EUROCONTROL

ATNP/WG2/WP/579
07/07/00 18:23

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Limerick 11.7.00 – 14.7.00

Proposed SARPs for the Frame Mode SNDCF

Presented By Tony Whyman

Prepared by Tony Whyman

SUMMARY

This paper provides the specification for a Mobile SNDCF designed to operate directly over a data link layer (a.k.a. frame mode service). The specification re-uses as much as possible from the existing Mobile SNDCF and especially re-uses the data compression components. Issue 2 also includes the simplified CLNP Header compression algorithm proposed for the VDL Mode 3 SARPs, aligned with the A/GCS.

TABLE OF CONTENTS

1. Introduction

1.1 Background

The specification of a "Frame Mode" for VDL Mode 3 is currently under way in the AMCP. This provides a minimal but efficient data communications service between an aircraft and a single ground system attached to a Ground Systems GNI. Provided that that Ground System is a router and that the data exchanged is routable (e.g. CLNP formatted packets) then this configuration is satisfactory for ATN operation.

However, the current ATN SARPs assume that the network access service for air/ground communications is compatible with the feature rich ISO 8208 specification. In order to use the simplified VDL Mode 3 frame mode, a new Mobile SNDCF will have to be developed.

1.2 Scope

This paper provides the specification for a Mobile SNDCF designed to operate directly over a data link layer (a.k.a. frame mode service). The specification re-uses as much as possible from the existing Mobile SNDCF and especially re-uses the data compression components.

Issue 2 also includes the simplified CLNP Header compression algorithm proposed for the VDL Mode 3 SARPs, aligned with the A/GCS.

1.3 Summary

The specification proposed in this paper incorporates the following features:

1. It can operate over any reliable data link communications service including the acknowledge connectionless service provided by VDL Mode 3 and the VDL Mode 2 AVLC.

2. It incorporates features known to be missing from the current Mobile SNDCF concerned with the introduction of new functions in a backwards compatible manner.

3. It includes a new communications sublayer (the A/GCS) in order to support data link management and the multiplexing of different routable protocols (e.g. CLNP for ATN and IP for APC).

4. It supports maintenance of the Data Compression State across data link Handoffs.

5. It includes optional security features for data link authentication.

6. Deflate Dictionaries and re-synchronisation are supported.

7. Other Routable protocols such as IPv4 can also be supported.

8. It includes support for a simple CLNP Header compression algorithm only operated directly over the link layer. This is designed to be implemented by small aircraft (e.g. General Aviation) and to be compatible with the more advanced A/GCS i.e. a Ground Station can simultaneously support this algorithm and the more powerful A/GCS.

2. Design Approach to a new SNDCF

2.1 Issues

1. The design of the original Mobile SNDCF was predicated on an ISO 8208 base and was heavily influenced by it. The new Frame Mode SNDCF is predicated on a much more basic service, that of a simple data link service that can be either:

   - a unicast reliable data link service, or
   - a broadcast connectionless service.

   The unicast reliable data link service can be provided by an acknowledged connectionless service (data transfer with a "window of 1") or a connection mode data link service (data transfer with a "window of *n*"). However, in neither case is a packet level acknowledgement assumed to be an acknowledgement of safe delivery to a peer system; this permits ground level link layer relays in order to optimise the air/ground data link.

2. It is intended that the new Mobile SNDCF uses the existing data compression algorithms. These require

   1. firstly, a reliable communications service (on which the specification is predicated), but also
   2. a means to negotiate compression options and to provide for recovery in the event of data corruption. In short, there needs to be some aspects of a connection mode service in order to build and maintain a relationship between compressor and decompressor. This is especially true of Deflate, although it is possible to operate LREF in a true connectionless fashion – but only at the expense of regularly sending uncompressed CLNP PDUs.

3. There are also several proposed enhancements for Deflate that need to be taken into account and specifically:

   - Use of Deflate Dictionaries in order to speed the convergence of the compression algorithm to the optimal compression ratio.
   - Recovery from checksum errors by returning to the last received packet rather than restarting the compressor.

   There may also be a need to have separate dictionaries for different data types (e.g. AOC and ATC) because of the different characteristics of the data streams, and this in turn implies that multiple Deflate compressed data streams may have to co-exist. But only if there is a clear performance gain.

4. Recently, there has also been attention paid to the need for backwards compatibility when introducing new features and the new SNDCF must ensure that this can be done.

5. It has also been recently proposed that Deflate on its own can be as efficient as LREF+Deflate. However, this requires a re-ordering of the CLNP header parameters. In order to test this out, a data format will also be defined for "re-ordered CLNP Headers". If successful, this means that LREF will not be needed in the future for non-broadcast operations.

6. Support for broadcast data transfer is also a design goal.

Note.-There is currently no ATN requirement for broadcast operations. However, multicast communications is part of the current ATNP work programme and a broadcast data transfer mode may be used in support of such communications.

~~6~~7. The AMCP have indicated a desire for a minimal CLNP Header compression algorithm for use over a Frame Mode service and for small aircraft (e.g. General Aviation).

~~1.2~~2.2 Analysis

Considering the above, it is clear that (at least for non-broadcast use) there will have to be some sort of Data Link Management protocol to negotiate compression options and to maintain the data communications path.

Modern communications networks tend to use an "out-of-band" approach to data link management. This is true of Frame Relay, Asynchronous Transfer Mode and ISDN. This technique ensures independence between data link management and data transfer and enables a very lightweight protocol approach to data transfer. It is proposed to adopt a similar approach to the data link management protocol required here. This should simplify the specification and be bandwidth efficient.

However, no out-of-band communications service is readily available from (e.g.) VDL Mode 3. Therefore, there is a need to provide for this by some sort of frame level protocol. The proposal is thus:

1. The air/ground data stream is subdivided into a number of individually prioritised bi-directional "logical channels", each identified by a channel number.

2. Data packets including data link management packets are always sent in the context of a logical channel i.e. they are encapsulated with a simple header identifying the channel and priority.

3. Subject to maintaining the semantics of data priority, packets sent on different channels may be concatenated and sent as a single transmission frame.

4. A Data Link Control Protocol (DLCP) is specified in order to negotiate data link capabilities and compression options, and to manage the purpose and use of each channel. Channel zero is reserved for the DLCP.

5. A channel assignment can specify that the data packets are Deflate compressed before transmission on a given channel. It is also possible to have multiple Deflate compressors with different groups of channels assigned to different compressors.

The channel concept is thus first to separate out the DLCP from user data and secondly allows for different Deflate compressed streams to be multiplexed together. It is also extensible as it permits other compression protocols to be introduced later (e.g. ADCMP for audio compression) and used in parallel to Deflate on other channels. Some channels (in addition to channel zero) could also be uncompressed, if that was needed.

The specification also deliberately groups multiple channels together for compression as a single data stream. This is done to ensure the most efficient compression while still allowing the channel concept to be used to differentiate different data streams. Essentially, a Deflate Compressor becomes a Server asked to compress a packet before it is encapsulated with a channel header and appended to the transmission frame. The channel determines the choice of compression Server.

At least two user data formats are foreseen. These are ISH PDUs, and CLNP PDUs that cannot be LREF compressed – or more generally any ISO TR 9575 identifiable protocol – and either LREF compressed CLNP PDUs or CLNP PDUs with reformatted headers. However, the channel concept can readily extend to supporting other data formats including IP and even ACARS messages.

1.32.3 Architecture

The architecture of the proposed approach is really more than an SNDCF. As illustrated in Figure 2-1, it is proposed to break down the specification into two parts: the SNDCF proper and an Air/Ground Communications Sublayer (A/GCS). The A/GCS comprises the multiplexing of many logical channels, the DLCP and the Deflate compression (which operates across channels). The SNDCF itself is responsible for providing the SN-Service over the A/GCS and also incorporates LREF compression, which is CLNP specific.

The underlying Data Link Layer is assumed to provide:

- A unicast communications service that provides reliable delivery and preservation of frame transfer sequence order. It may thus be a connection mode service (e.g. VDL2 AVLC) in addition to the acknowledged connectionless service of VDL3.
- a broadcast ground to air unacknowledged connectionless service.
- Join and Leave events to signal contact with a new Ground Station/Aircraft, and loss of contact, respectively.

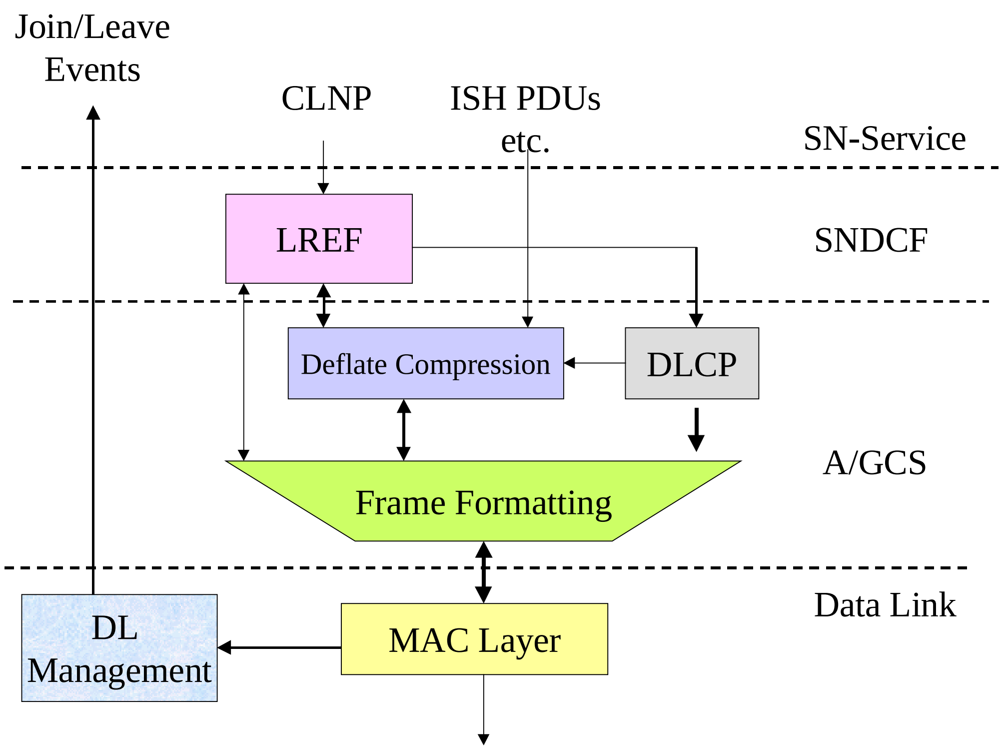

Figure 2-12-1 Proposed Architecture

The A/GCS provides a (DLCP supported) Data Link Management service to its user and a data communications service. The Data Communications service is channel oriented, with channel assignment performed through the Data Link Management interface. The data communications service is packet oriented and is guaranteed to maintain packet delivery order but does not guarantee to deliver all packets. The probability of packet loss is small but can come about (e.g.) through detection/recovery from a Deflate checksum failure.

The SNDCF provides the required SN-Service. It will use the A/GCS Data Link Management Service to maintain at least one channel for ISH PDUs, and CLNP PDUs that cannot be compressed using LREF. Otherwise, the SNDCF will use the A/GCS to assign a new channel for each local reference needed and use this channel to transfer LREF compressed CLNP PDUs associated with that Local Reference.

~~1.4~~2.4 Broadcast Mode

The underlying communications media typically support broadcast mode operations in the ground to air direction and the A/GCS and SNDCF are designed to permit seamless use of the broadcast service.

In broadcast mode:

- the DLCP is limited to channel assignment and channel assignments have a time limited validity i.e. they automatically lapse after a set period of time.
- LREF is supported.
- Broadcast Channel allocations are independent of unicast channel allocations.

Two purposes are foreseen for broadcast mode:

- The simultaneous uplink of an ISH PDU to multiple aircraft simultaneously.
- Broadcast/multicast of CLNP PDUs which are optionally LREF Compressed.

In the first case, it is expected that the Ground Station will allocate the channel and uplink the broadcast ISH PDU in a single frame for each broadcast that it performs. In the second case, it is expected that the Ground Station will only periodically re-allocate each LREF channel – as otherwise there will be no benefit from LREF compression given that the first packet has to be sent uncompressed.

The above means that every aircraft will always be able receive and process broadcast ISH PDUs, but on coming into range of a Ground Station, and aircraft will have to wait for channel re-allocation before being able to receive LREF compressed PDUs.

~~1.5~~2.5 Security

There are no clear requirements for subnetwork security as yet. However, VDL Mode 2 does appear to be especially vulnerable to a Denial of Service attack based on Ground Station or Aircraft masquerade and the general procedures for data link security have now been specified in subvolume 8 of the ATN SARPs. It thus appears reasonable to include the optional use of these procedures in this specification. The possible use of data link security and its implication can then be evaluated.

One possible benefit of data link security is that it means that IDRP is no longer being relied upon as the sole means of preventing such attacks and which "opens the door" to optimised versions of IDRP for air/ground use.

2.6 Support for CLNP Header Compression Only

The VDL Mode 3 draft SARPs currently contain a simplified CLNP Header compression algorithm for direct use over the VDL Mode 3 Frame Mode Service. This is similar to but not identical with the LREF Compression algorithm used in the ATN Mobile SNDCF. In particular:

1. The references are limited to 127 and are assigned separately in each direction
2. The security parameter is not included in the scope of a reference; only the NSAP Address pair.
3. Reference assignment is performed by replacing the Network Layer Protocol Identiifer octet in an uncompressed CLNP PDU by the assigned index.
4. The compressed header format is different.
5. Reference re-assignment is permitted dynamically as an unconfirmed service.

The AMCP has indicated that they want to retain the use of this basic compression algorithm to support low cost air/ground communications and in particular for General Aviation Aircraft. However, it is also necessary to support aircraft that have requirements that take advantage of the more powerful DEFLATE compression algorithm. This is particularly true of aircraft that support AOC communications.

The simple CLNP Header compression algorithm thus needs to be available as an alternative to the A/GCS and it should be possible for Ground Stations to support both concurrently. A Ground Station should be able to determine which compression method an aircraft uses by inspection of the first message received from it. This avoids being dependent on a subnetwork providing a means to negotiate the compression algorithm used.

The approach chosen is to use the first octet of the first frame downlinked as the means to determine the frame format. With the A/GCS this must always be zero; any other value implies an alternative frame format. This is because the first packet downlinked will always contain a DLCP packet on channel zero.

In VDL Mode3, the first octet in the frame is the payload octet and a value of zero is not assigned at present. This should remain the case. When the A/GCS is used with VDL Mode 3 there should be no payload octet and the A/GCS occupies the whole frame. With other formats (e.g. ISO8208, direct use of ISO8473) there is a payload octet as defined in the VDL Mode 3 SARPs.

3. Proposed SARPs for the Air/Ground Communications Sublayer (A/GCS)

3.1 General

Note.—This specification applies to mobile subnetworks having the following characteristics:

- *data packets are sent unicast over a data link layer service using either an acknowledged connectionless procedure that notifies the sender if the packet has been successfully delivered or not, or a connection mode service that guarantees delivery until failure is notified.*
- *The Data Link Service is assumed to have a low probability of packet loss or duplication.*
- *In the air to ground direction a single ground system receives all downlinks. In the ground to air direction, a specific aircraft is identified as the packet's destination.*
- *data packets are subject to a specified maximum packet size.*
- *unacknowledged ground to air broadcasts may also be supported.*

3.2 Architecture

Note 1.—The A/GCS communications model is that of a lightweight protocol dividing communications between a given aircraft and the ground system into a number of separate prioritised channels. One channel is reserved for control packets; the purpose of the remaining channels is determined through an exchange of control packets.

Note 2.—The architecture of the A/GCS is presented in Figure 3-1.

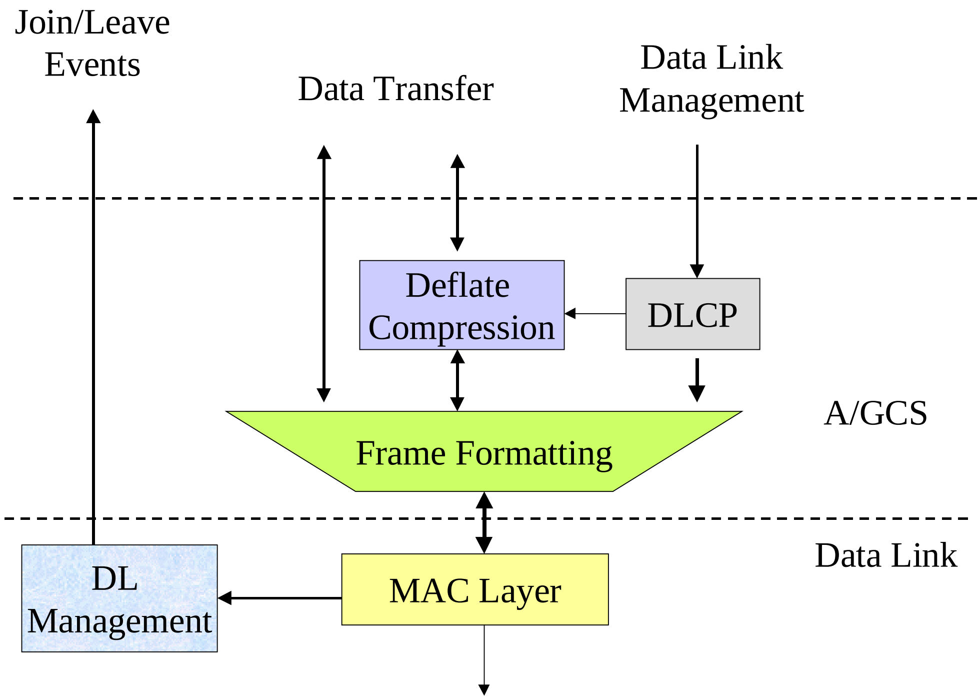

Figure 3-13-1 A/GCS Architecture

Note 2.—the A/GCS assumes direct access to a MAC layer communications service. A Data Link (DL) Management entity also provides Join and Leave events to the IS-SME.

In an aircraft, A separate instance of the A/GCS shall be created for each type of subnetwork supported. When multiple Service Providers are to be accessed concurrently over the same type of subnetwork, then a separate instance shall also be created for each Service Provider.

Note 3.—Compression state information is retained on Handoff between Ground Stations on the same subnetwork which either belong to the same Service Provider or its associates. Therefore, instances of the airborne A/GCS are not created and deleted for each individual data link connection but are instead persistent so that compression state is retained across data link handoff.

In a Ground System, instances of the A/GCS shall be created and deleted on demand for each data link connection with a given aircraft.

Note 4.—A Ground System may be in contact with many different aircraft simultaneously and it needs to balance its resources against demand. Hence, it is unlikely to be practicable to retain an A/GCS instance in the hope that the same aircraft may re-connect – although some implementations may choose to do just this. On the other hand, compression state information will need to be saved so that it can be restored later by the same or a different Ground System. Most likely this will be to a file or memory buffer.

~~1.3~~3.3 Logical Channels

Note 1.—Each transmitted frame is assigned to a logical channel. Channel number zero is reserved for Data Link Control messages. All other logical channels may be compressed using Deflate, although the protocol is flexible enough to be extended in a backwards compatible manner to support other compression schemes (e.g. voice compression). One deflate encoded channel is typically assigned to ISO TR 9575 identified packets (e.g. ES-IS and CLNP). This is used for ISH PDUs and any CLNP PDUs that cannot be compressed by LREF. Another channel may be assigned for LREF compressed PDUs and a further, experimental, channel may be assigned for CLNP PDUs with re-ordered header fields. The protocol design is aimed at both minimising bandwidth and providing the flexibility for future extension.

Note 2.— Multiple frames may also be concatenated into a single transmission frame in order to minimise transmission overheads. On receipt, the transmission frame is broken up into the frames contained within it which are then processed in the order in which they were concatenated into the transmission frame i.e. the transmission order within the frame determines the processing order. Each frame is then processed depending upon its logical channel.

Each frame shall be formatted as illustrated in Figure 3-3. There shall be four fields:

1. The Logical Channel (LC) field (12 bits);
2. The Priority field (4 bits);
3. The Length field (16 bits)
4. The User Data field (all remaining octets in the frame).

This four field group may be repeated multiple times within the maximum transmission frame size.

LC	Pr	Len	User Data

Figure 3-33-2 Frame Format

1.1.13.3.1 Field Definitions

The LC field comprises the first 12 bits of the frame transmitted (least significant bit first) and shall identify the logical channel on which the frame is sent. The first octet transmitted shall comprise the high order 8 bits and the most signficant four bits of the second octet shall comprise the low order 4 bits of the 12 bit channel number. Channel number zero shall be reserved for data link control. Channel numbers in the range FF0h to FFFh are not available for use and shall not be assigned to any channel.

The Pr field comprises the next low order 4 bits of the second octet of the frame transmitted (least significant bit first) and shall identify the frame's priority as an unsigned binary number in the range zero to 15. Zero shall represent the lowest priority.

The Len field comprises the next 16 bits of the frame transmitted (least significant bit first) and shall identify the length of the subsequent user data field in octets.

The user data field shall follow the Len field. This shall always a whole number of binary octets (as given by the Len field), and each octet is transmitted least significant bit first.

1.1.23.3.2 Concatenation

Multiple frames addressed to the same destination may be concatenated together for transmission in a single data link "burst" (i.e. transmission frame) up to the maximum frame size supported by the communications media. Frames of different priorities shall not be concatenated together unless:

a. the sender controls access to the medium and there are no unfulfilled requests for access to the medium for packets of a higher priority than the lowest priority frame in the concatenated frame.

b. the sender has already been given permission to send a frame with a priority equal to the lowest priority frame in the concatenated frame.

c. the transmission medium does not support priority based access.

Note.—In VDL Mode 3, the Ground Station controls access to the medium and gives permission to send based on data priority.

On receipt, the received frames shall be processed in strict order of receipt.

1.1.33.3.3 Frame Authentication and Verification

If required, a Frame Authentication and Verification pattern may be appended to a single or concatenated set of frames. The purpose and use of the Authentication and Verification pattern shall depend upon the Authentication and Verification procedures, if any, agreed using the DLCP.

The format of the Frame Authentication and Verification pattern shall be as illustrated in Figure 3-5. The first octet shall be set to binary ones.

Note.—It is always possible to distinguish the Authentication and Verification pattern from a normal frame as no normal frame can start with eight bits all set to one.

FFh	Seq. No.	Len	Security Data

Figure 3-53-3 Authentication and Verification Pattern

The second and third octets shall contain a sequence number expressed as an unsigned 16-bit binary number encoded least significant bit least significant byte first. The sequence number shall be initialised to zero when a new session key is agreed and incremented by one for each successive transmission.

The fourth octet shall contain the length in octets of the remainder of the Frame Authentication and Verification pattern.

The Security Data shall comprise the “Security Data” used for authentication and verification.

A receiving system shall discard any frames received when authentication and verification procedures have been agreed and either no authentication and verification pattern is present, or the sequence number is the same or less than that in the last frame that was received with a valid authentication and verification pattern.

If incrementing the sequence number results in an arithmetic overflow then the data link shall be terminated and a new data link initiated in order to establish a new session key.

1.1.43.3.4 Data Transfer

Once a channel has been assigned to a given purpose using the DLCP, user data may be transferred as a series of frames sent with that channel number included in the frame header. The frame priority shall be set to reflect the priority of the data contained within the frame.

The frames on a given channel shall comprise a continuous data stream fragmented and then re-assembled in strict transmission order. Each channel shall support bi-directional data transfer.

Note 1.—A given data format may specify that frame boundaries are significant in determining packet boundaries. However, this is a feature of the data format and not the channel concept.

On reception the channel number shall be used to determine the format of the data contained in the frame and how it is processed.

If a frame is received containing an unknown channel number, the frame shall be discarded and the problem reported to the peer system by using the DLCP to send a Channel Reset packet identifying the problem.

If the channel has been assigned to a data compression algorithm then the user data field of each frame sent over the channel shall be compressed using that algorithm. The compression shall take place immediately prior to transmission and in the order in which multiple frames sharing the same compression algorithm are concatenated into a transmission frame. On reception, the user data shall be decompressed using the corresponding decompression algorithm and in the order in which the frames were received and/or concatenated into the same data link frame.

Note 2.—It is important that the compression takes place immediately prior to transmission as data using the same compression algorithm can be sent at different priorities and hence may overtake each other in a transmission queue.

~~1.1.5~~3.3.5 Data Compression Procedures

3.3.5.1 Deflate Compression

Note 1.—The Deflate Compression procedures are specified in 5.7.6.5.

Note 2.—This SNDCF permits the concurrent use of multiple Deflate compressed data streams each associated with a different dictionary including the empty dictionary. Each such Deflate compressed data stream is unidirectional and is associated with one or more channels. Data on each such channel is compressed as part of the same data stream. Although the compressed data streams in each direction of data transfer are unidirectional, when Deflate compression is applied to a channel in one direction, it is also applied on the same channel in the other direction and using the same dictionary.

Note 3.—A Deflate Dictionary is an octetstring of frequently used symbols and may be up to 32KB long. A Deflate Dictionary Identifier uniquely identifies a unique octetstring.

Deflate Data Compression shall only be used when it has been listed as being supported in the Data Link Capabilities parameters included in the both an aircraft and Ground System's DLS/DLR packet and the exchange of DLS/DLR packets has been completed.

~~1.1.1.1.1~~3.3.5.1.1 Initialisation

When the use of the Deflate data compression algorithm has been agreed on data link initialisation or restart, the compressor and decompressor in each direction shall be initialised prior to their use on any channel.

If the use of multiple Deflate dictionaries has been agreed then a separate compressor/decompressor shall be used for each dictionary. The compressor/decompressor for a given dictionary shall be initialised by:

a) applying the contents of the dictionary into the compressor and discarding the result

b) initialising the history buffer of the decompressor with the dictionary contents.

When Deflate is re-initialised following a Link Reset, the applicable dictionary, if any, is also initialised as specified above.

~~1.1.1.1.2~~3.3.5.1.2 Data Transfer

If the use of Deflate and optionally a Deflate dictionary was specified in the Channel Start DLCP packet for a given channel, Deflate compression shall apply to all data sent on that channels in both directions of data transfer.

Note 1.–There is no requirement to re-initialise an existing data compression stream when a Channel Start is issued identifying a dictionary that is already in use. The identified channel simply joins the list of channels using the compressor/decompressor.

The User Data of a channel frame shall be compressed as a single packet as specified in 5.7.6.5.2. Frames are compressed in strict transmission order regardless of the channel with which they are associated. The resulting compressed frame shall include the FCS.

Note 2.—The channel header is not compressed – only the user data.

When a frame is received on a channel assigned for use with Deflate compression then the user data shall be decompressed using the Deflate decompressor associated with the Deflate Dictionary assigned to the channel, if any. Frames shall be decompressed in strict order of reception regardless of the channel with which they are associated.

A compressor shall not use a backwards reference greater than the Deflate Compression Window size agreed when the data link is initialised or restarted.

~~1.1.1.1.3~~3.3.5.1.3 Error Recovery

If an FCS failure is detected on receipt then the DLCP Reverse Link Reset procedure shall be invoked in order to report and recover from the problem. The sender shall indicate using the appropriate DLCP parameters:

a) the data compression algorithm to which the reset applies (i.e. Deflate) and the associated dictionary, if any, and

b) the data stream position of the last successfully received packet, expressed as the offset of the last received octet after decompression from the start of the data stream i.e. when the decompressor was last initialised.

Note. Link Reset applies only to one direction of data transfer at any one time.

~~1.1.1.1.4~~3.3.5.1.4 Receiving a Link Reset

When a DLCP Link Reset packet is received indicating resync of a Deflate compressed stream, the indicated compressor shall be reset. The compressor shall be set so that:

a) the Deflate Compression Window now ends with the last octet that was correctly received by the peer system, as indicated by the Link Reset, or

b) the Deflate Compressor is re-initialised with the associated Deflate Dictionary, if any, loaded into the compressor.

A DLCP Link Reset packet shall be returned indicating whether the compressor was reset to the requested position or re-initialised.

The AK Sequence number parameter shall be included to indicate that this is a confirmation of reset.

~~1.1.1.1.5~~3.3.5.1.5 Completing the Error Recovery Procedure

When a DLCP Link Reset packet is received in response to a Link Reset, the decompressor shall be re-initialised to the indicated position in the data stream. if the packet indicates that the compressor had been re-initialised to its initial state then decompressor is also re-initialised to the initial state and any associated dictionary reloaded.

Any compressed data packets received on a given Deflate compressed data stream between the transmission of a Link Reset and the receipt of a Link Reset acknowledgement shall be ignored.

~~1.1.1.1.6~~3.3.5.1.6 Restoring the Deflate Compression State

Note.—The Deflate compression state is the contents of current window into which backwards references may be made (up to 32KB) and the offset into the data stream of the last octet in that window.

A Ground System shall perform restoration of the Deflate Compression State by obtaining the current Deflate Compression state from the previous Ground System and loading the appropriate Deflate Compressor and Decompressor with the compression state.

An airborne system shall carry forward the compression state from the previous data link connection without change.

1.43.4 The Data Link Control Protocol (DLCP)

Note 1.—Channel zero is dedicated to the Data Link Control Protocol (DLCP). However, following Data Link Initiation, all other channels are unassigned and a major function of the DLCP is to control the use of the remaining channels and the functions that apply to the data link between an aircraft and Ground Station.

Note 2.—The DLCP is specified as a robust protocol designed to recover from packet loss in the MAC layer.

Channel zero shall be dedicated to the Data Link Control Protocol (DLCP).

The Data Link Control Protocol (DLCP) shall comprise the following packet formats:

1. DATA LINK START (DLS).
2. DATA LINK RESTART (DLR).
3. DATA LINK ERROR (DLE).
4. CHANNEL START (CS).
5. CHANNEL END (CE).
6. CHANNEL ABORT (CA).
7. CHANNEL RESET (CR).
8. LINK RESET (LR)

The format of each DLCP packet shall be as shown below.

ID	Seq. no.	Channel No.*	Optional Parameters

*optional, depending on ID value

Figure 3-73-4 DLCP Packet Format

The DLCP packet shall comprise

- an four bit Identifier field (ID) encoded as an unsigned binary number (least significant bit first),
- a sixteen bit sequence number also encoded as an unsigned binary number (least significant bit first),
- for the CS, CE and CR frames only, a 12 bit channel number encode as an unsigned binary number transmitted least significant bit first. In all other frames, the sequence number shall be padded with four trailing zero bits to the next octet boundary.
- zero, one or more optional parameters. The optional parameters are encoded as Type Length Value (TLV) parameters using the same encoding procedures as specified for the options part of the PDU header in ISO/IEC 8473. The permissible set of optional parameters is specified separately for each DLCP packet.

The DLS, DLR, CS and CE DLCP packets may have optional user specified parameters that are passed through transparently by the DLCP. Parameter codes in the range 1000 0000 to 1100 1111 shall be reserved for user specified parameters.

An implementation receiving an unknown DLCP packet (i.e. with an unknown identifier field value) shall declare a protocol error and invoke the Data Link Restart procedures to return the data link to a defined state.

Note 3.—The backwards compatible mechanism for the introduction of new features is provided by the DLS packet. Hence, an unidentified DLCP packet will always be a protocol error.

On data link initiation, the first DLCP packet sent shall have a sequence number of zero. The sequence number shall be incremented for each subsequent. On reaching the maximum value (i.e. 2^{16}-1, the sequence number shall wrap round to zero).

An implementation receiving a DLCP packet with a lower sequence number than that previously received shall ignore the packet.

Note 4.—Because of wrap around, implementers should treat the term "lower" with a certain degree of caution.

Note 5.—As a local matter, an implementation may limit the number of acceptable protocol errors from a specific peer system and terminate the data link if that limit is exceeded.

Both aircraft and ground systems shall maintain a variable tracking the last received sequence number from the peer system. This shall be set to zero on receipt of a DLS with a sequence number of zero, and thereafter set to the value of the sequence number in each received and processed frame.

With the exception of a DLS with a sequence number of zero, an incoming frame shall be ignored if its sequence number is the same or less than the last received sequence number.

All DLCP packets shall be sent using the highest priority – priority 15.

Note.—A DLCP packet exchange may be an essential preliminary to the sending of high priority data and hence some DLCP packets have to be sent at the highest priority i.e. 15. As the DLCP also requires that packets are sent and received in sequence number order, it does not make sense to differentiate DLCP packet priorities as this could result in unnecessary protocol errors.

~~1.1.1~~3.4.1 DLCP Procedures

3.4.1.1 Data Link Initialisation

Data Link Initialisation shall be performed by an aircraft only

When initialising a data link, the aircraft shall mark all channels other than channel zero as unassigned and send a DLS packet. On receipt of a DLS packet. the Ground System shall also mark all channels other than channel zero as unassigned. It shall then apply the Compression State recovery procedures specified in 0, and return its own DLS packet in acknowledgement.

The DLS's sequence number shall be set to zero for data link initialisation. The DLS sent in acknowledgement to a received DLS with a sequence number of zero shall also have a sequence number of zero.

A timer t_1 shall be started whenever a DLS is sent, and reset when the DLS is acknowledged. If timer t_1 expires before the DLS is acknowledged then the DLS shall be sent again with a sequence number of zero and timer t_1 restarted.

Note.—if the DLS is resent then any channel assignments and user messages that were sent after the first transmission have to be assumed lost and may have to be resent.

If a Ground System receives a duplicate DLS initialising the data link (i.e. with a sequence number of zero), it shall deallocate any channel allocations it had made since the receipt of the previous DLS and again return its own DLS packet in acknowledgement.

No other packet may be sent by the aircraft until a valid DLS has been received in response. Any packets other from a Ground System other than a responding DLS shall be silently discarded. A Ground System may send further DLCP packets as soon as it has responded to the DLS.

If an aircraft receives a duplicate DLS with sequence number zero from the Ground System after having already received such a DLS, then it shall discard any channel assignments received from the Ground System preceding that duplicate DLS. The aircraft shall not discard any channel assignments it made itself.

The following parameters shall be included in the DLS:

Parameter	Included By		Purpose
	Aircraft	Ground System	
Data Link Capabilities	M	M	To declare the implemented capabilities.
Compression Algorithm Identifier	O	O	To identify the Data Compression Algorithms supported
Deflate Compression Window	O	O	Identifies the largest backwards reference that will be made by the sender's Deflate compressor.
Highest Channel Number	O	O	Identifies the highest channel number that the sender can use.
Previous Ground System ID	O	-	When present, identifies a Ground System from which the current compression state may be recovered.
Ground System ID	-	M	Uniquely identifies the Ground System
Compression State Restored	-	O	When present indicates that the compression state was recovered from the identified Ground System.
Security Algorithm ID	O	O	Used to indicate support of a given security algorithm
Random Value	O	O	Required when authentication and verification procedures are to be used.
Public Key	O		Used to communicate and aircraft's public key to a Ground System.
Public Key Certificate	O	O	Used to communicate the system's public key certificate.

Parameter	Included By		Purpose
	Aircraft	Ground System	
User Data	O	O	Used to exchange a user data packet on the DLS e.g. an ISH PDU.

On completion of the exchange of DLS packets:

- Only those capabilities in common between Aircraft and Ground System shall be used on the Data Link.
- The highest channel number available for allocation shall be the lower of the Highest Channel Numbers supported by Aircraft and Ground System.

Note.—Initialisation of the Deflate Compressor/Decompressor is specified in 3.3.5.1.

If a user data parameter is present in an incoming DLS, the user packet contained within it shall be passed to the service user.

~~1.1.1.1.1~~3.4.1.1.1 Negotiation of Data Link Capabilities

An aircraft shall identify its supported data link capabilities by including a Data Link Capabilities parameter in its DLS and setting the appropriate bits.

A Ground System shall inspect the Data Link Capabilities parameter in a received DLS and determine the common set of availability data link capabilities. The Ground System shall return this common set in its DLS response by including a Data Link Capabilities parameter and setting the bits that correspond to the common set of capabilities.

Any unrecognised Data Link Capabilities shall be ignored by the Ground System.

~~1.1.1.1.2~~3.4.1.1.2 Negotiation of Compression Algorithms

An aircraft shall identify the compression algorithms and versions it supports by including a "Compression Algorithm identifier" parameter for each such algorithm in its DLS. Each such parameter shall identify the algorithm and version supported.

A Ground System shall determine the common set of supported compression algorithms and versions by comparing the list of compression algorithms given in the aircraft's DLS with those compression algorithms it supports. The Ground System shall list this common set in its DLS response by including a Compression Algorithm Identifier parameter for each such algorithm identifying both algorithm and version supported. When the Ground System supports an earlier version to that supported by the aircraft, then this earlier version shall be that included in the common set of supported algorithms.

Any unknown Compression Algorithms shall be ignored by the Ground System.

Note.—Version numbers are intended to be used incrementally and if a given version is supported then all earlier versions are also supported. The Ground System may therefore respond with an earlier version number if the version proposed is not supported. It is implicitly assumed that the aircraft will support this earlier version.

~~1.1.1.1.3~~3.4.1.1.3 Restoring the Compression State

If the aircraft's A/GCS instance has retained compression state information from a previous data link connection, it shall include the *Previous Ground System ID* parameter in its DLS.

This shall contain the Ground System Identifier that had been uplinked in the DLS from the Ground System with which the previous data link connection had been established.

If supported by the Ground System, the Ground System shall use a "Previous Ground System ID" parameter in the aircraft's DLS to contact the identified Ground System and to obtain from it:

a) the compression state for each compression algorithm supported by both Ground System and Aircraft, and

b) the current channel assignments, and

c) the point in each compressed data stream (both ground to air and air to ground) at which communication was terminated between the aircraft and that Ground System, expressed as the offset of the last received octet after decompression from the start of the data stream i.e. when the decompressor was last initialised.

If the compression state is successfully obtained, then Ground System shall restore the current channel assignments and set its own A/GCS compression/decompression functions to the obtained state. The Ground System shall include a "Compression State Restored" parameter in the returned DLS for each compression algorithm restored, indicating the stream position for which compression was restored.

Note 1.—The compression state may include Deflate compression state information and state information from any other A/GCS compression algorithm. it also includes the current channel allocations for each compression algorithm, which are implicitly restored. This is because compression algorithms are linked to channels.

Note 2.— A data stream may be restored to position zero which indicates that the channel assignments have been restored but not the data compression state which must be re-initialised.

Note 3.—LREF state is restored separately (See section 4.6.1.3. However, LREF compression cannot be restored unless the channel assigned to LREF is also restored.

When an aircraft receives a DLS response that includes a "Compression State Restored" parameter it shall restore the indicated compression functions and channels to their state when the data link with the previous Ground Station was terminated.

If the aircraft is unable to accept an indicated stream position in the ground to air direction, then the aircraft shall use the Reverse Link Reset procedure to return the data stream to the initial state.

If the aircraft is unable to accept an indicated stream position in the air to ground direction, then the aircraft shall invoked the Forward Link Reset procedures to indicate that the affected data stream is being returned to its initial state.

Note 4.—If the Ground System is the same as the previous Ground System – which is very likely when a single Ground System is connected to several Ground Stations in a given geographical error, then restoring the compression state should be trivial (i.e. the information is available locally). When the Ground System is remote then a communications protocol will be needed to recover the compression state. This could, for example be the Hypertext Transfer Protocol (http) with the Ground System ID and Aircraft address used to construct a conventional URL from where the required compression state will be found.

~~1.1.1.1.4~~3.4.1.1.4 Authentication and Verification Negotiation

Note 1.—This specification includes the optional capability to negotiate and use security procedures for authentication of the source of each frame and to verify the integrity of the data received.

Note 2.—Authentication may either be single entity (the airborne system authenticates the ground system only) or mutual authentication (both airborne and ground systems authenticate each other).

When required by the effective Security Policy, an aircraft shall initiate the agreement of a shared session key by including in the DLS:

1. a security algorithm identifier in order to indicate the security algorithm and version proposed.

2. a 32-bit random value generated using a suitable random number generator.

3. either the public key for the airborne system or its Public Key Certificate.

Note 3.—This feature is optional for implementation. However, the use of authentication and verification may be required by a Ground System. This may be known to the aircraft by a priori knowledge or configuration information in a subnetwork specific announcement (e.g.) a GSIF. Service may be refused if this feature is required by the Ground System but not implemented by the aircraft.

When a Ground System:

1. receives an incoming DLS that contains a security algorithm identifier, random value and either a Public Key or a Public Key certificate, and

2. it implements this optional feature, and

3. either mutual or single entity authentication is required or permitted by the effective security policy, then

it shall respond by including in its own DLS the security algorithm identifier to indicate the security algorithm and version that will be used, a Random Number (generated using its own random number generator) and its Public Key Certificate.

Note 4.—Version numbers are intended to be used incrementally and if a given version is supported then all earlier versions are also supported. The Ground System may therefore respond with an earlier version number if the version proposed is not supported. It is implicitly assumed that the aircraft will support this earlier version.

Note 5.—A Ground System that neither supports nor requires the use of authentication may ignore the security parameters in an incoming DLS. If an aircraft does not receive security parameters in response to a DLS containing the security parameters then whether or not it proceeds with the data link depends upon its own security policy.

Both the Ground System and the Airborne System, on receipt of a DLS containing the Ground System's Public Key Certificate, shall compute a shared secret value using the ATN Secret Value Derivation Primitive (ASVDP) according to the procedure specified in 8.5, and derive a shared session key using the ATN Key Derivation Function (AKDF).

If a Ground System receives a DLS proposing an unsupported security algorithm, or containing no security parameters, and

a) the effective security policy requires the use of data link authentication and verification, then it shall reject the DLS by returning a DLE. However, if

b) the Ground System's Security Policy does not require the use of data link authentication and verification then it may proceed with the data link by returning a DLS without any security parameters.

If the Airborne System receives a DLS specifying an unrecognised security algorithm or which does not contain any security parameters, and

i) the effective security policy requires the use of data link authentication and verification, then it shall reject the DLS by returning a DLE. However, if

ii) the Airborne System's Security Policy does not require the use of data link authentication and verification then it may proceed with the data link.

3.4.1.2 Data Link Authentication and Verification Procedures

Once a shared session key has been derived, a sending system shall calculate a message authenticator over each single frame or concatenated series of frames sent as a data link frame, generated using the ATN Keyed Message Authentication Code primitive (AMACP), according to the procedure specified in 8.5. The message authenticator shall be appended to the frame(s) as the security data field in the Authentication and Validation pattern (see 3.3.3).

When a system which has derived a shared session key receives a link layer frame with an Authentication and Validation pattern appended to it, then it shall verify the authenticator using the ATN Keyed Message Authentication Code Verification Primitive (AMAVP) according to the procedure specified in 8.5. If the verification procedure fails or an Authentication and Validation pattern was not present, then the entire frame shall be discarded.

Computation of the message authenticator shall include the authentication and verification pattern with an empty security data field (i.e. with a zero length).

Note.—This is necessary to include the sequence number in the message digest and hence to offer a protection against replay.

~~1.1.1.3~~3.4.1.3 Data Link Restart

The Data Link Restart procedures shall be performed in order to recover from a serious protocol error as specified by this specification. The Data Link Restart procedure may be initiated by either the aircraft or the Ground System.

To initiate a Data Link Restart, the initiator shall send a DLR packet. The packet's sequence number shall be the next sequence number in the series.

When a system receives a DLR packet with a non-zero sequence number and which is not in response to a Data Link Restart that it initiated itself, the system shall deallocate all allocated channels and re-initialise all compression functions. It shall respond with a DLR packet acknowledging the restart.

Note.—The AK Sequence number parameter is used to indicate that this is a response and to which DLR it is a response.

Once a system has initiated a Data Link Restart, it shall ignore and discard all received packets on all channels except for another DLR. When it receives a DLR acknowledging its own Data Link Restart, the system shall deallocate all allocated channels and re-initialise all compression functions.

A timer t_1 shall be started whenever a DLR is sent, and reset when the DLR is acknowledged. If timer t_1 expires before the DLR is acknowledged then the DLR shall be sent again and timer t_1 restarted. On retransmission, the sequence number shall be the next sequence number in the series.

The procedures for negotiation of data link capabilities and compression algorithm negotiation shall be as specified for Data Link Initiation.

Note 1.—There is no mechanism for restoring the compression state or channel assignments on a Data Link Restart.

Note 2.—There is no change to shared session key on a Data Link Restart.

The following parameters shall be included in the DLR for a Data Link Restart:

Parameter	**Included By**		**Purpose**
	Aircraft	**Ground System**	
Data Link Capabilities	M	M	To declare the implemented capabilities.
Compression Algorithm Identifier	O	O	To identify the Compression Algorithms supported
Deflate Compression Window	O	O	Identifies the largest backwards reference that will be made by the sender's Deflate compressor.
Highest Channel Number	O	O	Identifies the highest channel number that the sender can use.
AK Sequence Number	M	M	Used to acknowledge the received DLR. Required on a response only.
Diagnostic	M	M	Used to indicate the reason for the restart.

On completion of the exchange of DLR packets for a Data Link Restart:

- Only those capabilities in common between Aircraft and Ground System shall be used on the Data Link.
- The highest channel number available for allocation shall be the lower of the Highest Channel Numbers supported by Aircraft and Ground System.

Note.—The data link is now in its initial state except for any shared session key which remains unchanged.

~~1.1.1.4~~3.4.1.4 Data Link Termination

The data link shall be implicitly terminated either:

a) when the underlying data link reports loss of communications, or

b) when a DLS packet is received. The DLS packet shall be processed as specified in 3.4.1.1.

The data link shall be explicitly terminated by either airborne or ground system sending a DLE packet. Once a DLE packet has been sent, any further packet received from the peer system shall be silently discarded and the DLE re-sent. On receipt of a DLE packet a system shall regard the data link as being terminated.

Once a data link has been terminated no further data transfers shall be initiated. However, channel allocation and compression state shall be retained for possible use on the next data link connection.

Note.—The implicit termination of a data link when a DLS is received is compatible with the retransmission of a DLS (see 3.4.1.1) and the creation of a new session key required for data link security (see 3.3.3).

~~1.1.1.5~~3.4.1.5 Channel Allocation

The CS packet shall be used to assign the purpose and use of a logical channel, as indicated by the packet's parameters. If a CS packet is received for a channel that is already assigned and:

a. the assignment had been previously made by the sender of the CS packet, then the CS packet re-assigns the channel to the new purpose and use.

b. the assignment had been previously made by the receiver of the CS packet, then the CS packet is in error and a Channel Reset shall be sent in response.

Note.—If the channel assignment or re-assignment is accepted then no response is expected.

The sender of the CS packet shall be the *channel initiator* and the receiver shall be the *channel responder*.

When choosing a logical channel to assign, an aircraft shall choose the highest numbered logical channel available for assignment while a ground system shall choose the lowest numbered logical channel available. If no channel is available, a lower priority channel shall be selected out of those previously assigned by the sender of the CS packet, and re-assigned to the new purpose and use. If no such channel is available, the request for a new channel assignment shall fail and the service user notified.

In order to prevent channel assignment race conditions, there shall be at least once channel that remains unassigned at all times.

A single compression algorithm may be specified for the channel out of those in common between initiator and responder.

If a CS packet is received attempting to assign a channel number greater than that which the receiving system declared as the "highest channel number" in its DLS or DLR packet, then the channel assignment shall be rejected by returning a Channel Reset, with an appropriate diagnostic code.

An unknown parameter code or the use of an unrecognised data format shall be rejected as an error and a Channel Reset packet returned in order to report the error, with an appropriate diagnostic code. The channel shall return to the unassigned state.

~~1.1.1.6~~3.4.1.6 Channel Deallocation

The Channel End (CE) packet is sent in order to return a channel to the unassigned state. It shall be sent only by the channel initiator. Receipt of a CE by the channel initiator shall be regarded as a protocol error and the DLR procedure shall be used to re-initialise the data link. A CE received for an unassigned channel shall be silently ignored.

~~1.1.1.7~~3.4.1.7 Link Reset Procedures

The Link Reset procedures shall be used by a data compression function that operates on data from one or more channels, in order to recover from errors in the compression procedure that affect those channels. Either system may perform a link reset.

Note.—The only data compression procedure currently specified to use this procedure is Deflate.

~~1.1.1.1.1~~3.4.1.7.1 Forward Link Reset Procedure

The Forward Link Reset Procedure shall be used to announce that the compressed data stream from the initiator of the procedure to the receiver is being reset to its initial state.

To invoke the Forward Link Reset Procedure, the initiator shall send a Link Reset packet to the receiver.

The Compression Algorithm Identifier parameter shall be present and identifies the affected data compression algorithm and hence the affected data stream and channels.

The Diagnostic parameter shall be present and indicates the reason for the Link Reset.

When a Forward Link Reset is sent, the affected data stream compressor is re-initialised.

When a Forward Link Reset is received, the affected data stream decompressor is re-initialised.

Note.—No acknowledgement of receipt is required.

~~1.1.1.1.2~~3.4.1.7.2 Reverse Link Reset Procedure

To initiate a Reverse Link Reset, the initiator shall send an LR packet containing the following parameters:

Compressed Data Stream Resync	To identify the affected compression algorithm and by implication the affected channels, and to indicate the position in the data stream to which a reset may take place.
Diagnostic Reason	To identify the reason for the Link Reset.

Additional optional parameters may be specified for the specific compression algorithm.

When a Data Link Reset is received, the identified data compression function shall be alerted, and a Link Reset message returned acknowledging the Link Reset. This shall include the following parameters:

Compressed Data Stream Resync	To identify the affected compression algorithm and by implication the affected channels, and to indicate the position in the data stream to which a reset has taken place.
AK Sequence Number	Containing the sequence number of the LR packet that initiated the reset.

Additional optional parameters may be specified for the specific compression algorithm.

When such a Data Link Reset Response is received the identified data compression function shall be alerted.

Note.—The procedures carried out by the data compression function in response to a Data Link Reset are specific to that function.

A timer t_1 shall be started whenever an LR is sent to initiate a link reset, and reset when the LR is acknowledged. If timer t_1 expires before the LR is acknowledged then the LR shall be sent again and timer t_1 restarted.

Note.—The sequence number is incremented for each retransmission.

~~1.1.1.8~~3.4.1.8 Broadcast Operation

When used in support of broadcast:

1. DLCP packets shall be sent ground to air only
2. Channel Start shall be the only DLCP packet format used
3. DLCP errors shall be silently ignored by the receiver.
4. The maximum number of channels supported shall be 16.
5. Deflate shall be implicitly available with no dictionary supported and a maximum window size of 8KB.
6. No security procedures shall be available.

3.4.2 DLCP Packet Formats

Note. The DLCP procedures are specified in 3.4.1. Only the packet formats are specified here.

~~1.1.1.1~~3.4.2.1 Data Link Initiation (DLS)

Identifier (ID) 0001

The DLS packet shall be sent either to initialise a data link.

The following optional parameters are specified for the DLS packet:

1. Data Link Capabilities
2. Compression Algorithm Identifier.
3. Deflate Compression Window
4. Highest Channel Number.
5. Previous Ground System ID
6. Ground System ID
7. Compression State Restored
8. Security Algorithm ID
9. Random Value
10. Public Key
11. Public Key Certificate
12. User Data

The parameter codes for these parameters shall be as specified for each parameter. On receipt an unrecognised parameter shall be silently ignored.

~~1.1.1.2~~3.4.2.2 Data Link Restart (DLR)

Identifier (ID) 0010

The DLR packet shall be sent to restart a data link after an error has occurred

The following optional parameters are specified for the DLR packet:

1. Data Link Capabilities
2. AK Sequence Number
3. Compression Algorithm Identifier.
4. Deflate Compression Window
5. Highest Channel Number.
6. Previous Ground System ID
7. Ground System ID
8. Diagnostic (to indicate the restart reason)

The parameter codes for these parameters shall be as specified for each parameter. On receipt an unrecognised parameter shall be silently ignored

~~1.1.1.3~~3.4.2.3 Data Link End

Identifier (ID) 0011

The DLE packet shall be sent to terminate or reject the initiation of a data link

The following optional parameters are specified for the DLE packet:

1. Diagnostic.

The parameter codes for these parameters shall be as specified for each parameter. On receipt an unrecognised parameter shall be silently ignored

~~1.1.1.4~~3.4.2.4 Channel Start (CS)

Note.—The purpose of the CS packet is to assign the use of a previously unassigned channel and to define its operational parameters.

Identifier 0100

The CS packet header shall include the logical channel number to which the CS applies.

The following optional parameters are specified for the CS packet:

1. Compression Algorithm Identifier
2. Data Format.

The parameter codes for these parameters shall be as specified for each parameter. On receipt an unrecognised parameter shall be rejected as a protocol error.

~~1.1.1.5~~3.4.2.5 Channel End (CE)

Note.—The purpose of the CE packet is to restore a channel to the unassigned state.

Identifier 0101

The CE packet header shall include the logical channel number to which the CE applies.

The parameter codes for these parameters shall be as specified for each parameter. On receipt an unrecognised parameter shall be rejected as a protocol error.

~~1.1.1.6~~3.4.2.6 Channel Reset (CR)

Note.—The purpose of the CR packet is to signal a problem in channel assignment or use, and to restore the channel to a defined state.

Identifier 0110

The CR packet header shall include the logical channel number to which the CE applies.

The parameter codes for these parameters shall be as specified for each parameter. On receipt an unrecognised parameter shall be rejected as a protocol error.

The CR packet shall be sent only:

a) when required by this specification in order to signal a problem with a channel assignment or

b) on the request of the service user in order to report a problem in the data sent over the channel. In this case, the Diagnostic parameter shall indicate “User Problem”. The User Diagnostic parameter shall be present and set to a value specified by the service user.

The following optional parameters are specified for the CR packet:

1. Diagnostic

2. User Diagnostic.

If no User Diagnostic parameter is present then a Channel Reset results in the channel becoming unassigned.

If a User Diagnostic parameter is present then a timer t_1 shall be started by the sender.

All user data received on the same channel shall be discarded until a Channel Reset is returned by the peer system acknowledging receipt of the Channel Reset by including an AK Sequence number parameter containing the sequence number of the original Channel Reset.

If timer t_1 expires before such a Channel Reset is received, the Channel Reset shall be sent again, and timer t_1 restarted.

Note.—The DLCP protocol requires that the sequence number is incremented for each retransmission.

When a Channel Reset is received from a peer system with a User Diagnostic parameters but without an AK Sequence Number parameter. the Channel Reset and Diagnostic shall be reported to the service user and a Channel Reset returned in response. This shall include the AK Sequence Number parameter containing the sequence number of the received Channel Reset. No other parameters shall be included.

When a Channel Reset is received from a peer system with a User Diagnostic parameters and an AK Sequence Number parameter that is not in acknowledgement of the last sent Channel Reset, the Channel Reset shall be ignored.

~~1.1.1.7~~3.4.2.7 Link Reset (LR)

Note 1.—The purpose of the LR packet is to re-initialise a compressed data stream or to restart it at an identified point.

Note 2,—A Link Reset affects all channels using the affected compressed data stream.

Identifier 0111

The Link Reset packet shall be sent when an error is detected in a received Deflate compressed data stream, in order to return the data stream to a defined state.

The following optional parameters are specified for the Link Reset packet:

1. Compressed Data Stream Resync
2. Compression Algorithm ID
3. Diagnostic

The parameter codes for these parameters shall be as specified for each parameter. On receipt an unrecognised parameter shall be rejected as a protocol error.

~~1.1.3~~3.4.3 DLCP Optional Parameters

3.4.3.1 The Data Link Capabilities Parameter

Parameter Code	0000 0001
Parameter Length	variable
Parameter Value	see below

The parameter shall be interpreted as a variable length bitmap indicating support of data link capabilities specified in this and subsequent standards.

Note 1.—an important purpose of this parameter is to provide for the introduction of new capabilities in a backwards compatible manner. Therefore this specification requires implementations to ignore capabilities that they do not understand and to handle longer length parameters than they would otherwise expect.

The parameter value shall be encoded as least significant bit and least significant octet first. For the purposes of this specification, the bits in the bitmap shall be numbered b_0 through to b_n where b_0 is the least significant bit in the bitmap and b_n is the most significant bit. The sender shall send the minimum number of octets in order to transmit all non-zero bits in the bitmap. A receiver shall be able to accept any length bitmap up to the maximum length permitted by the encoding rules.

The Data Link Capabilities parameter shall be interpreted as follows:

Bit No.	Capability
0	ISO TR 9575 Format Data

Bit No.	Capability
1	LREF Data Format
2	Reformatted CLNP Headers
3	IPv4

The sender shall set the corresponding bit to one in order to claim support of the associated capability.

The data link capabilities that are used for communication between the sender and receiver shall be those in common between those declared in the sender's DLR and those declared in the DLR sent back in response. Any unrecognised bits in the capabilities bitmap shall be ignored.

Note 2.—LREF Data Compression is listed here as a capability for efficiency reasons. Formally, it is a capability of the service user.

~~1.1.1.2~~3.4.3.2 Compression Algorithm Identifier

Parameter Code	0000 0010
Parameter Length	0, 2 or 3 octets
Parameter Value	Algorithm ID and version

Note 1.—The purpose of the Compression Algorithm Identifier is to identify a Compression Algorithm supported by the sender of the DLS or DLR, and the version supported

Note 2.—Currently Deflate is the only compression algorithm that will be identified. However, it is intended that each Deflate dictionary supported is identified by a unique Algorithm ID.

The parameter value shall be either:

a) an unsigned 16 bit unsigned binary number that is a unique identifier for a Compression Algorithm. Compression Algorithm identifiers shall be globally known and the registry of Compression Algorithm identifiers shall be maintained by ICAO, or

b) a Compression Algorithm identifier as defined above followed by an 8-bit unsigned binary number that is the version number of the algorithm.

If no version number is present then version zero shall be assumed.

This parameter may occur more than once in a DLS or DLR and is repeated for each Compression Algorithm supported.

A compression algorithm ID of zero is defined by this specification to identify the Deflate stream compression algorithm with no initialisation dictionary. If the parameter length is zero and no parameter value is present then this shall equate to a parameter value of zero.

Note.—Version number are allocated incrementally and support for a given version number implies support for all earlier versions. For example, support for version 2 implies that versions 1 and 0 are also supported.

~~1.1.1.3~~3.4.3.3 Deflate Compression Window

Parameter Code	0000 0011
Parameter Length	1 octet
Parameter Value	an unsigned binary number in the range 10 to 15

Note 1.—The purpose of this parameter is to declare the largest backwards reference that will be made in the Sender's a Deflate compressed data steam. The receiver can use this information to reduce the size of the decompression buffer.

This parameter shall be included in a DLR in order to signal the largest backwards reference that will be made in the Sender's a Deflate compressed data steam. The parameter value shall be a number *n* in the range 10 to 15. The largest backwards reference shall be calculated as:

$$2^n-1$$

If the parameter is omitted then a value of *n* shall default to 15.

Note 2.—There is no requirement for the Default Compression Window to be the same in both directions.

~~1.1.1.4~~3.4.3.4 Highest Channel Number

Parameter Code	0000 0100
Parameter Length	2 octets
Parameter Value	Highest assignable Channel Number

Note.—The purpose of this parameter is to indicate the maximum number of channels supported by the sender. The actual number of channels available will be the lower of the maximum supported by both sides.

This parameter shall be included in a DLR to indicate the highest assignable channel number. The sending system will not attempt to assign a channel number greater than the parameter value, nor will it accept a channel number greater than the parameter value. If this parameter is not included then the highest assignable channel number shall default to 2^{12}-1.

~~1.1.1.5~~3.4.3.5 Ground System ID

Parameter Code	0000 0101
Parameter Length	variable
Parameter Value	Previous Ground System Identifier

Note.—The purpose of the parameter is to enable the Ground System to provide the aircraft with some unique identifier that can be used on a subsequent data link to restore the compression state.

The Ground System ID parameter shall be included in every DLR sent to an aircraft. It shall provide a unique identifier for the Ground System.

Note.—An example of a unique identifier is the NET of the ATN Router.

~~1.1.1.6~~3.4.3.6 Previous Ground System ID

Parameter Code	0000 0110
Parameter Length	variable
Parameter Value	Previous Ground System Identifier

Note.—The purpose of this parameter is to identify the previous Ground System on the same type of Air/Ground Subnetwork which the aircraft used for data communications using the procedures specified by this SNDCF. It is used as a hint to the receiver that it may be possible to transfer the compression state from the previous connection to the new one.

The Previous Ground System ID shall only be included in the DLS sent by an aircraft to initialise a new data link. It shall not be sent by a Ground System on when performing a Data Link Restart.

~~1.1.1.7~~3.4.3.7 Compression State Restored

Parameter Code	0000 0111
Parameter Length	>5
Parameter Value	Compression Algorithm ID and version followed by stream position

Note 1.—This parameter is included by a Ground System in order to indicate to an aircraft that it has been able to recover the compression state for the indicated Compression Algorithm. All channel assignments are restored; the compressors and decompressors are in the same state as at when the data link was closed.

Note 2.—It occurs once for each data compression algorithm restored.

Note 3.—This parameter is not used to signal restoration of the LREF Directory. This is formally a service user function and is signalled via a parameter code reserved for user parameters.

The Compression State Restored parameter shall only be included in a DLS sent by a Ground System to an aircraft, and to indicate that the compression state has been recovered from the Ground System attached to the previous Ground System, and for the specified Compression Algorithm.

The parameter value shall comprise four fields:

1. a 16-bit compression algorithm identifier
2. an 8-bit compression algorithm version number
3. the data stream position in the air to ground direction;
4. the data stream position in the ground to air direction.

In each case, the stream position expressed as

a) an 8-bit length expressed as an unsigned binary number least significant bit first and giving the number of octets in which the stream position is encoded, and

b) an unsigned binary number least significant bit least significant byte first and occupying the indicated number of octets.

The presence of a given compression algorithm identifier and version shall indicate that all channels that use that algorithm for data compression have been restored.

The stream position parameter for the air to ground direction shall indicate the data stream position of the last octet of the last packet received on a channel that uses the specified algorithm.

Note 4.—If the position is zero then this indicates that the decompressor has been re-initialised.

The stream position parameter for the ground to air direction shall indicate the data stream position of the last octet of the last packet sent on a channel that uses the specified algorithm.

Note 5.—If the position is zero then this indicates that the compressor has been re-initialised.

~~1.1.1.8~~3.4.3.8 Diagnostic

Parameter Code	0000 1000
Parameter Length	1 octet
Parameter Value	Diagnostic Code

Note.—The purpose of this parameter is to convey the reason for a data link restart, or a problem with a channel assignment or use.

The diagnostic parameter shall convey the reason for the restart, link reset or other problem using one of the reason codes given in . An invalid reason code shall be ignored on receipt.

Restart Reason Code	Interpretation
0000 0010	Channel Start Error
0000 0011	Highest channel number exceeded
0000 0100	Unknown parameter code
0000 0101	Unknown compression algorithm requested
0000 0110	Unknown Data Format requested
0000 0111	Channel not in use.
0000 1000	User Reset
0000 1001	Security Sequence Number Overflow

0000 1010	Protocol Error
0000 1011	Cannot restore compression state

Table 3-1~~3-1~~ Diagnostic Codes

~~1.1.1.9~~3.4.3.9 AK Sequence Number

Parameter Code	0000 1001
Parameter Length	2 octets
Parameter Value	Sequence Number

The parameter value AK Sequence number shall identify the sequence number of the DLCP packet that is being acknowledged.

~~1.1.1.10~~3.4.3.10 Data Format

Parameter Code	0000 1010
Parameter Length	1 octet
Parameter Value	Data Format Identifier

The Data Format identifier shall be used to indicate the format of the data sent on the channel. The parameter value shall be an unsigned 8-bit number interpreted as specified in Table 3-3

Data Format Identifier	Data Format
0000 0001	Data packets whose type and function can be determined according to ISO TR 9577 *Note.—This includes ISO/IEC 9542 (ES-IS) and ISO/IEC 8473 (CLNP) packets*
0000 0010	LREF encoded data
0000 0011	Reformatted CLNP
0000 0100	IPv4

Table 3-3~~3-2~~ Data Format Identifiers

In the absence of this parameter, data format 0000 0001 shall be assumed as the default.

~~1.1.1.11~~3.4.3.11 User Diagnostic

Parameter Code	0000 1011
Parameter Length	1 octet
Parameter Value	diagnostic code

The User Diagnostic parameter shall indicate that a problem has been detected in the user data and a Channel Reset has been used to report the problem. Action following a user generated channel reset shall

~~1.1.1.12~~3.4.3.12 Compressed Data Stream Resync Parameter

Parameter Code	0000 1100
Parameter Length	>3
Parameter Value	Compression Algorithm ID and version followed by stream position

This parameter shall comprise three fields:

1. a 16-bit compression algorithm identifier
2. an 8-bit version number
3. a data stream position parameter expressed an unsigned binary number least significant bit least significant byte first and occupying the remainder of the parameter value

The compression algorithm identifier and version shall be used to indicate the data compression algorithm to which the parameter applies.

The data position parameter shall be set to either:

1. (reync request) the total number of octets received in the data stream, up to and including the last packet received without error on that data stream, or
2. (resync response) the position in the data stream to which the compressor has been reset.

Note.—The purpose of this parameter is to signal to the sender a point in the data stream from which valid backwards references can be made.

~~1.1.1.13~~3.4.3.13 User Data

Parameter Code	0000 1101
Parameter Length	variable
Parameter Value	user data

The contents of this parameter shall comprise user data. This user data shall be a ISO TR 9575 format packet. On receipt. the contents of the packet shall be provided to the service user as data received in the ISO TR 9575 format.

~~1.1.1.14~~3.4.3.14 Security Algorithm Identifier

Parameter Code	0011 0011
Parameter Length	2 or 3
Parameter Value	Algorithm Identifier and version

The parameter value shall be either:

c) an unsigned 16 bit unsigned binary number that is a unique identifier for a Security Algorithm. Security Algorithm identifiers shall be globally known and the registry of Security Algorithm identifiers shall be maintained by ICAO, or

d) a Security Algorithm identifier as defined above followed by an 8-bit unsigned binary number that is the version number of the algorithm.

If a version number is not present then a version number of zero shall be assumed.

~~1.1.1.15~~3.4.3.15 Random Value

Parameter Code	0011 0100
Parameter Length	4
Parameter Value	Random Value

The Random Value parameter shall contain a 32-bit unsigned integer value. The random number generator used to generate this value shall use a source of random data that is not predictable by a third party.

~~1.1.1.16~~3.4.3.16 Public Key

Parameter Code	0011 0101
Parameter Length	43
Parameter Value	Public Key

This parameter shall contain the unique 43 octet public key of the sender.

Note.—The public key is in uncompressed form 04||x||y where x and y are co-ordinates of an elliptic curve point.

~~1.1.1.17~~3.4.3.17 Public Key Certificate

Parameter Code	0011 0110
Parameter Length	variable
Parameter Value	List of certificates

The value of this parameter shall comprise the sender's certificate followed by zero, one or more certificates that comprise the certificate path. Each certificate shall be encoded in compressed format as defined in 8.4.3.3.3.

~~1.5~~3.5 Data Transfer Formats

3.5.1 ISO TR 9577 Format Packets

Note.—This class of packets includes ISO/IEC 9542, 8208 and 8473 PDUs. The primary use is expected to be for ISH PDUs. A packet sent in this data stream can be unambiguously identified from its initial octet. Each frame contains a single such packet.

A frame sent on a channel assigned to this data format shall contain a single packet that can be identified from its initial octet according to ISO TR 9575. On receipt, the processing of such a packet shall be a local matter.

~~1.1.2~~3.5.2 LREF Formatted Data

Data sent over a channel assigned to LREF formatted data shall be formatted in compliance with the LREF CLNP header compression algorithm (see 4.6.1).

~~1.1.3~~3.5.3 Reformatted CLNP Data

The reformatted CLNP packet format shall be as illustrated below in Figure 3-9.

Note.—The parameter order has been revised in order to optimise Deflate compression by ordering the fields according to increased probability of change from packet to packet.

Version/Protocol Id Extension			
sec	pri	Source address Length Indicator	
Source Address			
rrc	qos	Destination Address Length Indicator	
Destination Address			
Security Parameter (if present)			
Priority Parameter (if present)			
The Length Indicator			
SP	Check	E/R	Type
Data Unit Identifier (if SP set)			
Total Length (if SP set)			
Lifetime			
Route Recording Parameter (if present)			
QoS Maintenance parameter (if present)			
MS	Segment length		
Segment offset (if SP set)			
Any other options			
Reason For Discard (for ER PDU only)			
Data			

Figure 3-9~~3-5~~ Reformatted CLNP Packet

When a CLNP PDU is reformatted as above, the value of each header field is transferred unchanged into the order expressed above.

The "sec", "pri", "rrc" and "qos" flag shall indicate respectively the presence or absence of the security, priority, route recording and QoS maintenance parameters. If the flag is set to one then this shall indicate that the corresponding parameter is present. If set to zero then this shall indicate that the parameter is absent.

The "check" flag shall indicate whether the checksum was used in the original NPDU.

Note.— the value of the checksum is not conveyed within the reorganised PDU format. This is because, as a result of the reorganisation reconstitution process, the rebuilt CLNP PDU while semantically identical may not be syntactically identical to the original CLNP PDU. For example, the order of options may change.

~~1.1.4~~3.5.4 IPv4 Data Format

Data sent over a channel assigned to IPv4 formatted data shall be formatted as an IPv4 packet as specified in IETF RFC 791.

~~1.6~~3.6 Broadcast Operations

Note.—The purpose of broadcast operations is to permit the broadcast of data from a Ground Station to many aircraft simultaneously.

Broadcast transmissions shall be ground to air only.

Channel one shall be pre-assigned to the Data Format for packets identified according to ISO TR 9575.

Note.—This assignment permits the uplink of broadcast ISH PDUs without additional overhead.

A Ground Station may assign other channels for use with other data formats and compression algorithms. However, if it does so then the channel assignment shall lapse after t_2 seconds.

An aircraft shall silently ignore and discard any frames received with errors or DLCP errors.

Any data compression/decompression function associated with a broadcast channel shall be separate from the same function used for singlecast communications i.e. the broadcast data stream is entirely separate from the singlecast data stream.

When all channel assignments associated with a given compression algorithm have timed out and the channels are deallocated, the associated compressor/decompressor shall be returned to its initial state.

3.7 Compatibility with other Frame Formats

Note.-During transition from older protocols, or to provide for lower cost alternatives for small aircraft, other frame formats may used by aircraft operating over the same data link. The A/GCS is designed to permit this to occur and for use of the A/GCS or an alternative frame format to be determined by inspection of the first octet of the first frame received from the aircraft.

If the first octet of the first frame received from an aircraft by a Ground Station after a data link has been established is non-zero then:

a) If the value of the octet corresponds with a known initial octet value of an alternative frame format that is valid for the datalink and supported by the Ground Station, then the aircraft shall be deemed as supporting that frame format and the A/GCS procedures shall not be applied. The procedures for that other frame format shall be applied instead.

b) If the value of the octet does not correspond with any known initial octet for an alternative frame format supported by the Ground Station, then the data link shall be terminated or reset, as appropriate, indicating a protocol error as the reason for the problem.

Note 1.-This is possible because the first downlinked frame must start with a DLCP packet on channel zero.

Note 2.-It is not possible for an alternative frame format to start with an initial zero octet and to be compatible with the A/GCS.

4. Proposed SARPS for the Frame Mode SNDCF

4.1 General

In an aircraft, a separate instance of this SNDCF shall be created for each type of subnetwork supported. When multiple Service Providers are to be accessed concurrently over the same type of subnetwork, then a separate instance shall also be created for each Service Provider.

Note 1.—Compression state information for the LREF compression algorithm is retained when a data link is terminated for possible use on a later data link connection with a Ground Station operated by the same Service Provider or an associate. Therefore SNDCF implementation instances are persistent rather than being created and deleted for each data link connection.

In a Ground System, instances of this SNDCF shall be created on demand and deleted when no longer required.

Note 2.—A Ground System may be in contact with many different aircraft simultaneously and it needs to balance its resources against demand. Hence, it is unlikely to be practicable to retain an SNDCF instance in the hope that the same aircraft may re-connect – although some implementations may choose to do just this. On the other hand, LREF compression state information will need to be saved so that it can be restored later by the same or a different Ground System. Most likely this will be to a file or memory buffer.

The A/GCS shall be used to support communications over the data link service provided by the Air/Ground subnetwork.

If data link authentication and verification is supported then the Security Policy shall be configurable by Subnetwork Type and Service Provider.

Note 3.—It may also be necessary to configure Security Policy variations (e.g. different security algorithms) by Ground Station or groups of Ground Station.

~~1.2~~4.2 SN Service

The Frame Mode SNDCF shall provide the SN-Unitdata.request and SN-Unitdata.indication service required by CLNP.

The Frame Mode SNDCF shall also provide a data link management interface for use by the IS-SME. This interface shall support:

1. Requests to establish data link communications (airborne systems only)
2. Requests to terminate data link communications

4.3 Data Link Initiation

4.3.1 Initiator Procedures

The Data Link Initiation service shall support the following parameters:

1. Ground Station Address
2. User Data.

Note.—When multiple instances of this SNDCF are implemented, a local means will be necessary to direct the data link initiation request to the appropriate instance.

On receipt of a Data Link Initiation request:

a) If a data link connection with another Ground Station already exists then this shall be terminated by using the A/GCS DLCP.

b) If a data link connection already exists with the identified Ground Station, then the request shall be ignored.

c) The A/GCS shall be used to initialise data communications with the Ground Station.

d) If User Data was provided with the Data Link Initialisation request then this shall be included in the DLCP DLS.

e) The Ground System Identifier of the Ground System with which the SNDCF last had a data link connection, if any, shall be included as the value of the “Previous Ground System ID” DLCP parameter

f) If LREF is supported then this shall be included in the list of Data Link Capabilities provided on the DLCP DLS, and the maximum LREF directory size other than the default of 128 shall be indicated to the remote system by including this as a DLS user parameter as specified in 4.6.1.2.1.

g) If LREF *Local Reference Cancellation* is also supported then the DLCP user parameter “Local Reference Cancellation supported” shall be included in the DLCP DLS.

h) If CLNP Header reformatting is supported then this shall be included in the list of data link capabilities.

i) If the Security Policy requires or permits the use of data link authentication and verification then the DLCP parameters required for negotiation of this function shall be included. The choice between inclusion of the public key only or the public key certificate shall depend upon the security policy.

If the A/GCS DLCP successfully establishes a data link then:

a) If user data was returned on the DLCP DLS then this shall be assumed to be an NPDU and passed to the service user using an SN-UNITDATA.indication.

b) If LREF is supported and the DLCP user parameter providing the maximum LREF directory size is included in the DLS then this shall used as the maximum directory size, otherwise the default of 128 shall be used as the maximum directory size. If the maximum directory size thereby determined is greater than that offered on the aircraft’s DLS then the data link connection shall be terminated with a protocol error diagnostic.

c) If the DLCP user parameter “Local Reference Cancellation supported” is present then the LREF *Local Reference Cancellation* option shall be available for use, unless the parameter was not included in the aircraft’s DLS when the data link shall be terminated with a protocol error diagnostic.

d) If the DLCP user parameter indicating “LREF compression state restored” is present then the LREF directory from the previous data link connection shall be retained and used for this data link connection. If the parameter is not present then the LREF directory shall be re-initialised to its empty state.

4.3.2 Responder Procedures

The responder procedures shall be implemented by a Ground System implementing this specification.

When the A/GCS indicates that a DLS has been received from an aircraft:

1. The Ground System shall, optionally, make a local decision as to whether to accept or reject the data link connection, and, if the data link connection is accepted:
2. If any user data is provided on the DLS this shall be assumed to be an NPDU and passed to the service user using an SN-UNITDATA.indication.
3. If LREF compression is included in the list of data link capabilities and LREF is also supported by the Ground System then the DLCP user parameter providing the maximum LREF directory size shall be extracted if present and a default of 128 assumed if it is not present.
4. If the DLCP user parameter "Local Reference Cancellation supported" is present and the LREF *Local Reference Cancellation* option is also supported by the Ground System then this option shall be available for use on the data link.
5. If a Previous Ground System ID parameter is included in the DLS and LREF compression state restoration is supported by the Ground System, then the Ground System shall attempt to recover the LREF compression state as specified in 4.6.1.3.

If the data link connection is rejected then the DLCP data link connection rejection procedure shall be invoked.

if the data link connection is accepted then the DLCP data link connection acceptance procedures shall be invoked to return a DLS to the aircraft. This shall include:

1. A user data parameter containing the Ground System's ISH PDU.
2. If LREF is supported and was also listed in the Data Link Capabilities parameter provided by the aircraft, a DLCP user parameter, as specified in 4.6.1.2.1, shall be provided indicating the maximum directory size that may be used, and calculated as the smaller of the maximum directory sizes supported by the Aircraft and Ground System, respectively.
3. If the LREF *Local Reference Cancellation* option is available for use (i.e. the DLCP user parameter "Local Reference Cancellation supported" was present in the aircraft's DLS and the option is also supported by the Ground System) then the DLCP user parameter "Local Reference Cancellation supported" shall be included.
4. If the LREF Compression state has been successfully restored, then the DLCP User Parameter "LREF Compression State restored" (see 4.6.1.2.2) shall be included.

4.4 Data Link Termination

If a data link termination request is received then the data link connection, if any, shall be terminated using the DLCP.

If LREF is supported and in use, the LREF compression state shall be retained.

~~1.5~~4.5 Data Transfer

4.5.1 SN-UNITDATA.Request

An SN-UNITDATA.Request service shall be provided. This shall take a single parameter comprising an NPDU to be sent to the Ground System.

if an SN-Unitdata.request is received and no data link connection exists, the NPDU shall be queued for transmission, in strict priority order, waiting for a data link connection to be established.

Note.—It is a local matter as to how long the NPDU will be queued awaiting a data link connection. However, this retention period should be related to the NPDU's expected lifetime in the network.

if an SN-Unitdata.request is received and a data link connection does exist, the NPDU shall be queued for transmission, in strict priority order, waiting for a data link to be available.

When the data link is available for use and NPDUs are queued for transmission then the NPDU with the highest priority shall be selected for transmission using the A/GCS.

Note.—A/GCS channels may be assigned to LREF format, CLNP Reformatted Headers or ISO TR 9575 format NPDUs i.e. uncompressed CLNP, ES-IS, etc. When LREF and CLNP Reformatted headers are both available, it is a local matter as to which is used. Otherwise, the NPDU has to be sent uncompressed. Either way, an A/GCS channel has to be established.

If:

a) neither LREF nor CLNP Reformatted headers are supported by the data link, or

b) the NPDU selected for transmission is not a CLNP NPDU, or

c) LREF compression is in use and the CLNP NPDU is a CLNP Echo PDU, or

d) LREF compression is in use and the CLNP NPDU is not compressible by LREF because it satisfies one of the conditions listed in 5.7.6.3.2.3.1,

then if a channel has not already been allocated for sending ISO TR 9575 format NPDUs, the DLCP shall be used to allocate such a channel. The NPDU shall be sent as a user data packet over such a channel.

Note.—For efficiency, it is expected that the Channel Start and NPDU are concatenated into the same transmission frame.

If LREF or CLNP Reformatted headers are supported by the data link and the NPDU selected for transmission is a CLNP Data or Error PDU then:

a) either LREF or CLNP Header reformatting shall be used to transfer the NPDU over the data link. The choice shall be a local decision of the sender.

b) If a channel has not already been allocated for the chosen data format then such a channel shall be allocated using the DLCP.

c) If LREF is the chosen transmission format then the NPDU shall be compressed using the LREF compression procedure and the resulting compressed NPDU transmitted using a channel assigned to the LREF data format.

d) If CLNP Reformatted Headers is the chosen transmission format then the NPDU header shall be reformatted as specified in 4.6.2 and the resulting reformatted NPDU transmitted using a channel assigned to the CLNP Reformatted Headers data format.

Note.—The above procedure can result in both sides simultaneously allocating a channel to the same data format. This is not an error nor is it particularly inefficient.

~~1.1.2~~4.5.2 SN-UNITDATA.Indication

If an NPDU is received on a channel assigned to ISO TR 9575 format NPDUs then the NPDU shall be passed to the service user as the user data parameter of an SN-UNITDATA.Indication.

If an NPDU is received on a channel assigned to the LREF Data Format, then the NPDU shall be assumed to be in LREF compressed format and decompressed using the LREF decompression procedures specified in 4.6.1.1. The resulting NPDU shall be passed to the service user as the user data parameter of an SN-UNITDATA.Indication.

If an NPDU is received on a channel assigned to the CLNP Reformatted Headers Data Format, then the NPDU shall be restored to the proper CLNP Header format by applying the procedures specified in 4.6.2. The resulting NPDU shall be passed to the service user as the user data parameter of an SN-UNITDATA.Indication.

~~1.1.3~~4.5.3 Broadcast Data Transfers

Only a Ground System shall use the broadcast data link service provided by the DLCP.

Note 1.—No data link initiation or termination procedures are required for broadcast operation.

Note 2.—Deflate may be used for broadcast transfers. However, its operation may be problematic as the loss of a single frame by a receiver will mean that all subsequent frames until the channel assignment times out will be unintelligible.

~~1.6~~4.6 Data Compression

4.6.1 LREF Compression

4.6.1.1 General

Note.—The LREF compression algorithm was previously specified for use with an ISO/IEC 8208 communications service. The same algorithm is specified for use here except that the DLCP is used to negotiate the use of LREF (instead of the ISO/IEC 8208 Call setup) and Channel Reset is used instead of an ISO/IEC 8208 Network Reset. Uncompressible PDUs are also sent using a separate channel rather than as part of the same data stream as compressed NPDUs.

The procedures specified in 5.7.6.3 shall be applied except that:

1. NPDUs are transferred using a channel assigned to the LREF data format instead of an ISO/IEC 8208 virtual circuit.

2. Channel Reset is used instead of Network Reset. The User Diagnostic parameter of the Channel Reset shall contain the SNDCF Error Report Diagnostic code.

3. When more than one channel is assigned to the LREF data format between the same aircraft and Ground System, they shall share a common LREF directory.

4.6.1.2 DLCP User Parameters supporting LREF Compression

4.6.1.2.1 Maximum LREF Directory Size

Parameter Code	1000 0000
Parameter Length	variable
Parameter Value	Max. Directory Size

This parameter shall contain the Maximum LREF Directory Size supported encoded as an unsigned binary number. The length of the parameter shall be the minimum number of octets needed to express the value.

If this parameter is omitted then a default of 128 shall be assumed.

~~1.1.1.1.2~~4.6.1.2.2 LREF Compression State Restored

Parameter Code	1000 0001
Parameter Length	0
Parameter Value	empty

The presence of this parameter shall indicate that the LREF compression state has been restored.

~~1.1.1.1.3~~4.6.1.2.3 Local Reference Cancellation Supported

Parameter Code	1000 0010
Parameter Length	0
Parameter Value	empty

The presence of this parameters shall imply the support of the Local Reference cancellation option.

~~1.1.1.3~~4.6.1.3 Restoring the LREF Compression State

A Ground System that receives an incoming data link connection from an aircraft that reports a previous data link connection with an identified Ground System shall optionally chose to recover the LREF Compression State, provided that the A/GCS has been able to restore the channel assignments for LREF. The previous Ground System Identifier and Aircraft address shall be used to determine the source of this information.

The LREF compression state information shall comprise the LREF directory.

If the LREF compression state has been successfully restored then the DLCP user parameter “LREF compression state restored” shall be returned in the DLS.

Note.—If the Ground System is the same as the previous Ground System – which is very likely when a single Ground System is connected to several Ground Stations in a given geographical error, the restoring the compression state should be trivial. When the Ground System is remote then a communications protocol will be needed to recover the directory information. This could, for example be the Hypertext Transfer Protocol (http) with the Ground System ID and Aircraft address used to construct a conventional URL from where the required compression state will be found.

~~1.1.1.4~~4.6.1.4 Broadcast Operation

When LREF is used for broadcast data transfer:

a) A maximum directory size of 128 shall be assumed.

b) Local Reference Cancellation shall not be used.

c) The LREF directory used for broadcast operation shall be separate from that used for single cast operation.

d) When a channel assignment used for LREF times out, the LREF directory used for broadcast shall be returned to its initial state.

e) If an error is detected in a received LREF compressed NPDU, the NPDU shall be silently discarded.

4.6.2 CLNP Header Reformatting

The Reformatted CLNP Header format is specified in 3.5.3.

The Header of an outgoing CLNP NPDU shall be reformatted by changing the encoding of the CLNP header to the header formatted illustrated in Figure 3-9.

The Header of an incoming CLNP NPDU shall be restored to its correct format by parsing the reformatted header and then recreating a proper CLNP Header from this information.

Note.—The reconstituted header will not necessarily be syntactically identical to the original although the semantics will be unchanged.

5. Route Management

5.1 Route Initiation

When the airborne IS-SME receives a Join Event from a mobile Air/ground subnetwork associated with the Frame Mode SNDCF, the IS-SME shall determine the instance of the SNDCF associated with subnetwork and Service Provider that is the subject of the Join Event, the IS-SME shall call the SNDCF's Data Link Initiation Service providing an appropriate ISO/IEC ISH PDU for the Airborne Router as the User Data.

The Ground System shall include its own ISH PDU in the response to the Data Link Initiation.

Both Airborne and Ground System IS-SMEs shall apply the procedures of 5.3.5.2.7 to ISH PDUs received by the Frame Mode SNDCF, except that the SNDCF's Data Link Termination service shall be used instead of a ISO/IEC 8208 Call Clear procedure.

The procedures of 5.3.5.2.8 through to 5.3.5.2.12 shall be applied to complete the Route Initiation procedure.

~~1.2~~5.2 Handoff

Handoff events from a mobile Air/ground subnetwork associated with the Frame Mode SNDCF shall be ignored.

~~1.3~~5.3 Route Termination

When the IS-SME receives a Leave Event from a mobile Air/ground subnetwork associated with the Frame Mode SNDCF, then SNDCF's Data Link Termination Service shall be invoked.

The procedures specified in 5.3.5.2.13.6 through to 5.3.5.2.13.9 shall be applied.

6. Proposed SARPs for the Direct Frame Mode SNDCF

Note 1.This SNDCF and accompanying CLNP Header compression algorithm is specified for use by small aircraft when a low cost ATS service is required over a frame mode link layer service i.e. a data link service that provides L-Unitdata.req and L-Unitdata.ind service elements. Only the CLNP header is compressed and there is no support for general data compression or other air/ground communications protocols. It is unlikely to be useful for AOC communications as these get the greatest advantage from DEFLATE compression and security labels encoded with an AOC traffic type cannot be compressed using this algorithm. Its use is thus expected to be only for General Aviation aircraft that require a low costs ATS datalink service.

Note 2.-This specification is dependent on the subnetwork providing a means to separately convey a 4 bit compression type parameter for each compressed packet.

Note 3.-For example, in VDL Mode 3 this is performed by including this information in a separate "payload" identifier octet that is inserted as the first octet in the frame.

6.1 Model of Operations

The model of operations for an SNDCF incorporating this compression algorithm shall be as shown in Figure 6-1. Network Layer PDUs shall be passed to the SNDCF using the SN-Unitdata.req service element.

Each such PDU shall be inspected to determine if it is a compressible CLNP PDU according to the data compression rules specified in 6.5.3. If so, the PDU shall be passed to the CLNP header compressor. If the PDU is not compressible, then it shall be passed to the data link service, without change and with a data type of TYPE_UNCOMPRESSED_PDU.

Note.-ISH PDUs are always uncompressible.

CLNP PDUs compressed by the CLNP Header compressor shall be passed to the data link service, and with a data type as indicated by the output of the compressor, and sent using the D-Unitdata.req service.

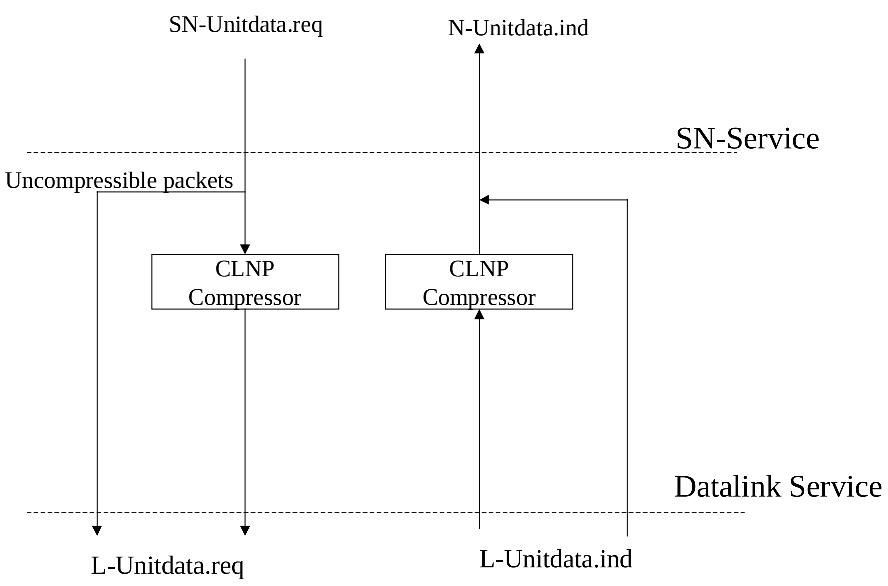

Figure 6-1 Model of Operations

When an incoming PDU is received from the data link service:

a) If it has a data type of TYPE_UNCOMPRESSED_PDU, it shall be passed unchanged to the SN Service user by invoking the SN-Unitdata.ind service element.

b) If the incoming PDU has any other data type associated with it, then the PDU shall be passed to the CLNP Header decompressor. The output of the decompressor shall be passed to the SN Service user by invoking the SN-Unitdata.ind service element.

6.2 Data Type Codes

The data type codes used by this SNDCF shall be as specified in Table 6-1 and are represented as four bit unsigned binary numbers.

Note.-These data type codes are used to identify the frame format. In VDL Mode 3, they are included in a Payload octet that is prefixed to the frame in each transmission.

Bit	**Meaning**
0000	TYPE_UNCOMPRESSED_PDU
0001	TYPE_RESTART
0010	TYPE_UNCOMPRESSED_CLNP
0011	TYPE_COMPRESSED_CLNP_LONG_WITH_OPTIONS
0100	TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS
0101	TYPE_COMPRESSED_CLNP_SHORT
0110	TYPE_MULTICAST
0111	Reserved
1000-1111	Reserved

Table 6-1 Data Type Codes

6.3 Compressed CLNP Header Format

The format of the compressed CLNP Header shall be as shown in Figure 6-2.

Note 1.-Depending on the data type and the value of the S, O, L and D bits, not all indicated fields are present.

Note 2.-The Payload field is not formally part of the compressed header and is shown here to illustrate how the data type information is passed when VDL Mode 3 is used as the data link. Other data links using this specification can adopt the same approach but may also define a different scheme to convey the data type information. In VDL Mode 3, the high order 4 bits of the payload field are always set to binary 0001 for data originated by this SNDCF.

A data type of TYPE_COMPRESSED_CLNP_SHORT or TYPE_MULTICAST shall identify a compressed CLNP Header comprising header fields up to and including the *Security* field. Such a packet shall contain the Q field, Index Number, QOS, Priority and Security fields. The compressed PDU shall be a compressed CLNP Data PDU.

A data type of TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS shall identify a compressed CLNP Header comprising header fields as illustrated in Figure 6-2 excluding the Options Length and Options fields. Additionally:

a) If the S bit is set to a binary 1 then the *DUI* field shall be present;

b) If the O bit is set to a binary 1 then the *Segment Offset* field shall be present;

c) If the L bit is set to a binary 1 then the *Total Length* field shall be present.

d) If the H bit is set to a binary 1 then the *Lifetime* field shall be present.

e) If the value of the D bit is set to a binary 1 then the *Discard Reason* field shall be present.

A data type of TYPE_COMPRESSED_CLNP_LONG_WITH_OPTIONS shall identify a CLNP Header comprising the same header fields as for a data type of TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS. Additionally, the compressed CLNP header shall be followed by one or more CLNP options fields copied from the original CLNP header. The total number of bytes occupied by these options fields shall be given by the value of the *Options Length* field.

Note.-a data type of TYPE_RESTART implies an empty packet follows and is used as an error recovery mechanism. A data type of TYPE_UNCOMPRESSED_CLNP is used when compression indexes are being defined; the packet has an uncompressed CLNP header.

Bit	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
Octet 0	Payload				Compression Type				
Octet 1	Q	Index Number							
	QOS				Priority				
	Security								
	S	E	M	T	H	O	L	D	(Bit Field)
	Lifetime (H)								
	Data Unit Identifier (S)								
	Segment Offset								
	(O)								
	Total Length (L)								
	Discard Reason (D - ER)								
Octet n	(Error PDU only)								
Octet n+1	Options length								
Octet n+2	Options								
...									
Octet p									

Figure 6-2 Compressed CLNP Header Format

The Semantics of the compressed CLNP header fields shall be

- The single bit Q field shall indicate the presence of QOS information. If not set (Q=0), no QOS information is present and the value of the QOS field is undefined.

- The Index Number shall be indicate the source and destination NSAP Addresses present in the original CLNP Header. The Index Number shall be in the range 0 to 127 (decimal).

- The QOS field shall consist of the CE, (bit 8) T/C (bit 7), E/T (bit 6), and E/C (bit 5) bits respectively of the ISO 8473 QoS Maintenance Parameter.

  Note.—The sequencing vs. transit delay (S/T) bit is sent in the T field (see Figure 6-2). This implies that whenever the S/T bit is set to 1, a long compression format has to be used.

- The Priority field shall be a 4 bit unsigned binary number representing a priority in the range 0 to 14 decimal. A value of 15 decimal shall imply that no priority has been specified.

  Note.-A CLNP PDU with a higher priority than 15 is compressed by including the priority parameter itself in the compressed header.

- The Security field shall be subdivided into two fields and shall indicate the security parameter of an ATN CLNP packet:

  a) The 5 high order bits shall comprise the 5 low order bits of the traffic type security tag of the CLNP security options parameter, and

  b) the low order 3 bits shall comprise the 3 low order bits of the security classification tag of the CLNP security options parameter.

  A zero value of either or both of the above two fields shall imply that the corresponding security tag is not present in the CLNP Header.

  Note.-The traffic type is implicitly ATSC which implies that a CLNP PDU containing any other traffic type (e.g. AOC) is compressed by including the security parameter itself in the compressed header.

- The Bit Field comprising the S, E, M, T, H, O, L and D bits, shall have the following semantics:.

Bit	**Meaning (Present == 1)**
S	SP flag of CLNP Header - Data Unit Identifier Present
E	Complement of CLNP ER flag
M	MS bit of CLNP Header
T	Sequence vs. Transit Delay Bit (from QOS Option)
H	Lifetime Field present (Hop Count)
O	Segment Offset Present
L	Total Length field present
D	Type of PDU (Error = 1, Data = 0)

- The presence of the Lifetime field shall be indicated by the H bit being set to 1. The absence of the Lifetime field shall imply a value for downlink PDUs of decimal 29, and for uplink PDUs, a value of decimal 5.

- The presence of the DUI field shall be indicated by the S bit being set to 1. The Data Unit Identifier shall always be presented for segmented packets or whenever the SP bit is set. Absence of this field shall imply that Segmentation is not permitted.

- The presence of the Segment Offset field shall be indicated by the O bit being set to 1. The Segment Offset shall be sent whenever the SP bit is set and the Segment Offset is greater than zero. Absence of this field shall imply a value of zero.

- The presence of the Total Length field shall be indicated by the L bit being set to 1. The Total Length field shall be present the first time a PDU fragment a given DUI is sent only.

  Note.-This implies that the value of the field is cached by the receiver by DUI and subsequent fragments with the same DUI are decompressed using the cached total length value.

- The presence of the Discard Reason field shall be indicated by the D bit being set to 1. It shall contain the value of the Discard Reason options parameter field.

- An Options Length field shall contain as its value the number of bytes occupied by the Options field.

- The value of the Options field shall comprise one or more CLNP options parameters.

6.4 Data Transmission Procedures

6.4.1 Determination of whether an NPDU is compressible

An NPDU received as the user data of an SN-UnitData.req shall be compressible if and only if:

- The Network Layer Protocol Identifier is binary 1000 0001 (i.e. it is a CLNP NPDU)

- The CLNP version/protocol id extension is set to binary 0000 0001.

- The PDU Type is for a Data or Error PDU.

If the NPDU is not compressible then it shall be passed unchanged to the datalink service for transmission, indicating a data type of TYPE_UNCOMPRESSED_PDU.

6.4.2 Assignment of a Compression Index

The CLNP Header compressor shall maintain a local compression directory with up to 128 entries relating an index number in the range 0 to 127, to Source and Destination NSAP Addresses.

Recommendation.*—A separate 128 entry directory and index number series should be used for each peer system with which the sending system is in contact.*

When a compressible NPDU has been submitted for transmission, this directory shall be interrogated in order to locate an entry corresponding to the Source and Destination NSAP Addresses of the NPDU. If such an entry is located, the associated index number shall be retrieved and the procedures specified in 6.4.3 shall be followed.

Otherwise, an unassigned index number shall be obtained and a local compression directory entry created associating this index number with the NPDU's Source and Destination NSAP Addresses. The Network Layer Protocol Identifier shall be replaced by the assigned index number encoded as an unsigned 8 bit binary number, and the NPDU passed unchanged to the datalink service for transmission, indicating a data type of TYPE_UNCOMPRESSED_CLNP.

If there are no unassigned index numbers available, the NPDU shall be passed otherwise unchanged to the datalink service for transmission, indicating a data type of TYPE_UNCOMPRESSED_PDU.

6.4.3 Creation of the Compressed Header

The CLNP PDU Header including the Network Layer Protocol Identifier shall be removed and replaced with a compressed header in the format illustrated in Figure 6-2:

- The Index Number field shall be set to the value of the assigned index number encoded as a 7 bit unsigned binary number.
- The Q bit shall be set to 1 if a Globally Unique QoS Maintenance Parameter is present in the original CLNP Header and the QOS field bits and T bit set according to the value of the Globally Unique QoS Maintenance Parameter and 6.3. The Q bit shall be set to 0 otherwise.
- If a Priority options parameter is present in the original CLNP Header and the priority value is 14 or less then the Priority field shall be set to the low order 4 bits of the Priority options parameter. The Priority field shall be set to zeroes otherwise.
- If a Security options parameter is present in the original CLNP Header and:
- the value of the parameter is:

  a) an ATN Security Label,

  b) the Traffic Type and Security Classification security tags are the only security tags present, and

  c) the Traffic Type is ATSC, then

  the value of the Security Field shall be set using the value of the Security Options Parameter and according to 6.3. Otherwise the Security Field shall be set to zeroes.

- If the PDU is an Error PDU then the D bit shall be set to 1. Otherwise the D bit shall be set to 0.
- The E bit shall be set to the complement of the E/R flag in the original CLNP Header.
- If the value of the Lifetime given in the original CLNP Header is greater than 5 or less than 29 (decimal) then a Lifetime field shall be included in the compressed header and the H bit set to 1. Otherwise the H bit is set to zero. The Lifetime field value shall be identical to the value given in the original CLNP Header.
- If the SP flag in the original CLNP Header is non-zero then a Data Unit Identifier (DUI) field shall be present and the S bit set to 1, and:

  a) The M bit shall be set to the value of the MS bit in the original CLNP Header.

  b) The value of the DUI field shall be set to the Data Unit Identifier contained in the original CLNP Header.

c) If a non-zero Segment offset is present in the original CLNP Header then the O bit shall be set to 1 and a Segment Offset field shall be present. The value of the Segment Offset field shall be set to the value of the Segment Offset in the original CLNP Header. Otherwise the O bit shall be zero.

d) If this is the first time that a packet with this DUI has been sent since the index number was assigned, then the L Bit shall be set to 1 and a Total Length Field shall be included and set to the value of the Total Length given in the original CLNP Header. Otherwise the L bit shall be set to zero.

Otherwise the S and M bits shall be set to zero.

Note 1.-It is not an error to include a Total Length field in more than one compressed header with the same DUI.

Note 2.-This implies caching by the receiver of the value of the Total Length field. The cached information need not be kept longer than the indicated PDU lifetime, and is discarded anyway when the associated index becomes unassigned..

✈ If the original CLNP PDU is an Error PDU then the Discard Reason field shall be present and set to the value of the Reason for Discard given in the original CLNP Header.

✈ If the original CLNP Header contains :

a) a priority parameter value greater than 14,

b) a security parameter that was uncompressible i.e. the value of the security field is zero, or

c) any other options parameters other than padding and a Globally Unique QoS Maintenance Parameter, then

such options parameters shall be copied to the compressed header. The Options Length field shall be present and set to the number of bytes in the copied parameters. Otherwise neither the Options Length nor Options shall be present.

The compressed header created above shall replace the original CLNP Header and the resulting compressed header and user data shall be passed to the datalink service for transmission. The data type shall be:

a) TYPE_COMPRESSED_CLNP_LONG_WITH_OPTIONS, if options parameters have been copied into the compressed header;

b) TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS, if no options parameters have been copied into the compressed header and the compressed header has a non-zero Bit Field.

c) TYPE_COMPRESSED_CLNP_SHORT otherwise. The Bit Field shall not be included in the compressed header for this datatype i.e. it is implicitly zero in this data type.

Note.—A zero Bit Field implies that no further fields follow this field as they are all dependent on the Bit Field being non-zero.

6.4.4 Compression Index Lifetime

For each assigned index number, a timer (CT3) shall be associated. This timer shall be (re)started every time a packet is sent with that index number.

When the timer expires, the index shall become unassigned.

When an underlying datalink is terminated, all associated index numbers become unassigned.

When an index number becomes unassigned, the corresponding local compression directory entry shall be removed.

6.5 Data Reception Procedures

6.5.1 Handling of an Incoming Packet

When an incoming packet is recevied from the datalink service the indicated data type shall be determined and:

- if the data type is TYPE_UNCOMPRESSED_PDU, the received packet shall be passed unchanged to the SN Service user using the SN-Unitdata.ind service element.
- if the data type is TYPE_UNCOMPRESSED_CLNP then the procedures specified in 6.5.2 shall be applied.
- If the data type is TYPE_RESTART the procedures specified in 6.5.6 shall be applied.
- Otherwise the decompression procedures specified in 6.5.3 shall be applied.

Note.—TYPE_MULTICAST packets are discussed in 6.6.

6.5.2 Index Number Assignment

When an incoming packet is received with a data type of TYPE_UNCOMPRESSED_CLNP, the first octet (an unsigned binary number) shall be decoded as the new index number and replaced by the Network Layer Identifier Octet for CLNP (binary 1000 0001). The PDU shall be passed otherwise unchanged to the SN Service user using the SN-Unitdata.ind service element.

The decompressor shall maintain a local decompression directory for each peer system with which it is currently in communication. This directory shall comprise a maximum of 128 entries relating an index number in the range 0 to 127, to Source and Destination NSAP Addresses.

This directory shall be interrogated to determine if an entry already exists for this index number. If such an entry exists and identifies the same Source and Destination NSAP Address pair as encoded into the header of the incoming packet, then no further action shall be taken. If a different Source and Destination NSAP Address pair is found then the error recovery procedures specified in 6.5.4 shall be followed.

Otherwise, a new decompression directory entry shall be created associating the received index number with the Source and Destination NSAP Address pair encoded into the header of the incoming packet.

6.5.3 Decompression Procedures

When an incoming packet is received then, with reference to the compressed header format given in Figure 6-2, a CLNP Header shall be constructed as follows:

- The Network Layer Protocol Identifier shall be set to binary 1000 0001.
- The Version/Protocol ID Extension shall be set to binary 0000 0001.

- The index number shall be decoded from the compressed header and used to determine the Source and Destination NSAP Addresses to be used in the reconstructed CLNP Header by interrogating the local directory specified in 6.5.2. If no corresponding directory entry can be found then the incoming packet shall be discarded and the error recovery procedures specified in 6.5.4 shall be applied.

- If the Q bit is non-zero, a Globally Unique QoS parameter shall be added to the CLNP Header options parameters and the QOS field bits used to determine the corresponding bits in the parameter value, as specified in 6.3.

- If the priority field is non-zero, a priority parameter shall be added to the CLNP Header options parameters and the decimal value of the priority field shall be encoded as the value of the priority parameter.

- If the security field is non-zero then a globally unique security parameter shall be added to the CLNP Header, indicating an ATN Security Label:

  a) If the most significant 5 bits of the security field are non-zero then a Traffic Type security tag shall be included in the ATN Security Label; the most significant 3 bits shall indicate a traffic type of ATSC and the least significant 5 bits shall be copied from the most significant 5 bits of the security field.

  b) If the least significant 3 bits of the security field are non-zero then a security classification security tag shall be included in the ATN Security Label; the value of this tag shall be the encoded decimal value of the least significant 3 bits of the security field.

Note.—A padding options parameter may also be included in the CLNP Header.

6.5.3.1 Decompression of Short Compressed Headers

When the data type of the received packet is TYPE_COMPRESSED_CLNP_SHORT, the CLNP Header shall be constructed as above, and:

- The PDU Type shall be set to indicate a Data PDU.

- The E/R flag shall be set to 1.

- The MS and SP flags shall be set to 0, and no segmentation part included in the reconstructed CLNP Header.

- The Lifetime shall be encoded as decimal 5 if the receiving system is airborne, or as decimal 29 otherwise.

- The Length Indicator field shall be set to the length of the reconstructed header

- The reconstructed header shall replace the compressed header and value of the Segment Length shall be set to the total length to the PDU.

- The checksum for the reconstructed header shall be recomputed and stored within it.

The resulting PDU shall be passed to the SN Service user using the SN-Unitdata.ind service element.

6.5.3.2 Decompression of Long Compressed Headers with no Options

When the data type of the received packet is TYPE_COMPRESSED_CLNP_LONG_NO_OPTIONS, the CLNP Header shall be constructed as above in 6.5.3. The Bit Field shall also be present and used to determine the further additional information in the reconstructed CLNP Header:

- If the D bit is set to 1 then the PDU Type shall be set to indicate an Error PDU. Otherwise the PDU Type shall be set to indicate a Data PDU.
- The E/R flag shall be set to the complement of the E bit.
- If the Q is set then the value of the S/T bit in the globally unique QoS Maintenance Parameter shall be set to the value of the T bit.
- If the H bit is set then the Lifetime in the reconstructed CLNP header shall be set to the value of the Lifetime field in the compressed CLNP Header. If the H bit is zero, the Lifetime shall be encoded as decimal 5 if the receiving system is airborne, or as decimal 29 otherwise.
- If the S bit is set to 0 then the SP and MS flags shall be set to zero and no segmentation part included in the reconstructed CLNP Header. Otherwise, the SP flag shall be set to 1 and a segmentation part included:

  a) The MS flag shall be set to the value of the M bit.

  b) The Data Unit Identifier shall be

  c) If the O bit is zero then the Segment Offset shall be set to zero. Otherwise the Segment Offset value shall be copied from the compressed header to the reconstructed header,

  d) If the L bit is set to 1 then the Total Length value shall be copied from the compressed header to the reconstructed header. Additionally, the Total Length shall be cached for use with later packets with the same DUI and index number, and from the same peer system. If a Total Length with the same DUI and index number, and from the same peer system had already been cached and was a different value, then the PDU shall be discarded and the procedures in 6.5.4 followed.

  e) If the L bit is set to zero, then the decompressor shall attempt to find a cached Total Length for the same DUI, index number and peer system. If found then this Total Length shall be copied into the reconstructed CLNP Header. If not found then the PDU shall be discarded.

  Recommendation.—*The error recovery procedures specified in* 6.5.4 *should be followed following the PDU discard.*

  Note.—Cached Total Lengths may be discarded when the PDU's lifetime has expired, the index number becomes unassigned, or the datalink with the peer system terminated.

- The Length Indicator field shall be set to the length of the reconstructed header
- The reconstructed header shall replace the compressed header and value of the Segment Length shall be set to the total length to the PDU.
- The checksum for the reconstructed header shall be recomputed and stored within it.

The resulting PDU shall be passed to the SN Service user using the SN-Unitdata.ind service element.

6.5.3.3 Decompression of Long Compressed Headers with Options

When the data type of the received packet is TYPE_COMPRESSED_CLNP_LONG_WITH_OPTIONS, the CLNP Header shall be reconstructed as specified in 6.5.3.2 above.

Additionally, the options parameters contained in the compressed header shall be copied to the reconstructed CLNP Header prior to the recomputation of the Length Indication, Segment Offset and Checksum .

6.5.4 Error Recovery Procedures

In order to perform error recovery, an empty packet with a data type of TYPE_RESTART shall be sent to the peer system, and the local decompression directory associated with packets received from that peer system shall be cleared i.e. all entries removed.

Received compressed packets shall be discarded but otherwise ignored until a packet is received with a data type of TYPE_COMPRESSED_CLNP. This shall implicitly acknowledge the restart.

Editor's note.—There may be a race condition here if the compressor sends a TYPE_COMPRESSED_CLNP and a compressed packet before it receives the TYPE_RESTART. This may result in a "restart loop".

6.5.5 Index Number Refresh

Whenever a valid packet is received with a given index number, a timer (CT3) is (re)started.

When this timer expires the local decompression directory entry for the associated index number shall be removed.

6.5.6 Processing a TYPE_RESTART Packet

When a TYPE_RESTART packet is received, the local compression directory entries associated when the sending peer system shall be removed. The associated index numbers shall become unassigned.

6.6 Multicasting

The TYPE_MULTICAST data type shall identify a TYPE_CLNP_COMPRESSED_SHORT format packet that is sent multicast to more than one destination NSAP.

Note 1.— An example of the use of TYPE_MULTICAST is a weather broadcast having a destination NSAP which indicates all hosts who want weather information, and a source NSAP indicating that the data originates from a CAA weather processor.

Note 2.—Multicast index numbers may be predefined or dynamically defined. The means to predefine multicast NSAP Addresses and associated index numbers is a local matter and outside the scope of this specification.

A PDU with a multicast destination NSAP Address that cannot be compressed into the above format shall be sent as TYPE_UNCOMPRESSED_PDU.

When a Ground Station uses predefined index numbers, the index numbers used for TYPE_MULTICAST compressed packets shall correspond to a specified and well known source NSAP Address and Destination Multicast NSAP Address. This correspondence shall be known to Ground Station and all aircraft able to receive the transmission.

6.6.1 Dynamic Assignment of Index Numbers

When index numbers are dynamically assigned then index numbers shall be assigned and maintained as for single cast communications

Note.—For example, when a Ground Station uses dynamically assigned index numbers, theTYPE_UNCOMPRESSED_CLNP packet format is used to assign the meaning of index numbers as specified in 6.4.2.

Recommendation.—*When assigning index numbers to multicast destinations, the Ground Station should use a different series of index numbers to those used for single cast communications.*

An airborne system shall use a separate local decompression directory for multicast index numbers to that used for single cast index numbers, and for each Ground System.

When a datalink is terminated, the index numbers associated with the peer system for multicast communications shall become unassigned.

When a TYPE_UNCOMPRESSED_CLNP packet is sent with a dynamically assigned index number for multicast communications, timers CT1 and CT2 shall be (re)started.

When the CT1 timer expires, the next PDU sent using this index number shall be sent in the TYPE_UNCOMPRESSED_CLNP format even if it is otherwise compressible as a TYPE_MULTICAST.

Note.—The purpose of this procedure is to ensure that aircraft that have recently joined the network have an upper bound on the length of time they are unable to decompress such PDUs.

When the CT2 timer expires, the associated index number shall become unassigned.

6.6.2 Compression of Multicast PDUs

If a PDU with a multicast Destination NSAP Address is

a) compressible according to 6.4.1,

b) may be compressed into the TYPE_COMPRESSED_SHORT format,

c) a suitable index number has been assigned, and

d) the PDU does not have to be sent as a TYPE_UNCOMPRESSED_CLNP (see 6.6.1 above), then

a compressed packet shall be constructed according to 6.4.3 and the packet transmitted multicast with a data type of TYPE_MULTICAST.

6.6.3 Reception of Multicast PDUs

When a TYPE_MULTICAST packet is received, it shall be decompressed according to 6.5.3 expect that the local decompression directory for multicast index numbers shall be used.

A decompression error shall result in the packet being discarded but the error recovery procedures shall not be followed.

When a TYPE_UNCOMPRESSED_CLNP packet is received that has a multicast destination NSAP Address, the procedures of 6.5.2 shall be applied except that the local decompression directory for multicast index numbers shall be used. If a directory entry for the index number is found, but the Source and Destination NSAP Address of the incoming packet do not match the existing directory entry then the directory entry shall be marked as unsafe and all subsequent compressed packets for this index number discarded until the index number becomes unassigned.

Additionally, a timer (CT2) shall be (re)started for each such TYPE_UNCOMPRESSED_CLNP received. When CT2 expires the associated index number shall become unassigned.

6.7 Timers

Symbol	Parameter Name	Minimum	Maximum	Default	Increment
CT1	Multicast Packet Period	1	255	5	1 packet
CT2	Multicast Refresh Timer	1	32000	180	1 second
CT3	Index Idle Timer	1	32000	20	1 minute

Table 6-2 Timers used by the CLNP Header Compression Algorithm

Note.—The default values shown are appropriate for VDL Mode 3. Other datalinks may specify different default values.

6.7.1 CT1 (multicast packet period) parameter

The Multicast Packet Period shall define the period whereby an uncompressed packet is sent to refresh the compressor state for the receiving unit.

Recommendation.—*When the underlying datalink uses XID messages to configure the datalink and set parameter values, the XID format for CT1 should be*:

Parameter ID 0 1 0 0 0 0 0 1 Multicast Packet Period

Parameter Length 0 0 0 0 0 0 0 1

Parameter Value V_8 V_7 V_6 V_5 V_4 V_3 V_2 V_1

6.7.2 CT2 (multicast refresh) timer

The Multicast Refresh Timer shall define an upper bound on the time between transmission of uncompressed headers in case message traffic is light.

Note.—This ensures the receiver can correlate the header with the compression index in a timely fashion.

Recommendation.—*When the underlying datalink uses XID messages to configure the datalink and set parameter values, the XID format for CT2 should be:*

Parameter ID 0 1 0 0 0 0 0 1 Multicast Refresh Timer

Parameter Length 0 0 0 0 0 0 1 0

Parameter Value V_{16} V_{15} V_{14} V_{13} V_{12} V_{11} V_{10} V_9

V_8 V_7 V_6 V_5 V_4 V_3 V_2 V_1

6.7.3 CT3 (index idle) timer.

The Index Idle Timer shall define an upper bound on how long the compressor shall wait before recovering an idle index.

Note.—An index is assumed idle if no message traffic has passed using it before the CT3 timer expires.

Recommendation.—*When the underlying datalink uses XID messages to configure the datalink and set parameter values, The XID format for CT3 should be*:

Parameter ID	0 1 0 0	0 0 1 0	Index Idle Timer
Parameter Length	0 0 0 0	0 0 0 1	
Parameter Value	v_{16} v_{15} v_{14} v_{13}	v_{12} v_{11} v_{10} v_{9}	
	v_{8} v_{7} v_{6} v_{5}	v_{4} v_{3} v_{2} v_{1}	