.2.3 The Connectionless Mode Transport Layer

The ATN CLTS is based on the ISO 8072/AD1 Standard Service Definition, and 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.

4.2.3.1 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. By avoiding

the overhead of transport connection establishment and connection management, it is possible to speed up the data exchanges and reduce transit delays of short TSDUs. 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); and,

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.

4.2.3.1.1 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.

4.2.3.1.2 Data Transfer

The data transfer procedure is used for one-shot, 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 TSDUs (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 fulfil 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).

4.2.3.1.3 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 behaviour 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' behaviour. 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.

4.2.3.2 ATN Connectionless Mode Transport Layer Quality of Service

4.2.3.2.1 Use of Transport Layer QoS

The use of transport layer QoS parameters for the CLTS is similar to that of the connection-mode service. However, 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.

4.2.3.2.2 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.

As with the connection mode, transit delay is not used, and, if specified, will be ignored. Two levels of residual error rate are provided, equivalent to use and non-use of the transport checksum. Both a priority and an ATN Security Label may be specified on a per TSDU basis.

4.2.3.2.3 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.

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. Chapter 2 of the ATN Internet SARPs specifies the mapping of transport layer priority values to network layer priority values.

4.2.3.2.4 ATN Security Label

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 the ATN Internet SARPs.

4.2.3.3 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 sequence of primitives in a successful CLTS transmission is defined in Figure 4-7.

4.2.3.3.1 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.

- **Quality of service:** The value of the QoS is a list of subparameters. The subparameters composing the CLTS QoS are presented in 4.2.3.2.1. The TS-provider does not guarantee that it can offer the requested QoS.

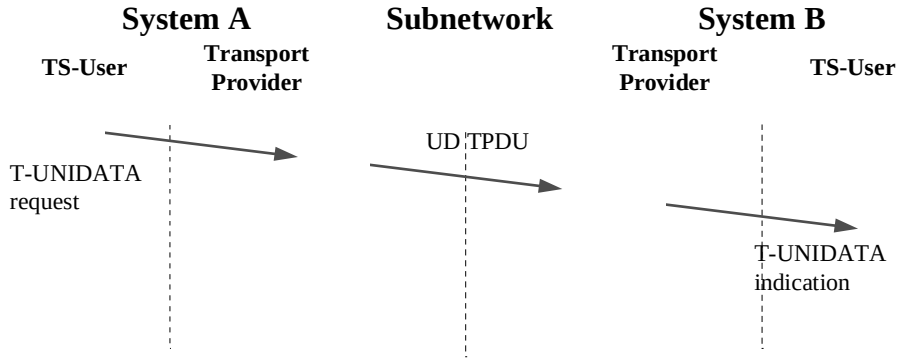

Figure 4-7 Sequence of Primitives and TPDU Exchange for Connectionless Data Transfer

- **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 the ATN Internet SARPs.

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.

4.2.3.3.2 T-UNITDATA Indication

Upon arrival at the destination TSAP, 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.

4.2.3.4 Use of the Network Service

Note.— Refer to 4.2.2.11.1 for more background on selection of requested network layer QoS parameters.

4.2.3.4.1 Use of the N-UNITDATA Request

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. The N-UNITDATA parameters are used as follows:

4.2.3.4.1.1 NS-user-data.

The transport layer sends the UD TPDU as an NSDU.

4.2.3.4.1.2 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.

4.2.3.4.1.3 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.

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 4.2.2.11.1.3.

The value of the ATN Security Label specified by the service user when invoking the T-UNITDATA service, is used as the value of the NS protection parameter for the N-UNITDATA that contains the UD TPDU.

4.2.3.4.1.4 Network Layer Priority.

There is no explicit priority parameter in a UD 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.

4.2.3.4.2 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. The N-UNITDATA parameters are interpreted as follows:

4.2.3.4.2.1 NS-user-data.

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

4.2.3.4.2.2 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.

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

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.

The value of the protection parameter received in an N-UNITDATA indication is provided to the TS-user with the received TSDU, as the ATN Security Label associated with the TSDU.

4.2.3.4.2.4 Priority

The CLTP must interpret the indicated network layer priority to determine the associated transport layer priority, since priority is not passed in the UD TPDU. See chapter 2 of the ATN Internet SARPs for the mapping between NL priority and TL priority.