NOT MEASUREMENT SENSITIVE

MIL-STD-187-721A
22 OCTOBER 1993

MILITARY STANDARD

PLANNING AND GUIDANCE STANDARD FOR AUTOMATED CONTROL APPLIQUE FOR HF RADIO

AMSC N/A

AREA TCSS

FOREWORD

1. This military standard is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: HQ U.S. Army Information Systems Engineering Command, ATTN: ASQB-OSE-TT, Fort Huachuca, Arizona 85613-5300, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. Interoperability of DoD telecommunications systems, and of DoD with non-DoD telecommunications systems, has been and will continue to be a major consideration in the development and adoption of standards for military use.

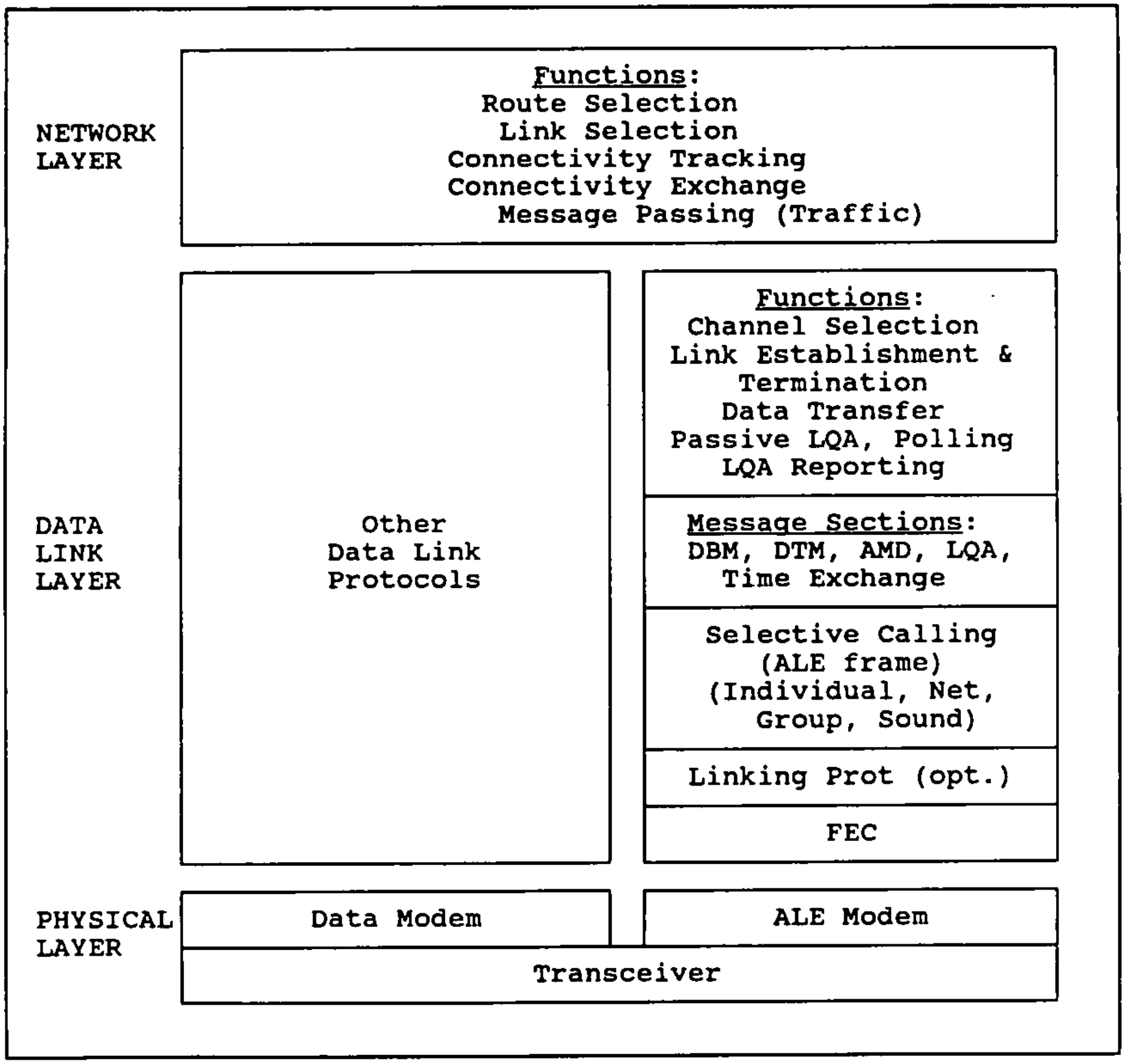
a. Military standards in the 188 series (MIL-STD-188-XXX) document telecommunications design parameters that are based on empirical data, and must be used in all new or major upgrades of inter- and intra-DoD systems and equipment to ensure interoperability.

b. Military standards in the 187 series (MIL-STD-187-XXX) document evolving telecommunications design parameters and concepts that are subject to change and that have not been adequately proven through the use of empirical test data. MIL-STD-187-XXX standards should be used as planning standards and guides until parameters are proven and included in approved federal, allied, MIL-STD-188-XXX, or DoD adopted commercial standards.

4. MIL-STD-187-XXX standards provide uniform guidance for the design of the evolving and future Defense information systems. Providing this guidance at the concept engineering stage will help to minimize ineffective designs and costly interoperability problems at later stages of implementation, as well as to assure utilization of appropriate advances in technology. Planning standards are developed considering present and future plans for the Defense Information System, commercial systems (both national and international), NATO, and other allied military systems.

5. The treatment of automatic link establishment (ALE) in MIL-STD-188-141 provides the technical foundation upon which this document rests. The second generation ALE system was one of the adaptive high frequency (HF) radio features developed through a MITRE effort in 1986. The remainder of the original concept is being documented in MIL-STD-187-721. Therefore, a brief summary of the basic principles of this ALE system is provided.

6. The principal functions included in an automated HF station are shown schematically on the figure below. This diagram is structured along the lines of the ISO Open Systems Interconnection Reference Model, with functions at each layer supporting higher layers and using lower layers.



Functional hierarchy of an automated HF station.

7. MIL-STD-188-141 specifies a basic HF radio, along with a set of robust physical and data link layer functions for ALE. The ALE modem employs 8-ary frequency shift keying (FSK) with 8

millisecond (ms) tones; the 3-bit symbols are sent at a rate of 125 per second, giving a raw data rate of 375 bits per second (bps). Forward error correction (FEC) coding is applied to the 24-bit ALE words used at the data link layer; a (24,12) Golay code is applied to each (12-bit) half of the 24-bit ALE word, producing two 24-bit results. These two 24-bit Golay words are then interleaved bit by bit, and a stuff bit is appended to produce a 49-bit word to be transmitted. Finally, each 49-bit word is sent three times, which allows the receiver to correct some errors using 2 of 3 majority voting.

8. At the receiver, received bits from the modem are (conceptually) shifted into a 99-bit register. Majority voting among the outputs of this shift register yields a 48-bit "majority word" (stuff bits are discarded), which is de-interleaved to produce two 24-bit Golay words. These are delivered to the Golay decoder, which attempts to recover a 24-bit ALE word.

9. Because no bits in the ALE word are spent on synchronization, the acquisition of word sync in this system employs a series of tests on the prospective word after each received symbol (tri-bit) is shifted in. First, the number of unanimous votes in the majority vote decoder must exceed a threshold. Next, the Golay decoder must successfully decode both halves of the 48-bit word. Finally, the resulting 24-bit ALE word must be acceptable to the ALE protocol module. Once word sync has been achieved, it is automatically tracked for the remainder of the transmission using these same tests.

10. The MIL-STD-188-141 data link layer comprises several sublayers. The lowest sublayer is concerned with error detection and correction (FEC sublayer). Above this is an optional protection sublayer (linking protection), which protects layers above it from unwanted interference. The ALE protocol is divided into three sublayers on the figure (see page iii): the lowest manages the exchange of ALE frames among stations that are specified using a standardized addressing structure; the next deals with orderwire and other message sections embedded within ALE frames; and the highest contains the data link layer functions apparent to users, such as channel selection, link establishment, and orderwire communications.

11. The contents of this document provide the technical parameters for the functions and features of advanced adaptive HF radio, and provide logical and cohesive guidelines for both industry and the Government.

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

1. SCOPE

1.1 Scope. The purpose of this document is to describe the technical parameters for adaptive high frequency (HF) radio that are more advanced than that described in MIL-STD-188-141, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment. This document is structured segmentally, with each segment being added as it is developed. Together, these segments will guide the planning of military adaptive HF radio network technology into the 21st century. The outline of MIL-STD-187-721 used in this document includes areas anticipated to be covered in other segments. These areas are referenced in this document as "not yet standardized." To fully understand and utilize this document, it is necessary to refer to portions of MIL-STD-188-141 for the basic ALE criteria.

1.2 Applicability. This standard is approved for use within the Department of Defense (DoD) in the design and development of new (adaptive) HF radio equipment. MIL-STD-187-721 contains theoretical designs and solutions that may have been supported by desk top analysis and modeling, but contains technology that has not been imbedded into hardware/software or undergone proof of concept testing.

1.3 Application guidance. MIL-STD-187-721 is a planning standard, organized in segments to allow the various functions and features of adaptive radio to be documented separately to encourage technical development. MIL-STD-188-141 contains only technical documentation that is supported by empirical data; whereas this standard documents the advanced techniques, providing a greater level of technology, but not yet supported by test data. Either a DoD user or an industry manufacturer may develop hardware or software implementations of technical parameters described in a MIL-STD-187-XXX document. A manufacturer may wish to implement the technical parameters described in this document in order to be first in a market offering, thereby, gaining market and advertising advantage. Also, a DoD user organization may have a requirement for technical features described in this document and include MIL-STD-187-721 in an acquisition contract, thereby, causing the development of the equipment or software as a part of the contractor's effort. Whether a manufacturer implements a MIL-STD-187-721 function using "venture capital" or a Government agency "sponsors" the development through inclusion in a contract, the result is the same; testable hardware/software and empirical data. This empirical data allows the MIL-STD-187-721 segment (wholly or in part) to migrate into a MIL-STD-188 series document. This process provides a logical and orderly progression while assuring a level playing field for Government and industry alike.

2. APPLICABLE DOCUMENTS

2.1 Government documents.

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DODISS) and supplement thereto, cited in the solicitation.

STANDARDS

FEDERAL

FED-STD-1037	- Telecommunications: Glossary of Telecommunications Terms.

MILITARY

MIL-STD-188-141	- Interoperability and Performance Standards for Medium and High Frequency Radio Equipment.

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Naval Publications and Forms Center, ATTN: NPODS, 5801 Tabor Avenue, Philadelphia, PA 19120-5099.)

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

USAISEC

Technical Report No. ASQB-OSI-S-TR-92-04	- A 24-Bit Encryption for Linking Protection (Johnson Algorithm).

2.2 Non-Government publications. None.

2.3 Order of precedence.

In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Terms. Definitions of terms used in this document are in accordance with (IAW) the current edition of FED-STD-1037. In addition, the following definitions are applicable for the purposes of this standard.

a. Application level 0 (AL-0) - In adaptive radio, the unprotected application level of linking protection.

b. Application level 1 (AL-1) - In adaptive radio, the unclassified, least protected application level of linking protection.

c. Application level 2 (AL-2) - In adaptive radio, the unclassified, enhanced application level of linking protection.

d. Application level 3 (AL-3) - In adaptive radio, the unclassified but sensitive application level of linking protection.

e. Application level 4 (AL-4) - In adaptive radio, the classified application level of linking protection.

f. Linking protection (LP) - In adaptive radio, a technique that protects the linking functions from unintentional or malicious interference by scrambling the ALE signaling exchanged among protected stations for cryptographic authentication of HF ALE signaling.

g. Protection interval (PI) - In linking protection, transmissions are encrypted using time-varying randomization data. The period between changes in the time of day portion of this randomization data is termed a protection interval.

3.2 Abbreviations and acronyms. The abbreviations and acronyms used in this document are provided below. Those listed in the current edition of FED-STD-1037 have been included for the convenience of the reader.

a. ACK - acknowledge.

b. ADC - available data capacity.

c. AI - articulation index.

d. AL-0 - unprotected application level.

e. AL-1 - unclassified application level.

f. AL-2 - unclassified enhanced application level.

g. AL-3 - unclassified but sensitive application level.

h. AL-4 - classified application level.

i. ALE - automatic link establishment.

j. ALQA - advanced link quality analysis.

k. AMD - automatic message display.

l. AME - automatic message exchange.

m. ARQ - automatic repeat-request.

n. ASCII - American Standard Code for Information Interchange.

o. AVQ - achievable voice quality.

p. BBS - bulletin board system.

q. BER - bit error ratio.

r. bps - bits per second.

s. CMD - ALE preamble word COMMAND.

t. COMSEC - communication security.

u. CONEX - connectivity exchange.

v. CQM - channel quality measure.

w. CRC - cyclic redundancy check.

x. DATA - ALE preamble word DATA.

y. dB - decibel.

z. DBM - data block message.

aa. DO - design objective.

ab. DoD - Department of Defense.

ac. DODISS - Department of Defense Index of Specifications and Standards.

ad. DTM - data text message.

ae. EFI - error-free interval.

af. FEC - forward error correction.

ag. FSK - frequency shift keying.

ah. GPS - Global Positioning System.

ai. HF - high frequency.

aj. Hz - Hertz.

ak. IAW - in accordance with.

al. ICD - interface control document.

am. ISO - International Organization for Standardization.

an. kHz - kilohertz.

ao. LP - linking protection.

ap. LPCM - linking protection control module.

aq. LPM - link performance measure.

ar. LQA - link quality analysis.

as. lsb - least significant bit.

at. MHz - megahertz.

au. MP - multi-path.

av. ms - millisecond.

aw. msb - most significant bit.

ax. NCS - net control station.

ay. NPODS - Naval Print on Demand System.

az. NSA - National Security Agency.

ba. OSI - open systems interconnection.

bb. OSI--RM - Open Systems Interconnection--Reference Model.

bc. PBER - pseudo bit error ratio.

bd. PI - protection interval.

be. ppm - parts per million.

bf. REP - ALE preamble word REPEAT.

bg. RF - radio frequency.

bh. SD - spectral distortion.

bi. S&F - store and forward.

bj. SINAD - signal-plus-noise-plus-distortion to noise-plus-distortion ratio.

bk. TOD - time of day.

bl. UTC - coordinated universal time.

bm. USAISEC - U.S. Army Information Systems Engineering Command.

bn. VF - voice frequency.

3.3 Timing symbols.

a. T_{lc} - leading call phase.

b. T_{lww} - last word wait time.

c. T_{rs} - redundant sound phase.

d. T_{rw} - redundant word time.

e. T_{sc} - scanning call phase.

3.4 ALQA mathematical expressions.

a. E_i - effective sensation level of energy in a speech sub-band (AI).

b. F_i - weighting factor relating human sensitivity to energy in a speech sub-band to measured energy in that sub-band (AI).

c. L_f - length of messages in queue when message transfer finishes (ADC).

d. L_m - length of message body (ADC).

e. L_s - length of messages in queue when message transfer begins (ADC).

f. R - effective message data rate (ADC).

g. T_b - beginning time of message transfer (ADC).

h. T_f - time when message transfer finishes (ADC).

i. U - station utilization (ADC).

j. W_i - non-linearly scaled sub-band energy (AI).

4. GENERAL REQUIREMENTS

4.1 Data link sublayers. The MIL-STD-188-141 data link layer contains three sublayers: a lower sublayer concerned with error correction and detection (forward error correction [FEC] sublayer), an upper sublayer containing the automatic link establishment (ALE) protocol (ALE sublayer); and an optional protection sublayer in between, as shown on figure 1. Within the FEC sublayer are redundancy and majority voting, interleaving, and Golay coding applied to the 24-bit ALE words which constitute the (FEC sublayer) service-data-unit, in terms of the International Organization for Standardization (ISO) model. The ALE sublayer specifies protocols for link establishment, data communication, and rudimentary link quality analysis (LQA) based on the capability of exchanging ALE words. Linking protection (LP) is placed in the intermediate "protection" sublayer so that it may make full use of the error correcting power of the FEC sublayer while intercepting unauthorized attempts to communicate with the local ALE protocol entity to establish links or otherwise disrupt operations.

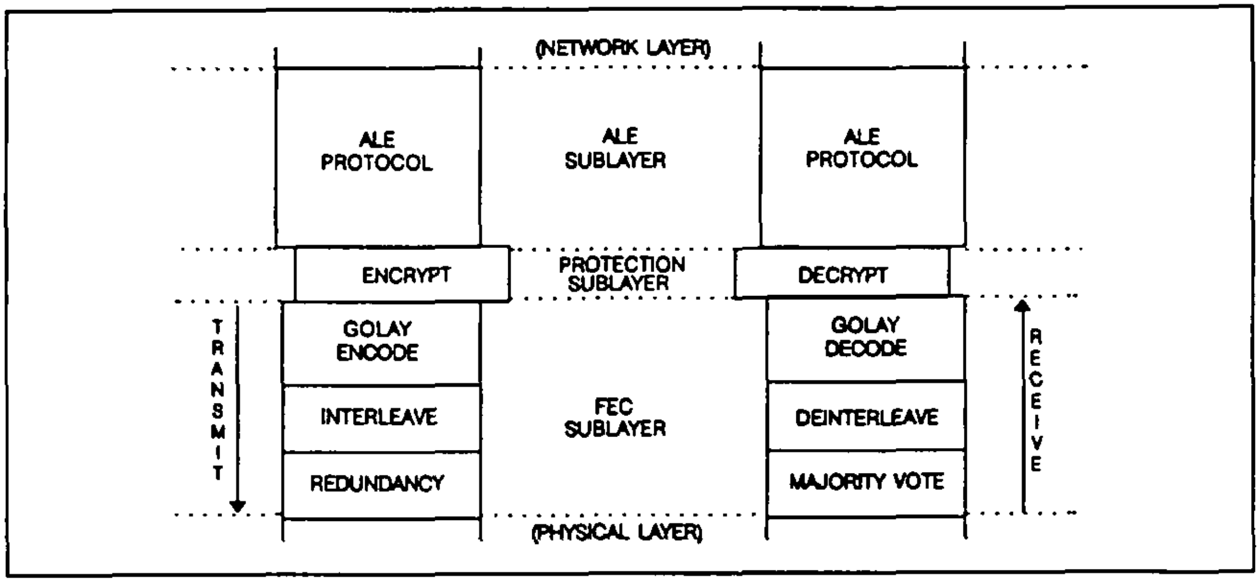


FIGURE 1. Conceptual model of data link layer protocols in MIL-STD-188-141.

4.2 Linking protection.

a. LP is intended to prevent the establishment of unauthorized links, and does this through an authentication process. (Some cryptographic protection is provided to the ALE words by the LP mechanism, but this is not the primary purpose of LP.)

b. Block diagrams of the data flow through unprotected and protected radios are shown on figures 2a and 2b. The blocks on the figures represent logical operations only, and do not necessarily represent distinct hardware modules.

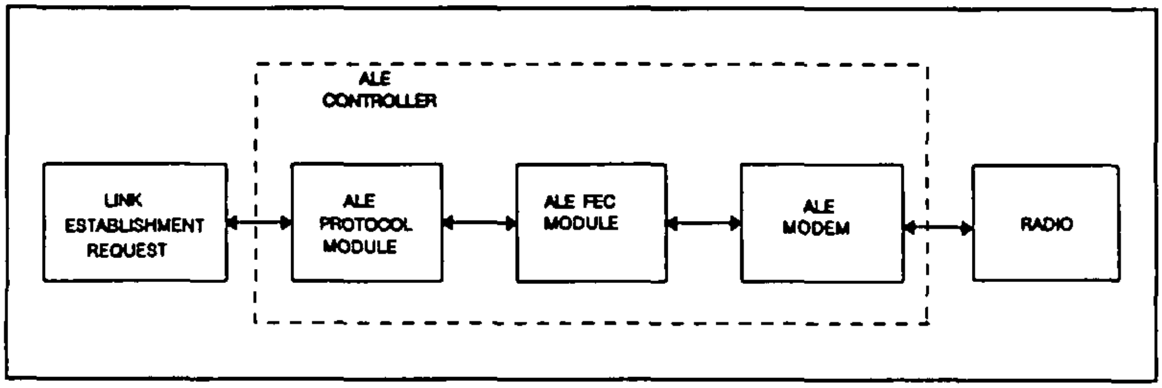


FIGURE 2a. Data flow in a system without LP.

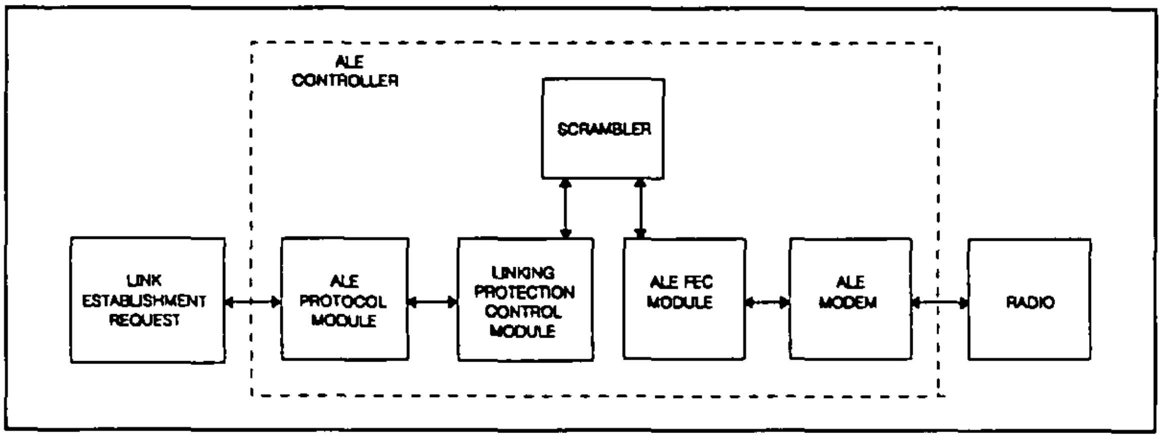


FIGURE 2b. Data flow in a protected system.

c. LP is achieved by encrypting ALE words under a private key that is changed periodically using known "randomization" information (frequency, time, date, etc.) to vary the results of this encryption on a shorter basis (a "protection interval [PI]"). The private key is entered directly into the scrambler via an appropriately protected circuit, and is protected during use by the design of the scrambler.

d. The addition of LP to a radio involves adding the functions of a linking protection control module (LPCM), that implements the LP protocol, and a scrambler, that scrambles ALE words under the control of the LPCM. The security of the system is based upon the inability of an adversary to "spoof" the LPCM, and relies on the difficulty of discovering the key used to scramble the ALE words. Because of the wide range of applications for LP, several different scramblers are specified; however, the LPCM function is common to all LP applications, as is a common denominator scrambler for assured interoperability of all protected radios.

e. Note that the existing LPCM handles unclassified ALE words only. Any classified traffic must be encrypted by a National Security Agency (NSA) approved cryptographic device; the resulting BLACK data may then be sent through the ALE controller or via a separate data modem.

4.2.1 Linking protection application levels. The following application levels of LP are defined in this section, with the classified application (AL-4) providing the highest degree of protection. The classified and unclassified but sensitive application levels (AL-4 and AL-3 respectively) require distinct hardware scramblers, while the unclassified enhanced application level and the unclassified application level (AL-2 and AL-1 respectively) scramblers may be implemented in software or firmware. All protected radios shall be capable of operation at AL-1. A method shall be provided to disable automatic linking at linking protection application levels less secure than the application level in use by the station being called. For example, a station which is operating at AL-3 shall be able to disable the receiver from listening for linking attempts at AL-0 through AL-2. (Design objective [DO]: Alert the operator but do not link automatically when a valid call is received from a transmitter with a lower linking protection application level.) This mechanism shall not preclude the operator from manually initiating ALE using a disabled application level. This manual override is required for interoperability.

4.2.1.1 AL-0 (unprotected application level). AL-0 indicates that no linking protection is being employed. No protection is provided against interfering, unintentional, or malicious linking attempts.

4.2.1.2 AL-1 (unclassified application level). The AL-1 scrambler shall employ the lattice encryption algorithm as specified in U.S. Army Information Systems Engineering Command (USAISEC), Fort Huachuca, Arizona, Technical Report, ASQB-OSI-S-TR-92-04, A 24-bit Encryption Algorithm for Linking Protection, March 1992. The AL-1 scrambler may be implemented in hardware or software with manufacturer specified interfaces. This scrambler is for general U.S. Government and commercial use. This application level is mandatory for all protected radio systems, and therefore provides protected interoperability within the U.S. Government. The AL-1 protection interval is 60 seconds, which provides slightly lower protection than that available using the unclassified enhanced application level, but which permits relaxed synchronization requirements.

4.2.1.3 AL-2 (unclassified enhanced application level). The AL-2 scrambler shall employ the same algorithm as specified for the AL-1, and may be implemented in hardware or software, with manufacturer specified interfaces. This scrambler is for general U.S. Government and commercial use. The AL-2 protection interval is 2 seconds.

4.2.1.4 AL-3 (unclassified but sensitive application level). The AL-3 scrambler (for U.S. Government use only) shall employ the algorithm and the interface control document (ICD) developed by NSA. Systems employing AL-3 LP must meet NSA security requirements. The protection interval is a maximum of 2 seconds.

4.2.1.5 AL-4 (classified application level). The AL-4 scrambler (for U.S. Government use only) shall employ the algorithm and the ICD developed by NSA. An AL-4 scrambler may be used to protect classified orderwire traffic. Systems employing classified application level LP must meet NSA security requirements. The AL-4 protection interval is a maximum of 1 second.

4.2.2 Protocol transparency. A principal consideration in implementing LP is that the presence of an LP module in a radio (or its controller) shall have no impact on any protocols outside of the protection sublayer in the data link layer. This means that achieving and maintaining crypto-sync must occur transparently to the ALE waveform and protocols. Furthermore, scanning radios must be able to acquire crypto-sync at any point in the scanning call portion of a protected transmission if this transmission was encrypted under the key in use by the receiving station. Thus, LP modules shall not insert sync bits into the data stream, and must acquire crypto-sync without the use of synchronization preambles or message indicator bits.

4.2.3 Transmit processing. The LP module in a sending station encrypts each 24-bit ALE word to be sent using the seed data then in use (frequency, PI number, word number, etc.; see 5.1.1.3) and delivers the encrypted word to the FEC module. (Data block message [DBM] mode is a special situation; see 5.1.2.3.)

4.2.4 Receive processing.

a. The receive side of an LP module is responsible for achieving crypto-sync with transmitting stations, and for decrypting protected ALE words produced by the Golay decoder. In operation, when a scanning receiver arrives at a channel carrying valid tones and timing, the FEC sublayer (majority voter, de-interleaver, and Golay decoder) shall process the output of the ALE modem and alert the LP receive module when an acceptable candidate word has been received. (This occurs roughly once every 8 milliseconds [ms] when the Golay decoders are correcting 3 errors, or once every 78 ms when correcting 1 error per Golay word.)

b. The receive LP module must then decipher the candidate words, and pass them to the receive ALE module which determines whether word sync has been achieved by checking for acceptable preamble and ASCII subset. This task is complicated by the possibility that the received word (even if properly aligned) may have been encrypted using a different PI than that currently at the receiver, requiring the receiving LP module to decrypt each candidate word under several seeds. (Seeds are discussed in 5.1.1.3.)

c. A further complication is the possibility that a word may satisfy the preamble and character set checks under multiple seeds. When this occurs, the valid successors to all seeds which produced valid words shall be used to decrypt the next word, and each result shall be evaluated in the context of the corresponding first word. The probability is increasingly minute that multiple PI possibilities will exist after this second word is checked. For example, if during a scanning call (or sound) a received word decrypts to "TO SAM" using seed A, and to "DATA SNV" using seed B, the next word is decrypted using the successors to those seeds, denoted A′ and B′. If the result of decrypting this next word under A′ is not "TO SAM", the first decrypt under seed A was invalid, because the word following a "TO" word in a scanning call must be the same "TO" word. To be valid in a leading call or sound, the word following "DATA SNV" must have three ASCII-38 characters and either "TO", "REPEAT", "THIS IS", or "THIS WAS" preamble. A diagram showing all valid preamble sequences can be found on the figure titled Valid Word Sequence in MIL-STD-188-141.

4.3 Time of day (TOD) synchronization.

a. Because LP employs protection intervals, which are time-based, all stations must maintain accurate TOD clocks. Practical considerations suggest that station local times may differ by significant fractions of a minute unless some means is employed to maintain tighter synchronization. Because the effectiveness of LP increases as the length of the PI decreases, there is a trade-off between protection and the cost of implementing and using a time synchronization protocol.

b. Operators must synchronize station time to a common time source to be within one minute (±30 seconds) and then employ a protocol to synchronize stations to be within one or two seconds (fine sync) for enhanced linking protection. While operating networks with only coarse (one minute) time synchronization, the protection offered by this system against playback (tape recorder) attacks is reduced.

c. Synchronization of local times for LP requires some cooperation between the protocol entity and the LP time-base. One concept of how the coordination across the ALE-LP sublayer boundary may be effected in this case is as follows:

(1) TOD is maintained by the ALE entity, and is provided to the LP entity as required.

(2) The transmit LP entity uses the TOD provided by the transmit ALE entity to form seeds during the scanning call phase (T_{sc}) and for the initial time setting for the leading call phase (T_{lc}). Thereafter, the TOD from ALE is ignored and the transmit LP entity sequences seeds IAW 5.1.2.1.

(3) On the receive side, seed sequencing is performed by the functions responsible for achieving and maintaining word sync. These functions may be implemented within either the LP or the ALE module, but must know the current phase of the ALE protocol (e.g., T_{sc}, T_{lc}, etc.).

(4) For authentication of unprotected time exchanges, the ALE module must be able to call upon the LP module to encrypt and decrypt individual ALE words "off line."

4.4 Link quality functions. Link quality functions, including passive LQA, polling, and LQA reporting, support a data base of recent propagation measurements of the channels available to a station for establishing links with other stations. This data base of bilateral link quality data, stored in the LQA matrix described in MIL-STD-188-141, is used to rank channels for the order in which to attempt link establishment and to select channels for voice and data traffic. LQA data is obtained from measurements of received traffic, sounds, and from data explicitly sent in the polling and LQA report protocols.

4.4.1 Passive LQA.

a. Evaluation of channel quality by measuring the characteristics of received signals is termed passive LQA because the local radio does not transmit a request for this data. Such passive LQA can obtain useful data from normal ALE traffic (while liked) as well as from sounds.

b. A key characteristic of passive LQA is the data it produces is unilateral; only the link quality from the distant transmitter to the local receiver is obtained.

NOTE: Certain military applications prevent use of active LQA techniques.

4.4.2 Polling.

a. Bilateral LQA data may be obtained using one of the active LQA techniques such as polling or LQA reporting.

b. The polling protocols are used to acquire current bilateral link quality data by handshaking with one or more other stations, directly measuring the transmissions received, and exchanging these measurements with the other station(s). Polling is used to actively acquire current bilateral LQA data for stations and channels for which recent LQA data may be unavailable in the LQA matrix.

c. LQA is mandatory in MIL-STD-188-141; existing radios can execute any polling protocol that does not depart from the standard ALE protocols. The protocols specified in section 5 support polling existing radios. Advanced polling protocols that provide greater efficiency of channel use are also specified.

4.4.3 LQA reporting. The LQA reporting protocol is used to exchange previously-measured LQA data, rather than to measure the quality of the current channel. This data may be from either active or passive sources. By exchanging unilateral measurements from passive LQA, stations can quickly accumulate bilateral data for many channels and stations.

4.5 Advanced link quality analysis (ALQA) function. ALQA link quality measures are divided into two types: channel quality measures and link performance measures. Channel quality measures evaluate the performance of individual channels between pairs of stations, while link performance measures combine measures of channel performance and traffic load to derive a single quantitative measure of link performance for use by network controller routing algorithms. ALQA techniques (except for error-free interval estimation) differ from the basic LQA techniques in the following respects:

a. Measurements shall be histogrammed in accordance with 4.5.3 rather than averaged.

b. The quality of a channel shall be reported as the fraction of measurements that exceeded a threshold in accordance with 5.5.3, rather than an average of the measurements.

4.5.1 Channel quality measures. All implementations of ALQA shall support signal-plus-noise-plus-distortion to noise-plus-distortion ratio (SINAD) and pseudo bit error ratio (PBER) as described in 5.5.1.1. Articulation index, spectral distortion, and error-free interval are optional; implementations shall comply with the applicable sections of 5.5.1. The following channel quality measures are standardized for ALQA:

a. SINAD measurements shall be derived from the automatic link establishment (ALE) modem on a baud-by-baud time scale (see 5.5.1.1).

b. Articulation index estimates shall also be derived from the ALE modem, using a non-uniform weighting of signal-to-noise ratios from each ALE tone (see 5.5.1.2).

c. PBER shall be derived from the majority vote decoder as described in MIL-STD-188-141. However, for ALQA use, the PBER values shall be histogrammed on a word-by-word basis, rather than contributing to a running average for the transmission (see 5.5.1.1).

d. Spectral distortion due to fading and multipath effects, causes degradation in the bit error ratio (BER) performance of the ALE modem, as compared to its performance over Gaussian noise channels. The severity of spectral distortion shall be gauged by comparing instantaneous samples of BER and SINAD (measured on received ALE words) to the theoretical Gaussian channel performance in accordance with 5.5.1.3.

e. The mean error-free interval shall be evaluated indirectly. ALE word errors detected by the Golay decoder and the ALE protocol shall be accumulated to estimate word-error and word-error-burst probabilities; these probabilities shall then be used to estimate error-free interval in accordance with 5.5.1.4.

4.5.2 Link performance measures. The link performance measures for ALQA are standardized as follows:

a. Achievable voice quality samples shall combine SINAD measurements (design objective [DO]: articulation index measurements) with channel occupancy to produce a histogram of the voice quality of the best channel available during each scan of the channels by the ALE controller, in accordance with 5.5.2.1.

b. Data link performance shall be gauged using available data capacity in accordance with 5.5.2.2. Available data capacity samples measure the effective data rate available to each station, including the effects of retransmissions due to channel errors, and contention for transmission facilities from other traffic.

NOTE: Achievable voice quality and available data capacity are optional; implementations shall comply with the applicable sections of 5.5.2.

4.5.3 ALQA histogramming. Measurements of SINAD, PBER, articulation index, spectral distortion, achievable voice quality, and available data capacity shall be accumulated for ALQA use as described below.

4.5.3.1 Exceedance distributions. An "exceedance distribution" $Q_X(x)$ is related to the cumulative probability distribution function $P_X(x)$:

$$Q_x(x) = Pr[X > x] = 1 - P_x(x).$$

Exceedance distributions for the channel quality measures and link performance measures listed in 4.5.3 shall be estimated by first histogramming samples of these measures, and then averaging the histograms over the integrating periods specified in 4.5.3.2. A history of these histograms shall be retained for use when no current data is available.

4.5.3.2 Integrating periods.

a. Four distinct time epochs shall be used for accumulating the histogram data. Within each epoch k, N_k histograms shall be accumulated and averaged, each containing measurements over a period of t_k. Epoch 1 represents the short term for the HF channel. Because the values defined in the channel quality measure descriptions above are intended to provide short-term granularity on the HF channel on the order of 1 minute, $t_1 = 60$ seconds. Since 15 minutes represents a time interval over which the statistics of the nominal HF channel may be considered approximately stationary, $N_1 = 15$. This first epoch represents the most up-to-date channel quality measure available.

b. The second, third, and fourth time epochs shall consist of 5 minute intervals up to 1 hour old (second epoch), hourly intervals from the current hour to 24 hours (third epoch), and cumulative results since start-up (fourth epoch). Epoch 2 employs $t_2 = 300$ seconds and $N_2 = 12$ so that five t_1-length samples from epoch 1 are summarized in each t_2-length sample ($t_2 = 5t_1$) in epoch 2. Similarly, epoch 3 consists of 24 1-hour samples: $t_3 = 3600$ seconds and $N_3 = 24$. Finally, epoch 4 contains counters which accumulate all samples.

4.5.3.3 Histogram generation.

a. For each channel quality measure or link performance measure X, where X is one of the channel quality measures or link performance measures listed in 4.5.3, sets of bins $h_X(i;\ j,\ k)$ shall be used to store exceedance histograms of the samples x of that measure as described below, for every channel to every reachable station. In the notation $h_X(i;\ j,\ k)$, the index k refers to an epoch ($1 \leq k \leq 4$), the index j refers to a particular exceedance histogram (set of bins) within that epoch ($1 \leq j \leq N_k$), and the index i refers to a particular bin within that histogram (see figure 3). In addition, for each epoch, a set of counters shall be used to accumulate current measurements to form the next set of histograms; these counters are labeled as $j = 0$ in the figure.

b. For the purpose of histogramming, the range of values for each measure shall be quantized into a number of subranges with lower thresholds in accordance with table XVII, (page 65) plus an additional (lowest) subrange with a threshold less than any valid sample. As each sample arrives, it shall be compared to the lower endpoint of each subrange. Each counter shall be incremented if the sample *exceeds* the lower endpoint of the subrange corresponding to that counter. Because the lower endpoint of the lowest subrange is always less than the smallest possible value, bin 1 in each exceedance histogram will contain a count of the total number of samples represented in that histogram. Because the same thresholds are used for each of the four epochs, only one quantizer is needed. Each epoch independently accumulates the samples as they arrive.

c. For each epoch, when an integrating period t_k has elapsed, the histograms shall be shifted one position to the right; the counter contents shall become $h_X(; 1, k)$, and the oldest histogram $h_X(; N_k, k)$ shall be discarded. Epoch 4 is a special case; epoch 4 counters shall simply accumulate all samples, with no averaging over individual integrating periods.

d. For epochs 1 through 3, the running average histograms $H_X(k)$ shall be computed from the most recent N_k histograms $h_X(i; j, k)$ as follows (each bin in H_X is denoted $H_X[i; k]$):

$$H_x(i;k) = \frac{1}{N_k} \sum_{j=1}^{N_k} \frac{h_x(i;j,k)}{h_x(1;j,k)} .$$

$$\text{where } h_x(1;j,k) \neq 0$$

4.5.4 <u>Link quality prediction programs</u>. Link quality predictions from programs such as IONCAP may be used, when available to the ALE controller, to supplement channel quality measures.

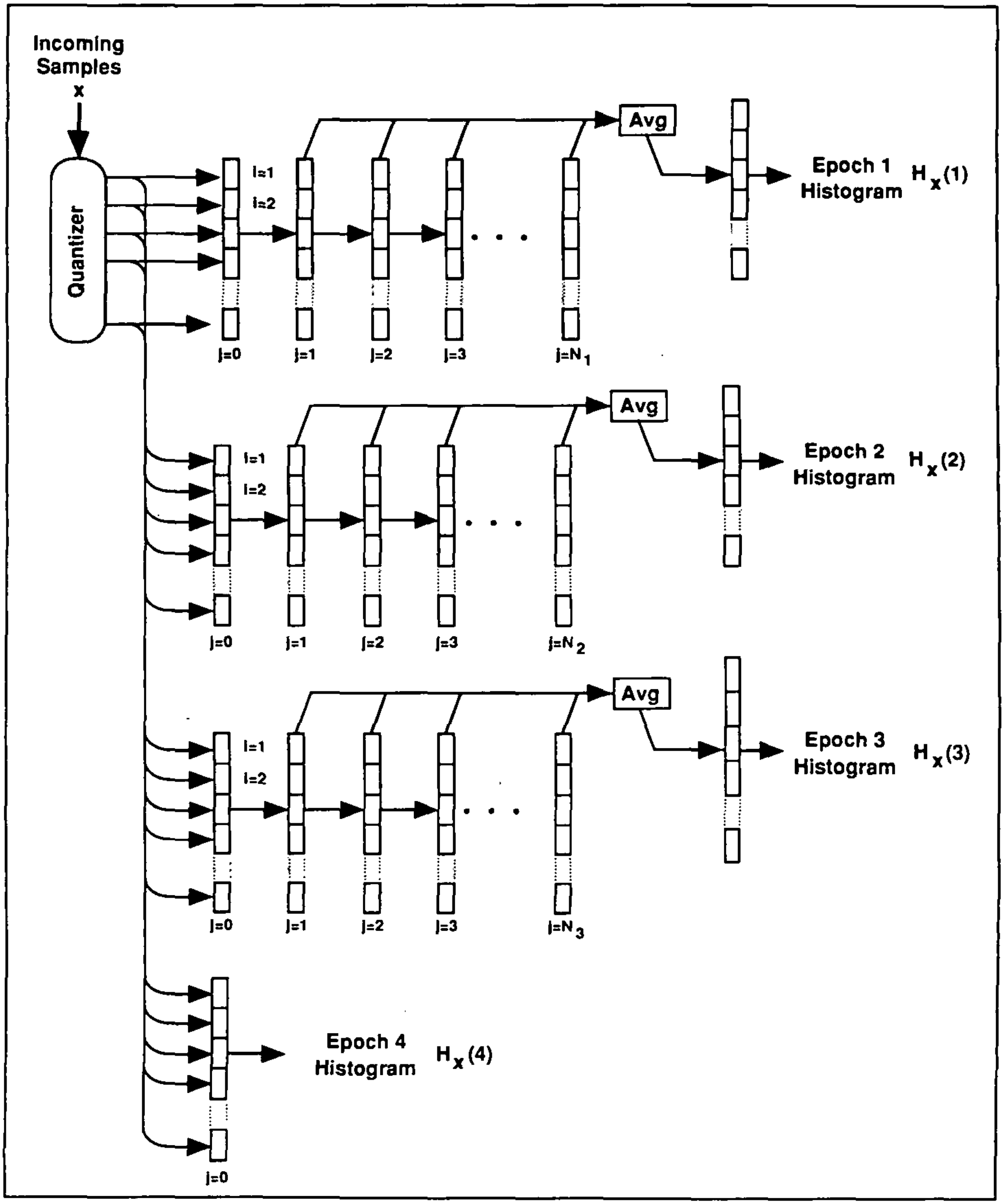


FIGURE 3. Histogram generation.

4.6 Networking functions.

a. MIL-STD-188-141 establishes the technology baseline needed for establishing and maintaining links among HF radio stations. Networking technology augments this capability for direct connections with the ability to find and use indirect routes.

b. The functions performed at the network layer may be grouped into two broad categories: routing functions and data management functions. Routing functions select paths through the network for voice and data traffic, using some stored information (provided by operators, local data link controllers, and remote networking controllers) about the quality of available links to other stations. Data management functions acquire and communicate that information.

c. Link-level data directly characterize the quality of single-link paths, and are used to compute end-to-end path quality for multiple-link paths through relays. These results are stored in a path quality matrix, which is organized to provide the path quality to any reachable destination via each directly reachable relay station. From this path quality data, a routing table is formed. This table lists the best path to each reachable station for various types of communication (e.g., voice, data, etc.).

4.6.1 Indirect calling and relaying. When a station cannot directly link with a desired destination, other stations may be employed to assist in getting the message through. The simplest option, termed indirect calling, establishes a link with a station other than the desired destination so the station operators can manually communicate (using either voice or data orderwire) after the fashion of a torn-tape relay. When the equipment at the intermediate station is able to automatically establish an indirect path to the destination, this is termed relaying. A variety of relaying techniques are possible, some of these are shown on figure 4 where these techniques are differentiated by where the cross-connection occurs in the protocol stack. Each alternative is briefly discussed in table I.

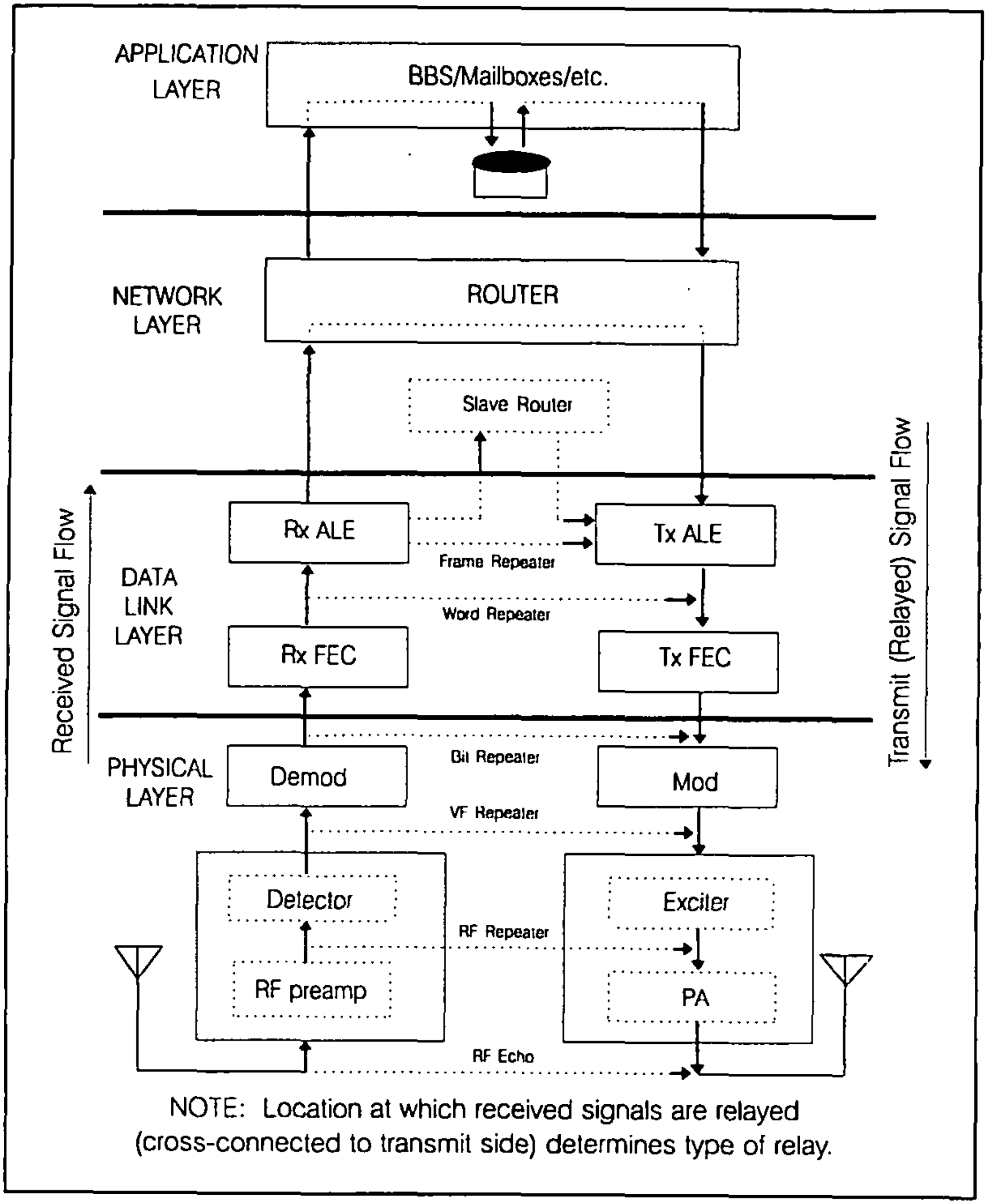


FIGURE 4. Relaying alternatives.

TABLE I. Relaying alternative notes.

Type	Description
RF echo	No radios required. Examples: float a large aluminized balloon, or use a billboard reflector.
RF repeater	Formed by connecting an RF amplifier between two antennas. Uses different RF frequencies by heterodyning or translating the received frequencies.
VF repeater	Formed by connecting two radios back-to-back through the audio ports. This and all following relays can easily use different RF frequencies.
Bit repeater	Formed by connecting data ports of modems. Regenerates audio and bit timing.
Word repeater	Occurs just above FEC sublayer. Corrects errors in ALE words but does not examine those words or otherwise manipulate their contents. Introduces one T_{rw}* delay.
Frame repeater	Occurs within the ALE sublayer. Like word repeater, but buffers an entire frame before retransmitting it; introduces delay of frame time plus at least T_{lww}**. This and all following relays require only one radio, but can use more if available.
Slave router	Occurs just above data link layer. Effectively connects data links in tandem as directed by indirect addresses in data link frames. Rotates the indirect addresses, but does not interpret message section. Makes no routing decisions; merely implements the routing scheme specified in frames that it receives (hence the name).
Router	Network layer function. Determines where to send each received frame using local routing information; this routing information may be entirely static, or it may include real-time data (in an adaptive router). Uses network layer message header; normally has access only to message section of data link layer (e.g., ALE) frame. May buffer data when no path currently exists to destination.
Mailbox	Application layer function. Stores messages for later retrieval by specified recipient.
BBS	Application layer function. Stores messages for later retrieval by anyone with access to that bulletin board.

* Transmission time for redundant ALE word: 392 ms.

** Last word wait delay at receiver to detect end of ALE frame: 392 ms.

4.6.2 Networking controller. The principal service provided by the network layer is the routing of communications, traffic among stations, and other networks. A networking controller implements network-layer traffic routing. In its simplest case, the network layer functions reside within a radio and have access only to links achievable by that radio. A more advanced radio may include MIL-STD-188-141 ALE, MIL-STD-188-110 data modem, and other HF data modems along with a networking controller capable of establishing links using the ALE modem and protocols, and switching to the data modem for data communication (see figure 5). Such a networking controller could use either (ALE or DATA) of the modems (via its respective data link layer entity) to carry traffic for the local user or to relay other users' traffic within the network. A still more sophisticated networking controller could manage several radios in a major communications hub, routing traffic through the radio that has the best path to the destination. Such a networking controller could be generalized to act as an internetwork gateway, routing traffic over media such as wire, fiber, microwave, and satellite links as well as HF links.

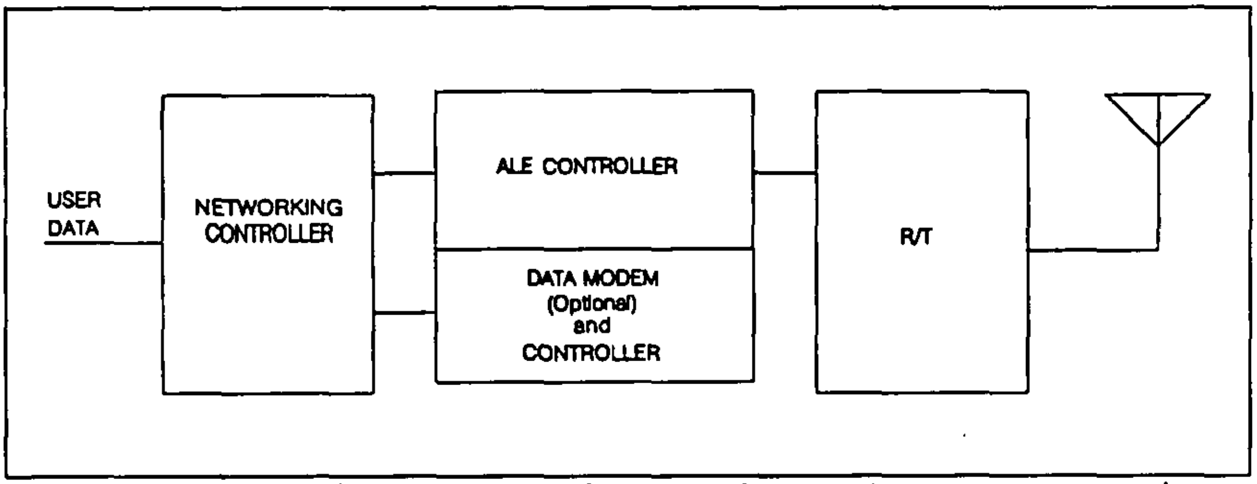


FIGURE 5. Functional block diagram of an automated HF station.

4.6.2.1 Data structures. Not yet standardized.

4.6.2.2 Route selection. Not yet standardized.

4.6.2.3 Message store and forward. Not yet standardized.

4.6.2.4 Automatic message exchange. Not yet standardized.

4.6.2.5 Link selection. Not yet standardized.

4.6.2.6 Connectivity exchange. Information about routes to stations that are not directly reachable, and which have not routed traffic through the local station recently, can sometimes be obtained from the connectivity data stored by a directly reachable station. This data may be shared either upon request, or by periodic broadcast. When stations report their path quality matrix contents to other stations, this is termed connectivity exchange (CONEX). When a station asks for replies from stations with connectivity to a specified destination, on the other hand, this is termed query routing (e.g., "Who can reach Joe?"). Protocols for both functions are specified in section 5.

4.7 Interface to link controllers. The following functions form a minimal interface between a networking controller and link controllers that it uses. Due to the wide range of possible implementations, the specifics of this interface are not yet standardized.

4.7.1 Data link control. The networking controller shall be able to request the establishment and termination of links to other stations.

4.7.2 Link quality reporting. The networking controller requires reports from the link controllers regarding the quality of links to other stations available from each link controller. These reports will specify the data necessary for path quality matrix entries (bit error ratio [BER], signal-plus-noise-plus-distortion to noise-plus-distortion ratio [SINAD], etc.), but will not contain data such as channel numbers that are relevant only to the link controller (see 5.4.4).

4.7.3 Network messages. Messages to be sent from one networking controller to another over a link will be delivered to a link controller in two parts: a network message, which is handled transparently by the link controller, and control information, which specifies to the link controller the data link layer addressee of the message as well as other requirements for the transmission.

4.8 Network management. Not yet standardized.

4.9 Multi-media networking. Not yet standardized.

4.10 Special requirements. Not yet standardized.

5. DETAILED REQUIREMENTS

5.1 Linking protection.

a. The LP procedures specified herein shall be implemented as distinct functional entities for the control functions and cryptographic functions. (Unless otherwise indicated, however, distinct hardware for each function is not required.) The LPCM shall perform all control functions specified herein and interface to the ALE controller as shown on figure 2b. Scrambler(s) shall perform all cryptographic operations on ALE words under the control of the LPCM.

b. Use of LP shall neither increase the time to establish a link compared to a non-protected radio, nor degrade the probability of linking below the requirements for non-protected linking (see MIL-STD-188-141 table titled Probability of Linking).

c. A means shall be provided to disable the LP functions and operate the radio in clear (unprotected) mode. Hardware scramblers shall be removable without impairment of the unprotected functionality of a radio.

5.1.1 Linking protection control module. The LPCM shall execute the LP procedure specified in 5.1.2 and control the attached scrambler(s) as specified below.

5.1.1.1 Scrambler interfaces. The LPCM shall interact with hardware scrambler(s) IAW the circuits and protocols specified in the ICD for each scrambler (see 4.2.1). Interaction with software implementations of scramblers shall comply with the applicable function call ICD, when specified.

5.1.1.2 Time and date. The LPCM requires accurate time and date for use in the LP procedure. The local time base shall not drift more than ±1 second per day when the station is in operation.

5.1.1.2.1 Time of day (TOD) entry. A means shall be provided for entry of time of day (date and time) via: (1) an operator interface; and (2) an electronic fill port such as an interface to a Global Positioning System (GPS) receiver. This interface may also provide for the entry of a measure of uncertainty of the time entered. If time uncertainty is not provided, a default time uncertainty shall be used. Defaults for the various time fill ports may be separately programmable; unless otherwise programmed, the default uncertainty shall be within ±15 seconds.

5.1.1.2.2 Time exchange protocols. After initialization of TOD, the LPCM shall execute the time protocols of 5.2 as required to maintain total time uncertainty less than the protection interval length of the most secure LP application level it is using. The LPCM shall respond to time requests IAW 5.2.3.2 unless this function is disabled by the operator.

5.1.1.3 Seed format.

a. The LPCM shall maintain randomization information for use by scrambler(s), and shall provide this information, or "seed," to each scrambler IAW the applicable ICD.

b. The 64-bit seed shall contain the frequency carrying the protected transmission, the current PI number, the date, and a word number, in the format shown on figure 6. The most significant bits of the seed and of each field are on the left. The TOD portion of the seed shall be monotonically non-decreasing; the remaining bits are not so constrained.

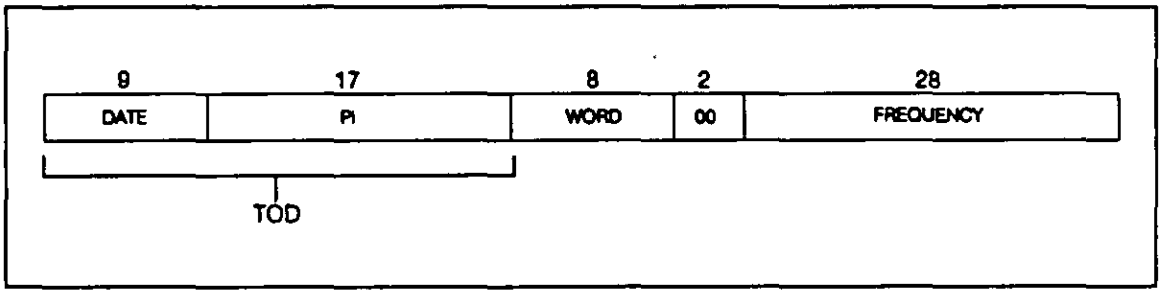


FIGURE 6a. Seed format.

c. The Date field shall be formatted IAW figure 6b. The Month field shall contain a 4-bit integer for the current month (1 for January through 12 for December); the Day field shall contain a 5-bit integer for the current day of the month (1 through 31). A mechanism shall be provided to accommodate leap years.

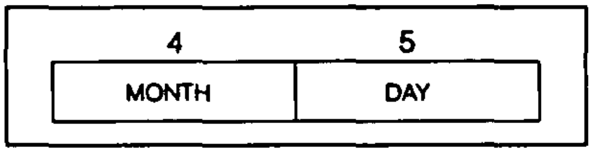


FIGURE 6b. Date format.

d. The PI field shall be formatted IAW figure 6c. The Coarse Time field shall contain an 11-bit integer that counts minutes since midnight. (Temporary discrepancies may occur as discussed in 5.1.2.1.) The 6-bit Fine Time field shall be set to all 1's when using AL-1 LP. When a time synchronization protocol (see 5.2) is employed to obtain more accurate time, the Fine Time field shall be set to the time obtained using this protocol and incremented as described in 5.1.2.

11	6
COARSE TIME	FINE TIME

FIGURE 6c. PI number format.

e. The Fine Time field shall always (except when all 1's) be a multiple of the PI length, and shall be aligned to PI boundaries (e.g., with a 2 second PI, Fine Time shall always be even).

f. The Word field shall be used to count words within a PI, as specified in 5.1.2.

g. The Frequency field shall be formatted IAW figure 6d. Each 4-bit field shall contain one binary-coded decimal digit of the frequency of the current protected transmission.

4	4	4	4	4	4	4
100 MHz	10 MHz	1 MHz	100 KHz	10 KHz	1 KHz	100 Hz

FIGURE 6d. Frequency format.

5.1.2 Procedure.

a. The procedure to be employed in protecting transmissions consisting entirely of 24-bit ALE words is presented in 5.1.2.1 and 5.1.2.2, followed by the procedure for the data block portion of data block mode transmissions.

b. When a radio is neither transmitting nor receiving, the PI number shall be incremented as follows:

(1) When using AL-2 LP, the Fine Time field shall be incremented at the end of each PI by the length of the PI, modulo 60.

(2) When the Fine Time field rolls over to 0, the Coarse Time field shall be incremented, modulo 1440.

(3) At midnight, the Coarse Time and Fine Time fields shall be set to 0, and the Date fields shall be updated.

c. When using AL-1 LP, the Fine Time field shall contain all 1's, and the Coarse Time field shall be incremented at the end of each minute, modulo 1440. At midnight, the Coarse Time field shall be set to 0, and the Date fields shall be updated.

5.1.2.1 Transmitting station.

a. Each word to be transmitted shall be encrypted by the scrambler using the current seed information. In the course of a transmission, the protocol described below may cause a discrepancy between the TOD fields in the seed and the real-time. Such a discrepancy is a normal consequence of the LP procedure, and shall persist until the conclusion of each transmission, whereupon the TOD fields of the seed shall be corrected.

b. The word number field $\mathbf{w}$ shall be used as follows:

(1) During the scan calling phase (T_{sc}) of a call, the calling station shall alternate transmission of words encrypted using $\mathbf{w} = 0$ and $\mathbf{w} = 1$. The first word of T_{sc} shall use the value of $\mathbf{w}$ that results in $\mathbf{w} = 1$ for the last word in T_{sc}. The TOD used during T_{sc} shall change as required to keep pace with real-time, except that TOD shall only change when $\mathbf{w} = 0$; words encrypted with $\mathbf{w} = 1$ shall use the same TOD as the preceding word.

(2) At the beginning of the leading call phase (T_{lc}) of a call (which is the beginning of a single-channel call), the first word shall be encrypted using $\mathbf{w} = 0$ and the correct TOD for the time of transmission of that word.

(3) All succeeding words of the call shall use succeeding word numbers up to and including $\mathbf{w} = \mathbf{w}_{max}$; for the word following a word encrypted with $\mathbf{w} = \mathbf{w}_{max}$, the TOD shall be incremented and $\mathbf{w}$ shall be reset to 0. The $\mathbf{w}_{max} = 2$ for a 1 second PI, $\mathbf{w}_{max} = 5$ for a 2 second PI, and $\mathbf{w}_{max} = 153$ for a 60 second PI.

(4) Responses and all succeeding transmissions shall start with $w = 0$ and the current (corrected) TOD, with these fields incremented as described in step (3) above for each succeeding word.

c. Figure 7a illustrates the permissible TOD¦w combinations for a transmitting station using a 2 second PI ($w_{max} = 5$), and the permissible sequences of these combinations. On the figure, T represents the stored TOD.

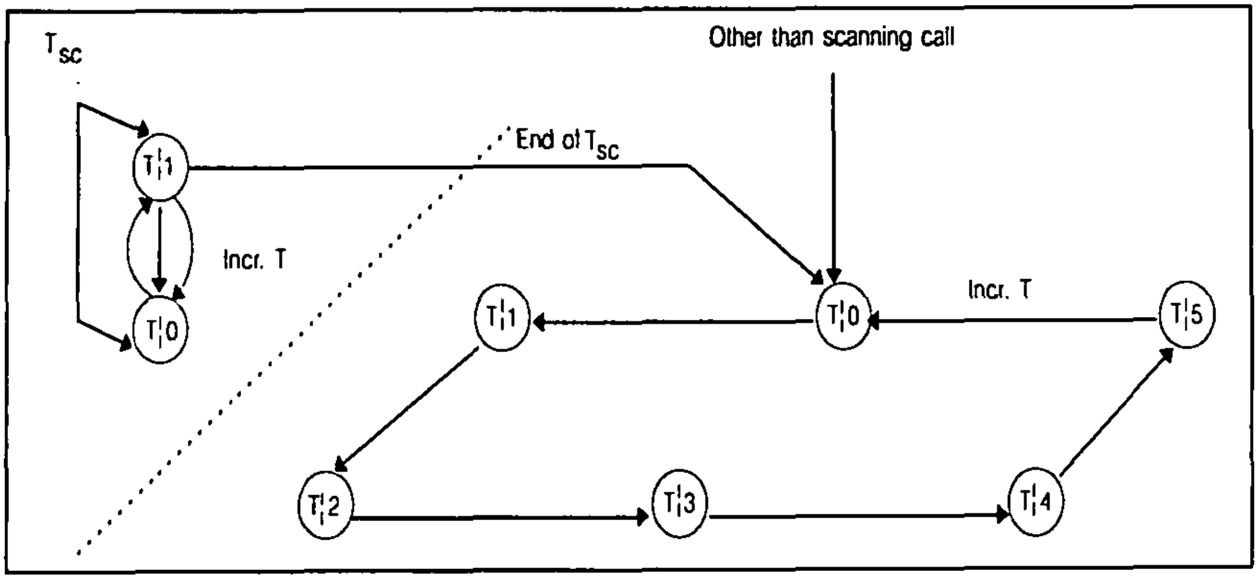


FIGURE 7a. Transmitting station state diagram (2 second PI).

d. Sounds are protected in the same fashion, with T_{rs} (redundant sound phase) in the place of T_{lc}. A single-channel sound is analogous to a single-channel call, and begins the above procedure at step (2) above. A multi-channel sound is analogous to a scanning call, and begins at step (1) above.

5.1.2.2 Receiving station.

a. Because of the possibility of acceptable decodes under multiple TOD/word number combinations, receivers shall attempt to decode received words under all allowed combinations (the current and adjacent PIs [future and past], and both $w = 0$ and $w = 1$) when attempting to achieve word synchronization with a calling station (six combinations). Stations prepared to accept time requests (see 5.2.3.2) shall also attempt to decode received words using coarse TOD (Fine Time = all 1's, correct Coarse time only) with both **w** = 0 and **w** = 1 (eight combinations total). All VALID COMBINATIONS SHALL BE CHECKED while seeking word sync; after achieving word sync, the number of valid combinations is greatly reduced by the LP protocol.

b. Figure 7b illustrates the permissible TOD¦**w** sequences for a receiving station using a 2 second PI after word sync is achieved. Note that, unlike the transmitter, the receiving station state machine may be non-deterministic. For example, when in T_{sc} and in state T¦1, a received word may yield valid preambles and ASCII when decrypted using all of the valid combinations: T¦0, (T+1)¦0, and T¦2 (the latter implying that T_{lc} started two words previously), and will therefore be in three states at once until the ambiguity is resolved by evaluating the decrypted words for compliance with the LP and ALE protocols.

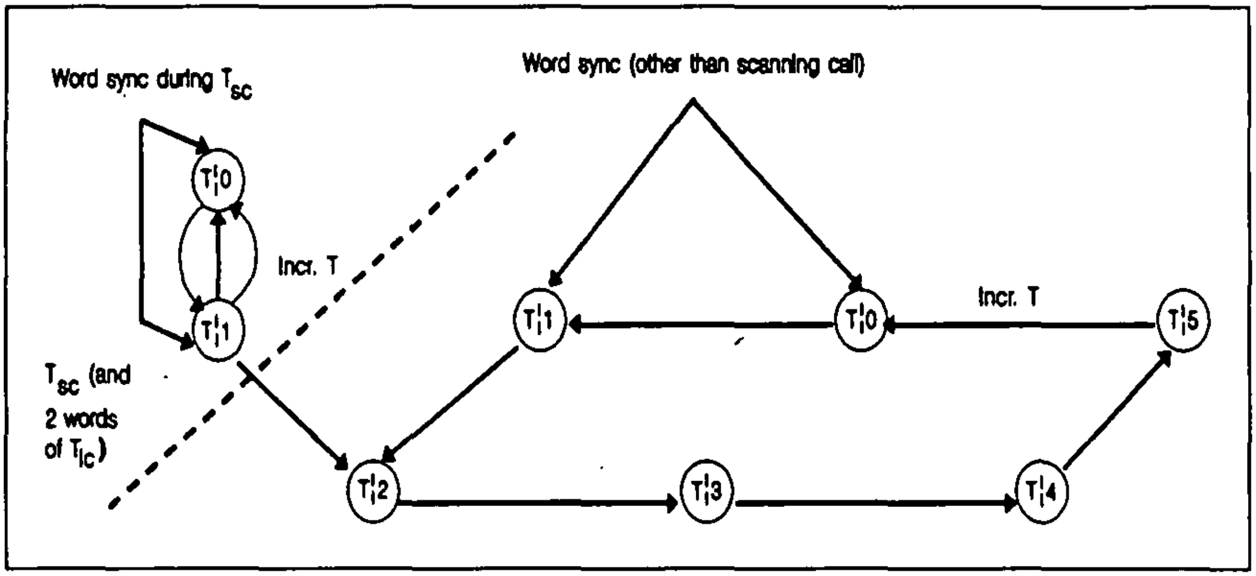


FIGURE 7b. Receiving station state diagram (2 second PI).

c. Stations using a protection interval of two seconds or less shall not accept more than one transmission encrypted using a given TOD, and need not check combinations using that TOD. For example, if a call is decrypted using TOD = X, no TOD before X + 1 is valid for the acknowledgment.

5.1.2.3 <u>Data block message mode</u>.

a. A DBM data block contains an integral number of 12-bit words, the last of which comprises the least significant 12 bits of a cyclic redundancy check (CRC). These 12-bit words shall be encrypted in pairs, with the first 12-bit word presented to the LPCM by the ALE protocol module as the more significant of the two. When a data block contains an odd number of 12-bit words (i.e., basic DBM data block and extended DBM data blocks with odd N), the final 12-bit word shall not be encrypted, but shall be passed directly to the FEC sublayer.

b. The word number field **w** of the seed shall be incremented only after <u>three</u> pairs of 12-bit words have been encrypted (rather than after every 24-bit word as in normal operation), except that the word number **w** shall be incremented exactly once after the last pair of 12-bit words in a DBM data block is encrypted, whether or not it was the third pair to use that word number. As usual, TOD shall be incremented whenever **w** rolls over to 0.

5.2 <u>Time exchange protocols</u>. The following protocols shall be employed to synchronize LP time bases. The time service protocols for active time acquisition, both protected (see 5.2.3) and non-protected (see 5.2.4), are mandatory for all implementations of LP.

5.2.1 <u>Word formats</u>. The mandatory time protocols employ following three types of ALE words: command words, coarse time words, and authentication words in the formats defined below.

5.2.1.1 <u>Command words</u>. Time exchange command words, including the time is command and the time request command used to request and to provide TOD data, shall be formatted as shown on figure 8. The three most significant bits (W_{1-3}) shall contain the standard command (CMD) preamble 110. The next seven bits (W_{4-10}) shall contain the ASCII character '~' (1111110), indicating a time exchange command word. The three time quality bits shall indicate the magnitude of time uncertainty at the sending station IAW 5.2.2. See 5.2.1.1.1 for a description of the Seconds and 40 ms Ticks fields.

3	7	3	6	5
CMD	Time Exchange	Time Quality	Seconds	40 ms Ticks

FIGURE 8. <u>Time exchange command words</u>.

5.2.1.1.1 Time is command.

a. The time is command word carries the fine time current at the sending station as of the start of transmission of the word following the time is command word, and is used in protected time requests and all time service responses. In a time is command word, the Seconds field shall be set to the current number of seconds elapsed in the current minute (0-59), and the Ticks field shall be set (or rounded) to the number of 40 ms intervals that have elapsed in the current second (0-24). The time quality shall reflect the sum of the uncertainty of the local time and the uncertainty of the time of transmission of the time is command IAW table II.

TABLE II. Time quality.

Time Quality Code	Time Uncertainty Window
0	*none**
1	20 ms
2	100 ms
3	500 ms
4	2 s
5	10 s
6	60 s
7	unbounded

*Reserved for use by UTC time standard stations.

b. When a protocol requires transmission of a time is command word, but no time value is available, a NULL time is command word shall be sent containing a time quality of 7, and the Seconds and Ticks fields both set to all 1's.

5.2.1.1.2 Time request command. The time request command word shall be used to request time when no local time value is available, and is used only in non-protected transmissions. In a time request command word, time quality shall be set to 7, the Seconds field to all 1's, and the Ticks field to 30 (11110).

5.2.1.1.3 Other encodings. All encodings of the Seconds and Ticks fields not specified here are reserved, and shall not be used until standardized.

5.2.1.2 Coarse time words. Coarse time words shall be formatted as shown on figure 9, and shall contain the coarse time current as of the transmission of the beginning of that word.

3	1	4	5	11
Data	0	Month	Day	Minute

FIGURE 9. Coarse time words.

5.2.1.3 Authentication words. Authentication words, formatted as shown on figure 10, shall be used to authenticate the times exchanged using the time protocols. The 21-bit authenticator shall be generated by the sender as follows:

a. All 24-bit words in the time command message preceding the authentication word (starting with the time is or time request command word that begins the message) shall be bit by bit "exclusive-ored."

NOTE: "Exclusive-or" is the condition that exists when each resulting bit is a 1 if the two input bits do not match, or the resulting bit is a 0 when the two input bits match.

b. If the message to be authenticated is in response to a preceding time command message, the authenticator from that message shall be exclusive-ored with the result of paragraph a above.

c. The 21 least significant bits of the final result shall be used as the authenticator.

3	21
DATA*	Authenticator

FIGURE 10. Authentication words.

* NOTE: In all cases throughout this standard that specify the use of a particular ALE word preamble (e.g., CMD or DATA), this preamble shall be replaced by a REP preamble (IAW MIL-STD-188-141) when the immediately preceding word in a transmission uses the specified preamble, and that preceding word is logically distinct.

5.2.2 Time quality.

a. Every time exchange command word transmitted shall report the current uncertainty in TOD at the sending station, whether or not time is transmitted in the command word. The codes listed in table II shall be employed for this purpose. The time uncertainty windows in the table are upper bounds on total uncertainty (with respect to coordinated universal time). For example, uncertainty of ±6 seconds is 12 seconds total, and requires a transmitted time quality value of 6.

b. Stations shall power up from a cold start with a time quality of 7. Time uncertainty is initialized when time is entered (see 5.1.1.2.1), and shall be maintained thereafter as follows: the uncertainty increases at a rate set by oscillator stability (e.g., 72 ms per hour with a ±10 parts-per-million [ppm] time base), until the uncertainty is reduced upon the acceptance of time with less uncertainty from an external source, after which the uncertainty resumes increasing at the above rate.

c. A station accepting time from another station shall add its own uncertainty due to processing and propagation delays to determine its own internal time uncertainty. For example, if a station receives time of quality 2, it adds to the received uncertainty of 100 ms (±50 ms) its own processing delay uncertainty of, perhaps, ±100 ms, and a propagation delay bound of ±35 ms, to obtain a new time uncertainty of ±185 ms, or 370 ms total. With a ±10 ppm time source, this uncertainty window would grow by 72 ms per hour, so after two hours the uncertainty becomes 514 ms, and the time quality has dropped to 4. In another 20 hours, the uncertainty grows approaching 2 seconds, and the station (if using a 2 second PI) shall request the correct time before it drops to time quality 5, and is presumed to have lost fine time synchronization.

d. If a low-power clock is used to maintain time while the rest of the unit is powered off, the quality of this clock shall be used to assign time quality upon resumption of normal operation. For example, if the backup clock maintains an accuracy of ±100 ppm under the conditions expected while the station is powered off, the time uncertainty window shall be increased by 17 seconds per day. Such a radio that has been powered off for much over three days may not be presumed to retain even coarse sync, despite its backup clock, and may require manual entry of time.

5.2.3 Active time acquisition (protected). A station that knows the correct date and time to within one minute may attempt to actively acquire time from any station with which it can communicate by employing the protocol described in the following paragraphs. The quality of time so acquired is necessarily at least one grade more uncertain than that of the selected time server. A station that does not know the correct date and time to within one minute may nevertheless employ this protected protocol by repeatedly guessing the time until it successfully communicates with a time server.

5.2.3.1 Time request call.

a. A station requiring fine time shall request the current value of the network time by transmitting a time request call, formatted as follows:

   TO <time server> **CMD** time is <time> **DATA** <coarse time> **REP** <authenticator> **THIS IS** <requester>.

   (In principle, any station may be asked for the time, but some stations may not be programmed to respond, and others may have poor time quality. Multiple servers may need to be tried before sufficient time quality is achieved.)

b. The time is command shall be immediately followed by a coarse time word and an authentication word. The authenticator shall be generated by the exclusive-or of the command word and the coarse time word, as specified in 5.2.1.3.

c. The time request call transmission shall be protected using the procedure specified in 5.1.2. When acquiring time synchronization, the coarse seed (Fine Time field in the seed set to all 1's) current at the requesting station shall be used; when used to reduce the time uncertainty of a station already in time sync, the current fine seed shall be used.

5.2.3.2 Time service response.

a. A station that receives and accepts a time request call shall respond with a time service response formatted as follows:

   TO <requester> **CMD** time is <time> **DATA** <coarse time> **REP** <authenticator> **THIS IS/WAS** <requester>.

b. The time is command shall be immediately followed by a coarse time word and an authentication word. The authenticator shall be generated by the 3-way exclusive-or of the command word and the coarse time word from this transmission and the authentication word (including the **REP** preamble) from the requestor, as specified in 5.2.1.3.

The entire time service response shall be protected as specified above, using the time server's current coarse seed if the request used a coarse seed, or the current fine seed if otherwise. Note that the seed used in protecting a time service response may differ from that used in the request that caused the response.

c. A time server shall only respond to the first time request call using each fine or coarse seed; i.e., one coarse request per minute, and one fine request per fine PI. Acceptance of each class of time requests (coarse and fine) may be disabled by the operator. Stations that are prepared to accept coarse time request commands shall decrypt the initial words of incoming calls under eight (versus six) possible seeds: **w** = 0 and **w** = 1 with the current coarse TOD, and with the current fine TOD ±1 PI. Note that only one coarse TOD is checked versus three fine TODs.

5.2.3.3 Time server request. Normally, the time server concludes the time service protocol by terminating its response with THIS WAS. A time server may instead request authenticated time from the original requester by returning a time server request, which is identical to the time service response as discussed above except, the THIS WAS termination is replaced by THIS IS. The original requester shall then respond with a time service response, as above, with an authenticator generated by the 3-way exclusive-or of the command word and the coarse time word from its time service response and the authentication word (including the **REP** preamble) from the time server request, as specified in 5.2.1.3.

5.2.3.4 Authentication and adjustment.

a. A station awaiting a time service response shall attempt to decrypt received words under the appropriate seeds: if the request used a coarse seed, the waiting station shall try the coarse seeds used to encrypt its request with **w** = 0 and **w** = 1, and those corresponding to one minute later. If the request used a fine seed, the waiting station shall try the usual six seeds:

w = 0 and **w** = 1 with the current fine TOD ±1 PI.

b. Upon successful decryption of a time service response, the requesting station shall exclusive-or the received command and coarse time words with the authentication word it sent in its request. If the 21 least significant bits of the result match the corresponding 21 bits of the received authentication word, the internal time shall be adjusted using the time received in the time is command and coarse time word, and the time uncertainty shall be set IAW 5.2.2c.

5.2.4 Active time acquisition (non-protected). A station that does not know the correct date and time to within one minute may attempt to actively acquire time from any station with which it can communicate in non-protected mode by employing the protocol in the following paragraphs. Because time is not known in this case with sufficient accuracy to employ LP, the entire exchange takes place in the clear with the authentication procedure as the only barrier against deception.

5.2.4.1 Time request call (non-protected).

a. A station requiring time shall request the current value of the network time by transmitting a non-protected time request call, formatted as follows:

TO <time server> **CMD** time request **DATA** <coarse time> **REP** <"random" #> **THIS IS** <requester>.

b. The time request command shall be immediately followed by a coarse time word, followed by an authentication word containing a 21-bit number, generated in such a fashion that future numbers are not predictable from recently used numbers from any net member. Encrypting a function of a radio-unique quantity and a sequence number that is incremented with each use (and which is retained while the radio is powered off) may meet this requirement.

5.2.4.2 Time service response (non-protected).

a. A station that receives and accepts (see paragraph c below) a non-protected time request call shall respond with a non-protected time service response formatted as follows:

TO <requester> **CMD** time is <time> **DATA** <coarse time> **REP** <authenticator> **THIS WAS** <time server>.

b. The time is command shall be immediately followed by a coarse time word and an authentication word. The 21-bit authenticator shall be generated by encrypting the 24-bit result of the 3-way exclusive-or of the command word and the coarse time word from this transmission and the entire random number word (including the **REP** preamble) from the requester, as specified in 5.2.1.3. The encryption shall use the AL-1 algorithm, and a seed containing the time sent with **w** = all 1's. The least significant 21 bits of this encryption shall be used as the authenticator.

c. A time server shall respond to only the first error-free non-protected time request call received each minute (according to its internal time). Acceptance of non-protected time requests may be disabled by the operator.

5.2.4.3 Authentication and adjustment (non-protected). Upon receipt of a non-protected time service response, the requesting station shall exclusive-or the received coarse time word with the received time is command word, exclusive-or the result with the entire random number word it sent in its time request call, and encrypt this result using **w** = all 1's and the coarse time contained in the time service response. If the 21 least significant bits of the result match the corresponding 21 bits of the received authentication word, the internal time shall be adjusted using the received coarse and fine time, and the time uncertainty shall be set IAW 5.2.2c.

5.2.5 Passive time acquisition.

a. As an alternative to the active time acquisition protocols specified above, stations may attempt to determine the correct network time passively by monitoring protected transmissions. Regardless of the technique used to otherwise accept or reject time so acquired, passive time acquisition shall include the following constraints:

(1) Local time may only be adjusted to times within the local window of uncertainty. Received transmissions using times outside of the local uncertainty window shall be ignored.

(2) Local time uncertainty shall be adjusted only after receipt of transmissions from at least two stations, both of which include time quality values, and whose times are consistent with each other within the windows implied by those time qualities.

b. A passive time acquisition mechanism may also be used to maintain network synchronization, once achieved.

c. Passive time acquisition is optional; if provided, the operator shall be able to disable it.

5.2.6 Time broadcast.

a. To maintain network synchronization, stations shall be capable of broadcasting unsolicited time is commands to the network, periodically or upon request by the operator:

TO <NET> **CMD** time is <time> **DATA** <coarse time> **REP** <authenticator> **THIS WAS** <time server>.

b. The time is command shall be immediately followed by a coarse time word and an authentication word. The authenticator shall be generated by the exclusive-or of the command word and the coarse time word from this transmission, as specified in 5.2.1.3. If the broadcast is made without LP (i.e., in the clear), the authenticator shall be encrypted as described in 5.2.4.2.

c. Note that the use of an authenticator that does not depend upon a challenge from a requesting station provides no protection against playback of such broadcasts. A station receiving such broadcasts must verify that the time and the time uncertainty that they contain are consistent with the local time and uncertainty before such received time is at all useful.

5.2.7 Advanced time exchange protocols. Not yet standardized.

5.3 Channel and frequency designators.

a. When two or more stations need to explicitly refer to channels or frequencies other than the one(s) in use for a link, the following encodings shall be used. A frequency is designated using binary-coded-decimal (BCD). The standard frequency designator is a 5 digit string (20 bits), in which the first digit is the 10 MHz digit, followed by 1 MHz, 100 kHz, 10 kHz, and 1 kHz digits. A frequency designator is normally used to indicate an absolute frequency. When a bit in the command associated with a frequency designator indicates that a frequency offset is specified instead, the command will also contain a bit to select either a positive or a negative frequency offset.

b. A channel differs from a frequency in that a channel is a logical entity that implies not only a frequency (or two frequencies for a full-duplex channel), but also various operating mode characteristics, as defined in the section on Channel Memory in MIL-STD-188-141. As in the case of frequency designators, channels may be specified either absolutely or relatively. In either case, a 7-bit binary integer is used which is interpreted as an unsigned integer in the range 0 through 127. Bits in the associated command indicate whether the channel designator represents an absolute channel number, a positive offset, or a negative offset.

5.4 Link quality functions.

5.4.1 LQA matrix. The central data structure for the link quality functions is the LQA matrix (see MIL-STD-188-141, the figure on connectivity and LQA memory). This is an array of link quality records, each containing bidirectional measurements for (at least) BER, SINAD, and multi-path (MP), and each tagged with the ages of the measurements. The matrix is conceptually organized as a two-dimensional array, indexed by channel number and by directly-reachable station (i.e., matrix contains an entry for the potential quality of a link to each station that can be called directly, on every channel defined for reaching that station).

5.4.2 Sounding. Sounding is the periodic broadcast of a station's address, so that other stations can evaluate the quality of the frequency carrying the sound for future link establishment to the sounding station.

5.4.2.1 Sounding intervals. The required rate of sounding is determined by how busy the intended recipients are, and the maximum acceptable probability that the most recent sounds received from some stations are older than some maximum acceptable age. For example, if B is the probability that a receiver is busy when a sound is sent, A is the maximum acceptable age (in hours), and P is the maximum acceptable probability that an entry is older than that age, then R sounds will be sent per hour, where:

$$R=\frac{\log P}{A\log B}.$$

A and P are chosen by the network manager to satisfy network performance goals. B is measured from actual network operation. Specifically, B is the fraction of time during a measurement period that the observed radio is not able to receive sounds; this usually means the fraction of time that the radio is not scanning. Note that B includes busy time due to both traffic and overhead (such as sounding and polling). For example, if polling is not used to fill in gaps in sounding data, the system may be willing to accept only a 10% probability that each entry in the LQA matrix is over one hour old. Then R is a function of B as illustrated in table III.

TABLE III. Example sounding interval calculation.

B (Prob. Station Busy)	R (Minimum Sounds/Hr/Chan)	Maximum Sounding Interval
1%	0.5	2 hr.
10%	1	1 hr.
32%	2	30 min.
46%	3	20 min.
56%	4	15 min.
68%	6	10 min.

5.4.2.2 Local noise report.

a. The call acceptance and call rejection sounding protocols defined in MIL-STD-188-141 result in only unilateral link quality assessment at the receiving station. The local noise report is an alternative broadcast technique that permits receiving stations to approximately predict the bilateral link quality for the channel used by the station sending the local noise report. An example application of this optional technique is for networks in which most stations are silent but which need to have a high probability of linking on their first attempt with a sounding station.

b. A station receiving a sound can measure unilateral link quality for the channel to it from the sounding station. If a local noise report is included in a transmission, the recipient can compare the noise level at the transmitter to its own local noise level, and estimate the bilateral link quality. The local noise report is contained in a single command (CMD) word as shown on figure 11, and reports the mean and maximum noise power measured on the channel (by the sending station) during the last 60 minutes.

3	7	7	7
CMD	Noise Report (ASCII 'n')	Max	Mean
110	1101110		

FIGURE 11. Local noise report.

c. Units for the Max and Mean fields are dB relative to 0.1 microvolt in a 3 kHz channel. If the local noise measurement to be reported is 0 dB or less, a 0 is sent. For measured noise ratios of 0 dB to +126 dB, the ratio in dB is rounded to an integer and sent. For noise ratios greater than +126 dB, 126 is sent. The code 127 (all 1's) is sent when no report is available for a field.

d. By comparing the noise levels reported by a distant station on several channels, the station receiving the noise reports can select a channel for linking attempts based upon knowledge of both the propagation characteristics and the interference situation at the distant station.

5.4.3 Polling protocols. The polling protocols are used to measure and exchange current bilateral link quality data.

5.4.3.1 Individual poll: two stations, one channel. A two-station poll may be performed using a 3-way handshake with an LQA request in the call, an LQA report with a request in the response, and an LQA report in the acknowledgment (which may also terminate the link).

5.4.3.2 Multiple station - single channel polling. Slotted response structures (net and group calls) in star topologies yield bilateral results at the hub (which receives hub-to-spoke reports in the slotted responses, and measures spoke-to-hub LQA during those responses), but only unilateral (hub-to-spoke) LQA measurements at the out stations. For the hub to report the LQA values measured on the responses, the existing protocols require individual handshakes with each out station. With slight extensions to the existing protocols, however, efficient bilateral LQA measurements for all stations' links to the hub can be obtained. (Some unilateral spoke-to-spoke measurements may also be made by stations able to do so.)

5.4.3.2.1 Hub net poll.

a. The hub net poll protocol evaluates bilateral connectivity between the originator of the call and each of the responding net members. At the completion of the protocol, only the calling station (the "hub") knows all of the bilateral measurements; each responding net member may know only the hub-to-spoke link quality that it measured from the call and the acknowledgment (see figure 12).

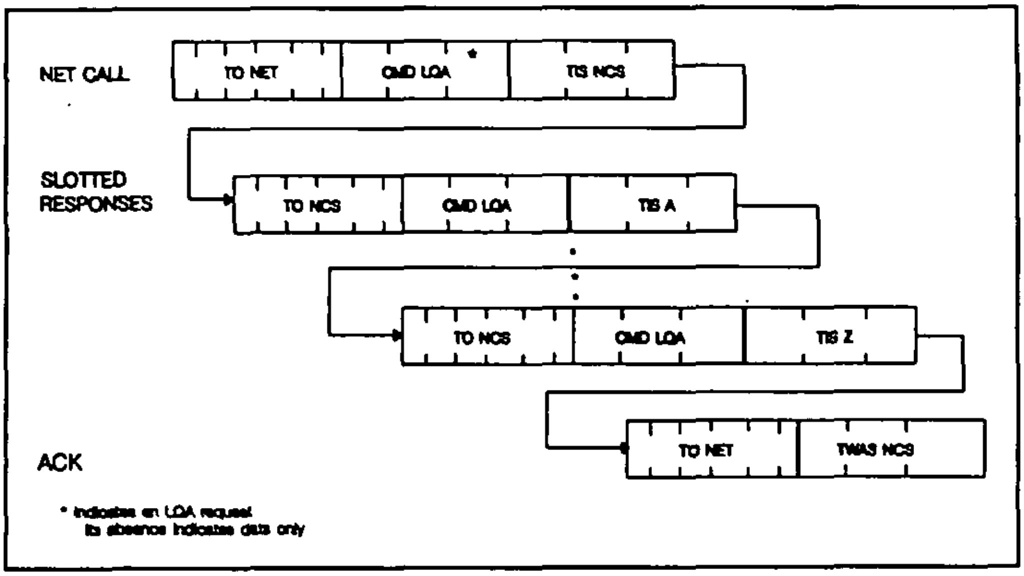


FIGURE 12. Hub net poll (T_{SC} not shown).

b. Although the hub is called "NCS" in the example, this call may be originated by any station. The hub calls the net, with an LQA request embedded in the call. Each net member that hears the call responds in its assigned slot, reporting the LQA data that it acquired from the call. The hub completes the three-way handshake with an acknowledgment that contains no LQA report, and returns the net to scan with a THIS WAS termination.

c. If any responding station requests LQA from the hub in its response, the hub shall insert an LQA report in its acknowledgment, but the LQA report shall contain all fields set to all 1's ("no report") to avoid confusing other stations.

5.4.3.2.2 Full net poll.

a. The full net poll protocol evaluates and reports bilateral connectivity between the originator of the call and each of the responding net members (see figure 13). The hub calls the net, with an LQA request embedded in the call. Each net member that hears the call responds in its assigned slot, reporting the LQA data that it acquired from the call and requesting that the hub return an analysis of the station's response in the acknowledgment. The hub completes the three-way handshake with an acknowledgment that returns LQA data to the net members in slot order and returns the net to scan with a THIS WAS termination. For compatibility with stations not equipped to receive this data, the message section in the acknowledgment shall start with a "no report" LQA CMD, followed by LQA reports embedded in DATA words. The first DATA word shall contain the LQA report for the station in slot 1, and so on. Note that positions in the acknowledgment corresponding to nonresponding net members (including the hub) shall be filled with "no report" words.

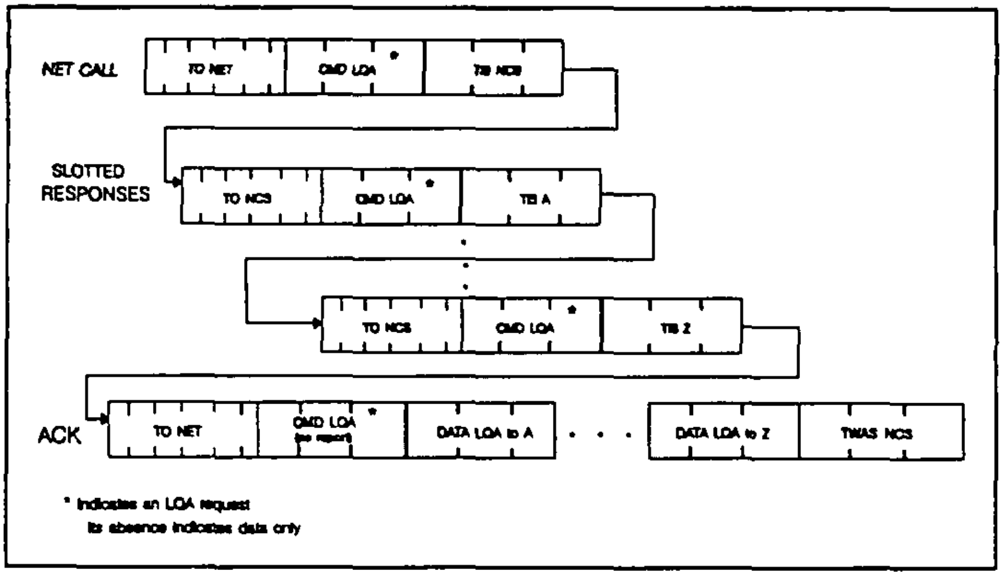


FIGURE 13. Full net poll (T_{SC} not shown).

b. The time required to execute this protocol on one channel (including the scanning call time for [T_{SC}]) is about 40 seconds for a 10 station net with a 10 channel T_{SC}, or 275 seconds for 100 stations.

5.4.3.2.3 Hub group poll. The hub group poll is structurally similar to the hub net poll, except that the net call is replaced by a group call. The acknowledgment may address all of the stations addressed in the call; alternatively, those stations not heard by the hub to respond may be omitted in the acknowledgment.

5.4.3.2.4 Full group poll. The full group poll is structurally similar to the Full Net Poll, except that the net call is replaced by a group call. The acknowledgment may address all of the stations addressed in the call; alternatively, those stations not heard by the hub to respond may be omitted in the acknowledgment. The order of LQA reports in the acknowledgment (following the "no report" LQA CMD) is determined by the order of addresses in the acknowledgment. Non-responding stations may be omitted from both the leading call and message section of the acknowledgment.

5.4.3.3 Two station - multiple channel polling.

a. A technique commonly called "poll before linking" evaluates several channels immediately before linking to select the current best channel. This may be performed using an individual poll on each channel, but a significant amount of time is wasted in unnecessary scanning calls. For example, evaluating 10 channels takes about 150 seconds, with over half of this time consumed by calling cycles of scanning calls. All but the first scanning call may be eliminated if the stations involved agree upon a list of channels to be evaluated, and then step through this list synchronously.

b. When stations with identical scan sets want to evaluate all channels in their common scan set, the following protocol is used:

(1) The caller embeds **CMD** <LQA request> **CMD** <channel scan request> in the call. (A channel scan request carries as a parameter the sender's tune time, as shown on figure 14).

(2) The responder shall respond to the LQA request (requirement of MIL-STD-188-141). If the response contains **CMD** <channel scan request>, the requested channel scan has been accepted, and both stations are obligated to complete it. Otherwise, an individual poll is completed on the current channel, and the protocol terminates.

(3) When the response contains a channel scan request (along with an LQA report with the request bit set), an individual poll is completed on the initial channel. The acknowledgment from the caller will contain an LQA report with the request bit negated.

(4) Both stations proceed to the next channel, listen for activity, and tune. After the longer of the two tune times in the channel scan request has elapsed, the caller initiates a non-scanning individual poll: a leading call, an LQA request, and the caller's frame termination. The response will contain an LQA report with the request bit set, and the acknowledgment from the caller will contain an LQA report with the request bit negated.

3	7	2	3	2	7
CMD	Channels (ASCII 'c')	Type	Tune	Mode	Control
110	1100011	00			

FIGURE 14. Channel scan request CMD format.

c. The synchronous polling shall proceed through the channels from the initial channel to the next lower frequency, and so on, wrapping around from the lowest frequency to the highest, and continuing through all of the channels. Busy channels are not evaluated. Since both stations tune before the call, no tune time is needed between the call and the response. This permits additional speed-up in evaluating the channels. The stations always proceed to the next channel synchronously, whether or not they successfully measure the current channel (e.g., busy or non-propagating channels). The time step per channel is the longer tune time plus 18 T_{rw} (redundant word time) (assuming three-character addresses).

d. The Type field of the channel scan request CMD word is set to 00 to distinguish it from other types of channel commands.

e. The Tune Time field is encoded as listed in table IV. It indicates the time that must be allowed for tuning before each non-scanning call.

TABLE IV. Tune time encoding.

Tune Field	Tune Time
000	100 ms
001	200 ms
010	500 ms
011	1 s
100	2 s
101	5 s
110	10 s
111	30 s

f. The Mode field of the channel scan request CMD word is encoded as listed in table V. The purpose of this field is to indicate whether data words follow the channel scan request CMD word, and whether they contain channel designators or frequency designators.

TABLE V. Mode field encoding.

Mode Field	Meaning
00	Use current scan list channels
01	Channel list follows
10	Frequency list follows
11	List accepted without modifications

g. In mode 01 or mode 10, the Control field is set to 1000000 when the channel or frequency designators (respectively) are positive offsets relative to the initial channel, or to 1100000 for negative offsets. In all other cases, the Control field is set to 0000000.

h. When the set of channels to be evaluated must be negotiated before the channel scan, channel designators are sent following the Channel Scan Request CMD word in DATA words. Up to three channel designators are sent in each DATA word. The order of channels scanned is determined by the order the channels are listed.

(1) The first channel scanned after the initial channel is designated in the most significant character position of the first DATA word.

(2) The scan proceeds in order through the remaining channels designated in the first data word followed by channels designated in subsequent data words.

(3) Unused character positions in the final DATA word shall be filled with 0's.

i. When the caller provides an explicit list of channels following its channel scan request, the responder may either accept this list without modifications by returning a channel scan request with a mode of 11, or it may add channels to the list by returning a channel scan request with a mode of 01 followed by the list of channels to be added.

j. When the correspondence of channel numbers to frequencies may be different for the stations wishing to poll before linking, the set of frequencies to be evaluated shall be negotiated before the channel scan. In this case, frequency designators are sent following the channel scan request CMD word in DATA words. One frequency designator is sent in each DATA word in positions W_5 through W_{24}. W_4 is set to 0. The order of frequencies scanned is determined by the order the frequencies are listed.

(1) The first frequency scanned after the initial channel is designated in the first DATA word.

(2) The scan proceeds in order through the frequencies designated in subsequent data words.

k. When the caller provides an explicit list of frequencies following its channel scan request, the responder may either accept this list without modifications by returning a channel scan request with a mode of 11, or it may add frequencies to the list by returning a channel scan request with a Mode 10 followed by the list of frequencies to be added.

5.4.4 LQA report protocol.

a. The unilateral LQA data derived from measurements on traffic and sounds received on several channels can be exchanged among the stations sending and measuring those transmissions to provide each with bilateral LQA data for those channels. Thus, the LQA report protocol "closes the loop" with passive LQA. The LQA report protocol is used by station A to report to station B the LQA data collected by A from transmissions from B to A.

b. LQA reports are embedded in ALE frames as follows: The first word in an LQA report message is an LQA report CMD word, formatted as shown on figure 15. This is followed by LQA reports for the number of channels specified in the chan field in the LQA Report CMD. These are carried either in a Data Text Message (DTM), or in a Data Block Message (DBM), as specified by control bit KR5 (see table VI). In either case, the message carrying the reports shall immediately follow the LQA Report command word.

3	7	2	5	2	5
CMD	LQA Report (ASCII 'r')	Type	Control	*	Chan
110	1110010	00		00	
* Reserved block (set to 00)					

FIGURE 15. LQA report CMD format.

TABLE VI. Control bit assignments (LQA report CMD word).

Control Bit	Meaning
KR5 (most significant bit)	0 if reports in DTM message 1 if reports in DBM message
KR4, 3, 2	000 data only (no channel or frequency designators) 001 data and channel designator (negative offset) 010 data and channel designator (absolute) 011 data and channel designator (positive offset) 100 data and frequency designator (negative offset) 101 data and frequency designator (absolute) 110 data and frequency designator (positive offset) 111 (reserved)
KR1 (least significant bit)	(reserved)

c. The individual reports have one of three formats, as specified by control bits KR4, KR3, and KR2; data only (16 bits per report), channel and data (23 bits), or frequency and data (36 bits) (see figure 16). In all cases, the data portion of the report has the same format: age of the data (3 bits), multipath (3 bits), SINAD (5 bits), and BER (5 bits), with encodings as specified in paragraph e below. When a channel or frequency designator is included in each report, it immediately precedes its corresponding data field, and is formatted as described in 5.3.

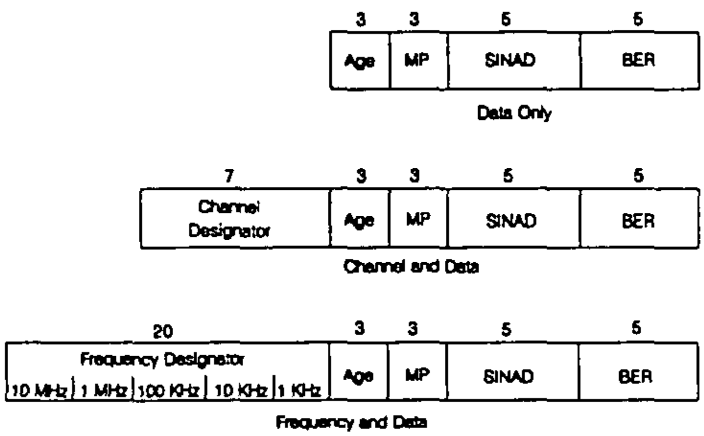


FIGURE 16. LQA report formats.

d. When a DTM is used to carry LQA reports, the reports are packed bit-by-bit into the 21-bit data fields without aligning each report with the start of a new word. When the reports do not fill the final ALE word, the remaining bits after the last report are filled with 0's. The DBM data block is likewise filled with packed reports, with the Length field set to indicate the length of reports.

e. The BER field in LQA reports is encoded as in LQA CMD words (MIL-STD-188-141, Basic Bit Error Ratio Values). SINAD is encoded as an integer in dB: 0-30, with the code 31 (11111) reserved to indicate no SINAD report. Multipath is similarly encoded as an integer in ms: 0-6, with the code 7 (111) reserved to indicate no multipath report. The age of each report is encoded as shown in table VII.

TABLE VII. Age field encoding.

Age Field	Age of Reported Data
000	0-15 min
001	15-30 min
010	30-60 min
011	1-2 hr
100	2-4 hr
101	4-23 hr
110	23-25 hr
111	>25 or unknown

f. LQA reports may be sent either upon request or by pre-arranged schedule. A station may request an LQA report by sending an LQA report request, which shall be formatted as shown on figure 17. The bits of the control field are used to request the format of LQA reports, and shall be assigned in accordance with table VI. The Age field specifies the maximum age acceptable for the reports, shall be encoded in accordance with table VII. If the Age field is set to 110, all channels with LQA measurements shall be reported; if the Age field is set to 111, all channels common to the two stations shall be reported, including those for which no data is available.

3	7	2	5	4	3
CMD	LQA Report (ASCII 'r')	Type	Control	*	Age
110	1110010	10		0000	
* Reserved block (set to 0000)					

FIGURE 17. LQA report request CMD format.

5.5 Advanced link quality analysis. Stations supporting ALQA shall maintain an ALQA matrix analogous to the LQA matrix (see the section on Connectivity and LQA Memory in MIL-STD-188-141) that stores histograms as described in 4.5.3 for the stations listed in the section on Other Address Memory in MIL-STD-188-141. For each station, the ALQA matrix shall contain one set of histograms for each implemented channel quality measure for each channel scanned, and one set of histograms for each implemented link performance measure.

5.5.1 Channel quality measures. Channel quality measurements for ALQA shall be in accordance with the applicable paragraph below.

5.5.1.1 SINAD and PBER. SINAD and PBER shall be measured as described in MIL-STD-188-141 for each ALE word received beginning when word synchronization is achieved. For ALQA use, the word-by-word samples shall not be averaged (as in MIL-STD-188-141), but shall be histogrammed as described in 4.5.3.

5.5.1.2 Articulation index.

a. Articulation index shall be computed using a weighted sum of the signal-to-noise ratios within the frequency bands centered on the 8 ALE modem tones in accordance with table VIII. (The weights F_i shown in table VIII reflect the varying sensitivity of human hearing to different frequencies.) The effective sensation levels E_i in each sub-band ($1 \leq i \leq 8$) shall be accumulated during each ALE triple-redundant word reception (49 symbol periods). For each sub-band i, S_i is the mean spectral density of the ALE modem input signal in the i-th frequency band (in dBm/Hz) averaged over those symbol periods for which the demodulator chose symbol i, while N_{Oi} is the mean spectral density in the i-th frequency band (in dBm/Hz) averaged over those symbol periods for which symbol i was not chosen (an estimate of the noise and interference in sub-band i). The E_i (in dB) shall be determined from these measurements using the formula $E_i = S_i - N_{Oi}$.

TABLE VIII. ALE tone weighting factors.

Tone(i)	Nominal Freq.	Freq. Sub-Band	Weight (F_i)
1	750	625 - 875	0.161
2	1000	875 - 1125	0.147
3	1250	1125 - 1375	0.142
4	1500	1375 - 1625	0.131
5	1750	1625 - 1875	0.131
6	2000	1875 - 2125	0.113
7	2250	2125 - 2375	0.095
8	2500	2375 - 2625	0.080

b. Scaled measurements W_i (ranging from 0 to 1) shall be determined from the effective sensation level E_i of each speech sub-band as follows:

(1) For $E_i < 1$ dB, $W_i = 0$.

(2) For 1 dB $\leq E_i \leq$ 12 dB, get W_i from table IX.

(3) For 12 dB $< E_i \leq$ 36 dB, $W_i = (E_i - 6)/30$.

(4) For $E_i > 36$ dB, $W_i = 1$.

The articulation index sample for each received ALE word shall be computed from measurements W_i within each frequency band as follows. The weighting factors F_i shall be taken from the last column of table VIII above:

$$AI = \sum_{i=1}^{8} F_i W_i .$$

Articulation index samples shall be histogrammed as specified in 4.5.3.

NOTE: The articulation index measurements are performed only over the 625 - 2625 Hz frequency range, but the articulation index value obtained is extrapolated to the entire voice range so that the range of articulation index values is 0 to 100%.

TABLE IX. E_i to W_i conversion ($1 \text{ dB} < E_i \leq 12$ dB).

E_i (dB)	W_i	E_i (dB)	W_i
1.0 - 2.2	0.01	8.4 - 8.7	0.11
2.3 - 3.1	0.02	8.8 - 9.1	0.12
3.2 - 3.9	0.03	9.2 - 9.5	0.13
4.0 - 4.6	0.04	9.6 - 9.9	0.14
4.7 - 5.3	0.05	10.0 - 10.3	0.15
5.4 - 6.0	0.06	10.4 - 10.7	0.16
6.1 - 6.6	0.07	10.8 - 11.1	0.17
6.7 - 7.2	0.08	11.2 - 11.5	0.18
7.3 - 7.8	0.09	11.6 - 11.8	0.19
7.9 - 8.3	0.10	11.9 - 12.0	0.20

5.5.1.3 Spectral distortion.

a. Spectral distortion shall be measured by comparing pairs of SINAD and PBER measurements of received ALE words to the theoretical modem performance curve (the dashed line labeled 'G' on figure 18). Each (SINAD, PBER) measurement pair falls within one of the regions on figure 18; the number of that region is the spectral distortion measurement for that received ALE word.

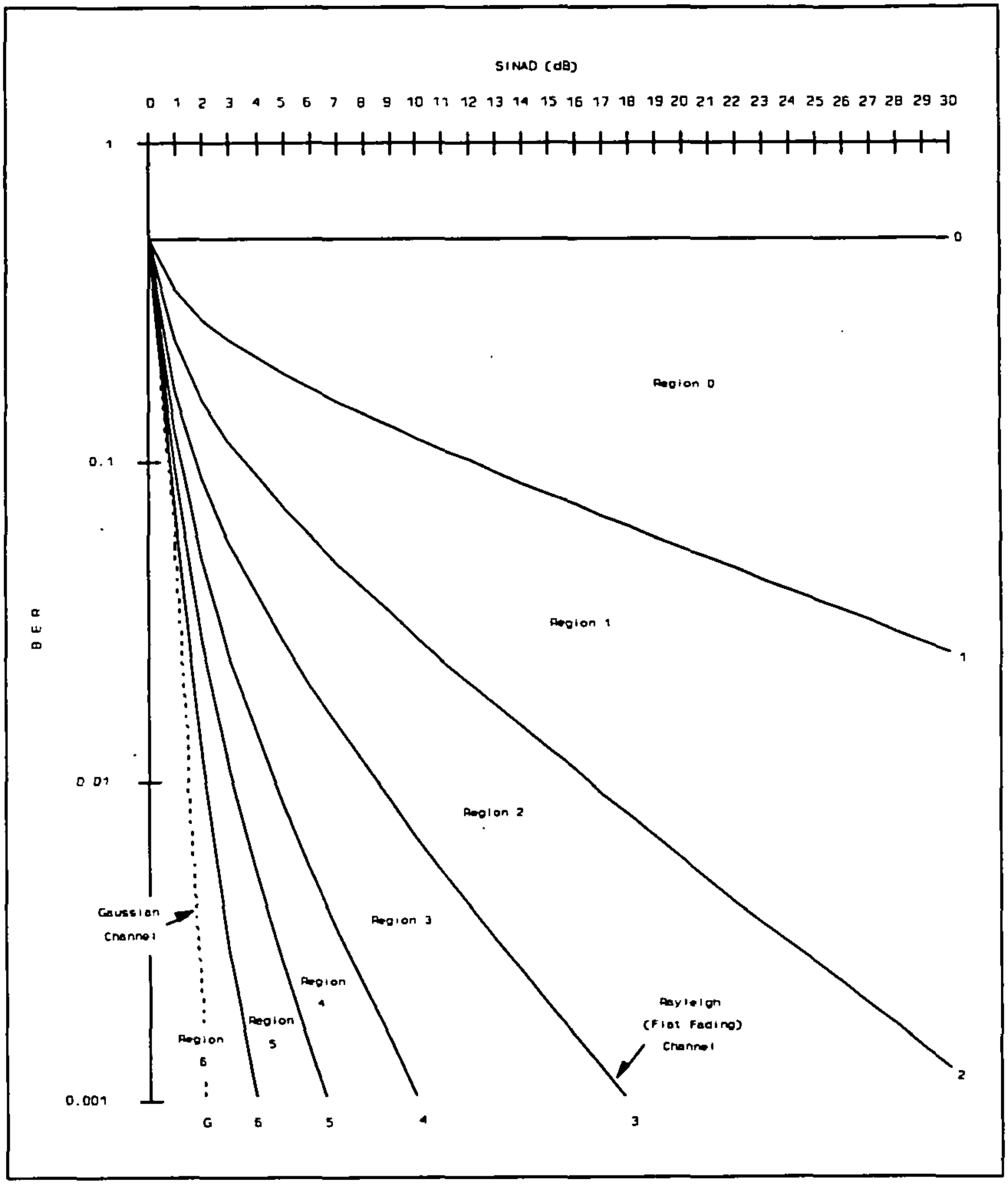


FIGURE 18. Spectral distortion partition of BER versus SINAD sample space.

Spectral distortion measurements shall be histogrammed in accordance with 4.5.3.

b. Points along the lines that separate the regions shown on figure 18 are tabulated in table X; each column in the table is labeled with the corresponding curve number from the figure.

c. The following simple algorithm, using the data from table XI, may be used to quickly compute spectral distortion.

(1) Measure SINAD and PBER for each word received.

(2) Convert the measurements of each word to LQA codes (range 0-30) in accordance with MIL-STD-188-141.

(3) Use the SINAD code to select a row in table XI.

(4) Find the column in that row that includes the PBER code; the spectral distortion region number at the head of that column is the spectral distortion value for that word. The spectral distortion value is 7 ("no measurement") if either SINAD or PBER is unknown (code 31), or if the SINAD code is 0 ("no signal").

5.5.1.4 Error-free interval. The word error statistics described in table XII shall be obtained from the receiving Golay decoder and ALE protocol (errors which cannot be corrected in either or both Golay words or the entire ALE word count as one word error). Each of the counts shall be accumulated separately for each of the four epochs.

TABLE X. Maximum BER for each spectral distortion region (boundary coordinates).

SINAD (dB)	0	1	2	3	4	5	6	Gaussian
1	0.5000	0.34697	0.24077	0.16708	0.12560	0.09442	0.06957	0.05432
2	0.5000	0.28121	0.15816	0.08895	0.04965	0.02771	0.01187	0.00154
3	0.5000	0.24090	0.11607	0.05592	0.02480	0.01100	0.00300	0.00001
4	0.5000	0.21198	0.08987	0.03810	0.01394	0.00510	0.00095	
5	0.5000	0.18943	0.07177	0.02719	0.00841	0.00260	0.00034	
6	0.5000	0.17094	0.05844	0.01998	0.00529	0.00140	0.00014	
7	0.5000	0.15529	0.04823	0.01498	0.00344	0.00079	0.00006	
8	0.5000	0.14178	0.04020	0.01140	0.00226	0.00045	0.00003	
9	0.5000	0.12986	0.03373	0.00876	0.00154	0.00027	0.00001	
10	0.5000	0.11923	0.02843	0.00678	0.00104	0.00016	0.00001	
11	0.5000	0.10970	0.02407	0.00528	0.00073	0.00010		
12	0.5000	0.10107	0.02043	0.00413	0.00050	0.00006		
13	0.5000	0.09322	0.01738	0.00324	0.00036	0.00004		
14	0.5000	0.08607	0.01481	0.00255	0.00023	0.00002		
15	0.5000	0.07950	0.01264	0.00201	0.00018	0.00002		
16	0.5000	0.07353	0.01081	0.00159	0.00013	0.00001		
17	0.5000	0.06786	0.00921	0.00125	0.00009	0.00001		
18	0.5000	0.06279	0.00788	0.00099	0.00007			
19	0.5000	0.05824	0.00678	0.00079	0.00005			
20	0.5000	0.05372	0.00577	0.00062				
21	0.5000	0.04966	0.00493	0.00049				
22	0.5000	0.04603	0.00424	0.00039				
23	0.5000	0.04264	0.00364	0.00031				
24	0.5000	0.03969	0.00315	0.00025				
25	0.5000	0.03684	0.00271	0.00020				
26	0.5000	0.03420	0.00234	0.00016				
27	0.5000	0.03175	0.00202	0.00013				
28	0.5000	0.02934	0.00172	0.00010				
29	0.5000	0.02714	0.00147	0.00008				
30	0.5000	0.02520	0.00127	0.00006				

TABLE XI. PBER code ranges for each spectral distortion region.

SINAD code	Spectral Distortion Region 0	1	2	3	4	5	6
1		27 - 30	21 - 26	16 - 20	13 - 15	10 - 12	0 - 9
2	30	20 - 29	12 - 19	7 - 11	4 - 6	2 - 3	0 - 1
3	27 - 30	15 - 26	8 - 14	4 - 7	2 - 3	1	0
4	25 - 30	12 - 24	6 - 11	2 - 5	1		0
5	23 - 30	10 - 22	4 - 9	2 - 3	1		0
6	21 - 30	8 - 20	3 - 7	1 - 2			0
7	19 - 30	7 - 18	3 - 6	1 - 2			0
8	18 - 30	6 - 17	2 - 5	1			0
9	17 - 30	5 - 16	2 - 4	1			0
10	16 - 30	4 - 15	1 - 3				0
11	15 - 30	4 - 14	1 - 3				0
12	14 - 30	3 - 13	1 - 2				0
13	13 - 30	3 - 12	1 - 2				0
14	12 - 30	3 - 11	1 - 2				0
15	11 - 30	2 - 10	1				0
16	10 - 30	2 - 9	1				0
17	10 - 30	2 - 9	1				0
18	9 - 30	2 - 8	1				0
19	8 - 30	1 - 7					0
20	8 - 30	1 - 7					0
21	7 - 30	1 - 6					0
22	7 - 30	1 - 6					0
23	6 - 30	1 - 5					0
24	6 - 30	1 - 5					0
25	6 - 30	1 - 5					0
26	5 - 30	1 - 4					0
27	5 - 30	1 - 4					0
28	5 - 30	1 - 4					0
29	5 - 30	1 - 4					0
30	4 - 30	1 - 3					0

TABLE XII. Word error statistics.

Statistic	Description
Total words	A running count of the number of ALE words received on the channel during the epoch, including words during which word synchronization was achieved.
Total errors	A running count of the number of word errors that have occurred in the epoch on the channel.
Burst errors	A running count of the number of error words that immediately followed another error word.

The estimated error-free interval on a channel for any epoch shall be computed as follows:

$$P_e = \frac{Total\ errors}{Total\ words} \qquad P_b = \frac{Burst\ errors}{Total\ errors}$$

$$EFI = \frac{(1/P_e)-1}{1-P_b}.$$

5.5.2 Link performance measures. The link performance measures, achievable voice quality and available data capacity, shall represent the combined performance available using any of the channels available to the ALE controller. Achievable voice quality and available data capacity samples for each station listed in the ALQA matrix shall be histogrammed as described in 4.5.3.

5.5.2.1 Achievable voice quality.

a. Achievable voice quality shall be measured while the ALE controller is scanning. During each ALQA scan of the available channels (see paragraph 5.5.2.1b), the ALE controller shall note which channels are unoccupied. When occupancy of each channel has been evaluated, the most recent voice channel quality measure samples (see paragraph 5.5.2.1c) to each station via the unoccupied channels shall be compared; for each station, the channel quality measure sample having the largest value shall be histogrammed as the achievable voice quality sample for that station, for that ALQA scan.

b. If channel occupancy can be accurately determined at the normal ALE scanning rate, the ALQA scan shall coincide with the ALE scan (i.e., an ALQA scan shall be performed during each ALE scan). However, if the equipment available to the ALE controller for measuring channel occupancy requires a longer dwell time on each channel than does normal ALE scanning, the number of channels evaluated on each ALE scan shall be limited so that the ALE scan is not extended beyond a total of 2 C T_{rw}, where C is the number of channels scanned. Because multiple ALE scans are then required to evaluate all channels, this results in an ALQA scan period that is several times longer than the ALE scan period.

c. The voice channel quality measure used for achievable voice quality shall be articulation index if available. Otherwise, SINAD shall be used.

5.5.2.2 Available data capacity. An available data capacity sample shall be computed and histogrammed each time the ALE controller successfully sends a message to another station. (DO: also compute available data capacity samples when messages are sent by other data link controllers.) See table XIII for the applicable symbology. Available data capacity samples require the measurements for the symbols listed in table XIII for each message sent.

TABLE XIII. Available data capacity symbols.

Symbol	Meaning
T_b	Time when the first transmission related to sending the message began (e.g., the call to establish a link for sending the message).
T_f	Time when the (final) data link ACK arrived, indicating that the message had been completely received by the receiving station, and could be discarded at sending station.
L_m	Number of bits in the message body, exclusive of data link layer overhead bits.
L_s	Sum of the L_m's for all *other* messages (to any destination) waiting to be sent after the current message, as of time T_b.
L_f	Sum of the L_m's for all *other* messages (to any destination) waiting to be sent as of time T_f, including messages not in the queue at time T_b.

The effective data rate R for the message shall be computed as follows:

$$R = \frac{L_m}{T_f - T_b}.$$

Station utilization U shall be computed as follows:

$$U = \frac{L_f - L_s}{L_m}.$$

The available data capacity sample X shall be computed as:

$$X = R(1 - U).$$

For example, consider a 300-character message to be sent as a data text message. L_m in this case is 2100 bits. Assume that two other messages were waiting when link establishment to send this message began, and that they contained a total of 480 characters, so L_s = 3360 bits. Link establishment succeeds on the first channel tried, and the message is sent in the ALE acknowledgement. However, a fade during the message transmission causes an ARQ NAK, a (successful) retransmission, and an ACK. This requires a total of 100 seconds = $T_f - T_b$. During this process, another message has joined the waiting queue; it contains 120 characters, so L_f = 7 (480 + 120) = 4200. For this example,

$$R = \frac{2100}{100} = 21\ bps$$

$$U = \frac{4200 - 3360}{2100} = 0.40$$

$$X = 21(1 - 0.40) = 12.6\ bps.$$

5.5.3 ALQA reporting protocol. The following ALQA orderwire protocol shall be used to request and to report channel quality measure and link performance measure measurement data. ALQA reports shall convey historical data (including measurements of the ALQA request itself) for all channels common to the parties to the exchange. (This protocol is similar to the LQA report protocol described in 5.4.4.)

5.5.3.1 ALQA command word. The ALQA command word (shown on figures 19 through 21 and 23) shall be used both to request and to report ALQA measurements. All instances of the ALQA CMD contain Epoch and Control fields. In requests, the Epoch field shall specify the desired timeliness of data, while in a report, the Epoch field shall indicate the epoch actually used (see table XIV). (Note that the Epoch field in a report need not have the same value as in the request.)

TABLE XIV. Epoch field encoding.

Epoch Field	Request	Report
00	Data accumulated since startup (epoch 4)	Data from epoch 4
01	Data from current 15 minute interval (epoch 1)	Data from epoch 1
10	Data from most recent epoch with more than zero samples	Data from epoch 2
11	Data from epoch with greatest density of samples (number of samples divided by $N_k t_k$)	Data from epoch 3

The Control field shall describe the format of the reports requested or delivered in accordance with table XV. The reporting station should always comply with the reporting format requested unless it is not equipped to do so. All implementations of ALQA reporting shall support the minimum interoperability format which corresponds to all control bits set to 0 (i.e., reports in DTM messages, containing data only, and using default thresholds, as described below).

TABLE XV. Control bit assignments.

Control bit	Meaning
KL5 (most significant bit)	0 if reports in DTM message 1 if reports in DBM message
KL4, 3, 2	000 data only (no channel or frequency designators) 001 data and channel designator (negative offset) 010 data and channel designator (absolute) 011 data and channel designator (positive offset) 100 data and frequency designator (negative offset) 101 data and frequency designator (absolute) 110 data and frequency designator (positive offset) 111 (reserved)
KL1 (least significant bit)	0 If default thresholds 1 If thresholds follow this CMD

5.5.3.2 Channel quality measure request. Channel quality measure requests shall use the channel quality measure request CMD word as shown on figure 19a. The Control and Epoch fields shall be encoded as described above. Each channel quality measure selector bit (see table XVI) shall be set to 1 to request that the corresponding channel quality measure be reported, or to 0 to suppress reporting of that channel quality measure.

3	7	2	5	2	5
CMD	1100000 ('\':ALQA)	10	Control	Epoch	CQM Selectors

FIGURE 19a. ALQA channel quality measure request CMD format.

TABLE XVI. Channel quality measure selector bit assignments.

Selector Bit	CQM
5 (msb)	SINAD
4	P_c = 1 - PBER
3	Articulation Index
2	Spectral Distortion
1 (lsb)	Error-Free Interval

If KL1 is set to 1 in a channel quality measure request (which signals that the requestor wishes to use thresholds other than the default), the channel quality measure request CMD word shall be followed by a DATA word containing the respective thresholds desired, (see figure 19b) encoded as in table XVII. Threshold fields containing all 1's indicate that the default threshold for the corresponding channel quality measure should be used. Unless otherwise programmed, the default threshold for each channel quality measure shall be that corresponding to code 6 (0110) in table XVII.

3	2	4	4	4	3	4
DATA	00	SINAD	P_c = 1 0 PBER	AI	SD	0000

FIGURE 19b. ALQA channel quality measure threshold word.

TABLE XVII. Quantization of channel quality measure thresholds, error-free interval reports, and exceedance percentages.

Code	SINAD (dB)	P_c = 1 - PBER	AI	SD	EFI	AVQ (dB)	ADC	Percent
0000	2	0.700	0.01	0	1	2	1	0
0001	4	0.725	0.05	1	2	4	2	5
0010	6	0.750	0.09	2	5	6	3	10
0011	8	0.775	0.13	3	10	8	4	20
0100	10	0.800	0.19	4	20	10	5	30
0101	12	0.825	0.26	5	50	12	8	40
0110	14*	0.850*	0.33*	6*	100	14*	15*	50
0111	16	0.875	0.40	-	200	16	25	60
1000	18	0.900	0.47	-	500	18	50	70
1001	20	0.925	0.53	-	1,000	20	100	80
1010	22	0.950	0.60	-	2,000	22	200	85
1011	24	0.975	0.67	-	5,000	24	400	90
1100	26	0.985	0.73	-	10,000	26	800	95
1101	28	0.993	0.80	-	20,000	28	1600	97
1110	30	0.999	0.90	-	50,000	30	3200	99
1111	use de-fault	use default	use de-fault	use de-fault	no report	use de-fault	use de-fault	no report
* indicates default								

5.5.3.3 Link performance measure request. Link performance measure requests shall use the link performance measure request CMD word as shown on figure 20. The Control and Epoch fields shall be encoded as described above, except that KL 2-4 shall be set to 0 (channels are irrelevant to link performance measure reports). The D bit shall be set to 1 to request a data link performance measure report, or to 0 to request a voice link performance measure report. The link performance measure Threshold field shall contain the threshold for the selected link performance measure, encoded in accordance with table XVII. (If both voice and data link performance measure reports are desired, two link performance measure request CMDs shall be sent.)

3	7	2	5	2	1	4
CMD	1100000 ('\':ALQA)	11	Control	Epoch	D	LPM Threshold

FIGURE 20. ALQA link performance measure request CMD format.

5.5.3.4 Channel quality measure reports. The channel quality measure Report CMD (figure 21) shall precede channel quality measure reports. The Control field shall specify the format of the reports that follow this CMD word (until any following ALQA report CMD word, if any), and the Epoch field shall indicate the epoch of data used for all reports that follow. The Channels field shall contain a binary count of the number of reports that follow this CMD word.

3	7	2	5	2	5
CMD	1100000 ('\':ALQA)	00	Control	Epoch	Channels

FIGURE 21. Channel quality measure report CMD format.

Channel quality measure reports shall be formatted as illustrated on figure 22, except that channel quality measure fields not requested shall not be present in the reports. Each channel quality measure field is 4 bits, and carries the code from table XVII corresponding to:

a. the percentage of samples of the channel quality measure from the epoch in use that equaled or exceeded the threshold used for that channel quality measure (for SINAD, P_c, articulation index, or spectral distortion), or

b. the estimated error-free interval.

4	4	4	4	4
SINAD	P_c	AI	SD	EFI

7	4	4	4	4	4
Channel Designator	SINAD	P_c	AI	SD	EFI

20	4	4	4	4	4
Frequency Designator	SINAD	P_c	AI	SD	EFI

FIGURE 22. Channel quality measure report formats.

When a DTM is used to carry ALQA reports, the reports shall be packed bit-by-bit into the 21-bit data fields without aligning each report with the start of a new word.

When the reports do not fill the final ALE word, the remaining bits after the last report shall be filled with 0s. The DBM data block shall be likewise filled with packed reports, with the length field set to indicate the length of reports.

5.5.3.5 Link performance measure reports. Link performance measure reports shall use the link performance measure report CMD word as shown on figure 23. The Control and Epoch fields shall be encoded as described above for link performance measure requests. The D bit shall be set to 1 to indicate a data link performance measure report, or to 0 to indicate a voice link performance measure report. The link performance measure report field shall contain the percentage of time that the link performance equaled or exceeded the threshold specified for the indicated link performance measure on the link between the requesting and reporting stations, encoded in accordance with table XVII.

3	7	2	5	2	1	4
CMD	1100000 ('\':ALQA)	01	Control	Epoch	D	LPM Report

FIGURE 23. ALQA link performance measure report CMD format.

5.6 Additional orderwire functions. A variety of orderwire functions in addition to those in MIL-STD-188-141 are described in the following paragraphs. Some are required for support of linking protection, networking, and other functions to be described later. The remainder are provided to simplify and to add capabilities to the operation of automated HF radio networks.

5.6.1 Version command. The Version command is used to request ALE controller version identification. The response to a Version command is an automatic message display (AMD) message in manufacturer-specific format that shall indicate the version of hardware, software, and firmware of the responding ALE controller. The command is formatted as a user-unique CMD, with '@' in place of the manufacturer ID to indicate general applicability, and 'v' in the third character position (see figure 24).

NOTE: The pipe symbol "¦" is used on figure 24 instead of the ASCII vertical bar symbol to differentiate from the lower case "L".

3	7	7	7
CMD	User-Unique (ASCII '¦')	All Vendors (ASCII '@')	Version Command CMD (ASCII 'v')
110	1111100	1000000	1110110

FIGURE 24. Version CMD format.

5.6.2 Capabilities command. Not yet standardized.

5.6.3 Frequency select command.

a. The frequency select CMD word is formatted as shown on figure 25. A frequency designator (IAW 5.3) is sent in a DATA word immediately following the frequency select CMD, bit W_4 of this DATA word shall be set to 0, as shown.

3	7		6	4	4
CMD	1100110 ('f': frequency)		Control	100 Hz	10 Hz

		Frequency Designator				
Data	0	10 MHz	1 MHz	100 kHz	10 kHz	1 kHz
3	1	4	4	4	4	4

FIGURE 25. Frequency select CMD format.

b. The 100 Hz and 10 Hz fields in the frequency select CMD word contain BCD digits that extend the precision of the standard frequency designator. These digits shall be set to 0 except when it is necessary to specify a frequency that is not an even multiple of 1 kHz (e.g., when many narrowband modem channels are allocated within a 3 kHz voice channel).

c. The control field shall be set to 000000 to specify a frequency absolutely, to 100000 to specify a positive offset, or to 110000 to specify a negative offset.

d. A station receiving a frequency select CMD word shall in general make whatever response is required by an active protocol on the indicated frequency.

e. For example, transmit and receive frequencies for use on a link may be negotiated independently as follows:

(1) The caller selects a frequency believed to be propagating to the distant station (the prospective responder), and places a call on that frequency. The caller embeds a frequency select CMD word in the call to ask the responder to respond on a frequency chosen for good responder-to-caller propagation (probably from sounding data in the caller's LQA matrix).

(2) If the responder hears the call, it will respond on the *second* frequency, asking the caller to switch to a better caller-to-responder frequency by embedding a frequency select CMD word in its response (also based upon sounding data).

(3) The caller sends an acknowledgment on the frequency chosen by the responder (the original frequency by default), and the full duplex independent link is established.

5.6.4 Mode control. Many of the advanced features of an ALE controller are "modal" in the sense that when a particular option setting is selected, that selection remains in effect until changed or reset by some protocol event. The mode control command is used to select many of these operating modes, as described in the following paragraphs. The mode control CMD word is formatted as shown on figure 26. The first character is 'm' to identify the mode control command; the second character identifies the type of mode being selected, the remaining bits specify the new setting for that mode selected. Mode ID has not been standardized except as indicated below.

3	7	7	7
CMD	Mode Control (ASCII 'm')	Mode ID	Mode Selection
110	1101101		

FIGURE 26. Mode control CMD format.

5.6.4.1 Modem negotiation and handoff. Not yet standardized.

5.6.4.2 Crypto negotiation and handoff. Not yet standardized.

5.6.4.3 Voice port selection. Not yet standardized.

5.6.4.4 Data port selection.

a. The data port selection command is used to specify the destination for the immediately following data text message (DTM) or data block message (DBM). By default, any DTM or DBM message that arrives without an immediately preceding data port selection CMD, is assumed to carry a message for the station operator, and is routed to an appropriate data port (e.g., an operator display or a printer). The station operator data port (the default) may also be explicitly specified by preceding a message with a data port selection CMD with a port number of 0. A message destined for an attached network controller shall be preceded by a data port selection CMD with a port number of 1. A message intended for over-the-air fill shall be preceded by a data port selection CMD with a port number of 2. Other port numbers from 3 through 15 have station-specific meanings (see figure 27).

3	7	7	3	4
CMD	Mode Control (ASCII 'm')	Data Port Select (ASCII 'd')	*	Port No.
110	1101101	1100100	000	
* Reserved block (set to 000)				

FIGURE 27. Data port selection CMD format.

b. Note that the data port selected by a data port selection CMD persists only until the end of the DTM or DBM that immediately follows the data port selection CMD. Thus, a data port selection CMD not immediately followed by a DTM or DBM has no effect.

5.6.4.5 Digital LINCOMPEX zeroization. Not yet standardized.

3	7	7	7
CMD	Mode Control (ASCII 'm')	LINCOMPEX Zeroize (ASCII 'z')	(To Be Determined)
110	1101101	1111010	

FIGURE 28. Digital LINCOMPEX zeroization CMD format.

5.6.4.6 Digital squelch. Not yet standardized.

3	7	7	7
CMD	Mode Control (ASCII 'm')	Digital Squelch (ASCII 'q')	(To Be Determined)
110	1101101	1110001	

FIGURE 29. Digital squelch CMD format.

5.6.5 Power control. Not yet standardized.

3	7	14
CMD	Power Control (ASCII 'p')	(To Be Determined)
110	1110000	

FIGURE 30. Power control CMD format.

5.6.6 Scheduling functions. Not yet standardized.

5.7 ALE support for relaying. Not yet standardized.

5.8 Networking functions. Not yet standardized.

5.8.1 Route and link selection. Not yet standardized.

5.8.2 Indirect calling. Not yet standardized.

5.8.3 Network layer header.

a. All messages between network controllers begin with a single ASCII character which denotes the type of message to follow.

Within an ALE controller, the message types identified are all routed to either port 1 or port 2 based on the decision previously made for data port selection. When a networking controller receives a message, it examines this one-character header to determine the format and protocol to use in interpreting the remainder of the message.

b. The following header characters and message types have been defined. Characters not listed shall not be used until standardized.

Header	Message Type
C	Connectivity exchange
D	Remote data fill
K	Key distribution and management
M	User message
P	Remote software update
Q	Routing query
S	Network status message

5.8.4 Connectivity exchange.

a. Networking controllers exchange the contents of their path quality matrices using the following connectivity exchange (CONEX) protocol. Note that CONEX messages may be carried on any type of data link that connects the parties to the exchange. Because these messages may be relatively large, a high speed modem should be used for CONEX whenever possible; the ALE modem should only be used when no other data link is available.

b. A CONEX report pertains to the path from one station to another, which may consist of a single link (a "direct path"), or of multiple links (an "indirect path") through one or more intermediate (relay) stations. In all cases, each CONEX report includes the number of relay stations included in the path, estimates of the path quality for voice and for data, and the age of the oldest data used to estimate these path qualities.

5.8.4.1 Voice path quality. The voice quality for a path is an estimate of the end-to-end SINAD of the path. For SINAD less than 2 decibels (dB), the voice path quality is 0; for 2 through 26 dB, the quality is 1/2 SINAD (in dB); for SINAD greater than 27 dB, the quality is 14; and when the end-to-end SINAD is unknown, the quality is 15 (1111) (default value). Voice quality shall be computed as follows:

TABLE XVIII. Voice path quality cascading.

Quality 1	Quality 2	Result Quality	Quality 1	Quality 2	Result Quality
0	any	0	6	11	5
1	any	0	6	12	5
2	any	0	6	13	5
3	3	0	6	14	5
3	4	1	7	7	5
3	5	1	7	8	5
3	6	1	7	9	6
3	7	1	7	10	6
3	8	1	7	11	6
3	9	1	7	12	6
3	10	1	7	13	6
3	11	1	7	14	6
3	12	1	8	8	6
3	13	1	8	9	6
3	14	1	8	10	7
4	4	2	8	11	7
4	5	3	8	12	7
4	6	3	8	13	7
4	7	3	8	14	7
4	8	3	9	9	7
4	9	3	9	10	7
4	10	3	9	11	8
4	11	3	9	12	8
4	12	3	9	13	8
4	13	3	9	14	8
4	14	3	10	10	8
5	5	3	10	11	8
5	6	3	10	12	9
5	7	4	10	13	9
5	8	4	10	14	9
5	9	4	11	11	9
5	10	4	11	12	9
5	11	4	11	13	10
5	12	4	11	14	10
5	13	4	12	12	10
5	14	4	12	13	10
6	6	4	12	14	11
6	7	4	13	13	11
6	8	5	13	14	12
6	9	5	14	14	13
6	10	5	15	any	15

a. For a single-link path, the mean SINAD for that link (median SINAD if ALQA data is available) shall be obtained from the link controller and converted directly to a path quality code.

b. For a multi-link path, the voice quality obtained in a CONEX report from the best relay station for the ultimate destination shall be combined with the quality of the best link to that station to obtain the resulting voice path quality as specified in table XVIII. (Note that a multi-link path will never have quality 14.) The "best relay" is the station among all potential relays that gives the highest result quality after the qualities of links to those stations have been included.

5.8.4.2 <u>Data path quality</u>.

a. The data quality for a path is an estimate of the efficiency of the path in passing data traffic. The data path quality code used is based upon estimates of the time required to pass messages over each link in the path; the resulting code reflects several measures of importance to data networks: data throughput, message latency, and resource utilization (stations and channels).

b. Computing the end-to-end data path quality through one or more relay stations shall proceed as follows. Assume that station A receives a CONEX report from B about the best data path from B to X. Station A computes its path quality to X through B by combining the quality of its link to B with the report from B about B's best path to X:

(1) Station A computes the quality of its link to B as described later, and compares the result to the quality of the path from B to X as reported by B.

(2) If either quality is 0, the result is 0. Likewise, if either is 15 (unknown), the result is 15.

(3) In all other cases, the quality of the path from A to X through B is 1 less than the lower path quality of the two components.

c. The quality of a single data link is computed from the nominal data rate and measured error characteristics of that link obtained from the link controller. The result of the following formula shall be truncated to an integer in the range of 0 through 14, inclusive (e.g., if the result is less than zero, 0 shall be used).

Data link quality = 7 + Nominal Speed - ARQ Repeats.

d. The "nominal speed" term in the formula is obtained from the nominal data rate (in bps) as follows; the result shall be rounded to the nearest integer. Note that the logarithm is taken with a base of 2.

Nominal speed = $\log_2$ (data rate/75 bps).

e. The "ARQ repeats" term in the formula is the mean number of error-induced retransmissions per message of messages sent over that link during the past hour. If no messages were sent over the link during the past hour, the ARQ repeats term may be estimated using the BER of the link (measured before error correction):

BER	ARQ Repeats Est.
<0.1	0
$0.1 \leq$ BER ≤ 0.199	$\frac{\text{BER} - 0.1}{0.2 - \text{BER}}$
> 0.199	100 (link unusable)

Table XIX illustrates the use of this formula:

TABLE XIX. Examples of data path quality computations.

Link Type	Nominal Data Rate	Nominal Speed	ARQ Repeats (measured)	BER	ARQ Repeats (estimated)	Data Link Quality
DTM (ALE Modem)	53.6	0	0			7
	53.6	0		0.1181	0.22	6
HF Data Modem	2400	5	0.1			11
	2400	5		0.167	2.03	9
Wireline Modem	9600	7		0.0105	0.00	14
	9600	7	1.2			12

5.8.4.3 CONEX message format.

a. A CONEX message consists of a header, identifier(s) of the net or specific stations reported, and reports of path quality to those stations. When a net is named, the reports for the stations in the net are listed in the standard order for that net, without sending the individual station identifiers. A flow diagram for the structure of a CONEX message is shown on figure 31.

CONEX messages are formatted in even multiples of 7 bits to simplify the insertion of these reports into the natural data blocks of the links likely to be available (e.g., the 21 bits available in the DTM words of the ALE controller or 7-bit ASCII characters which should be compatible with nearly any wireline modem protocol).

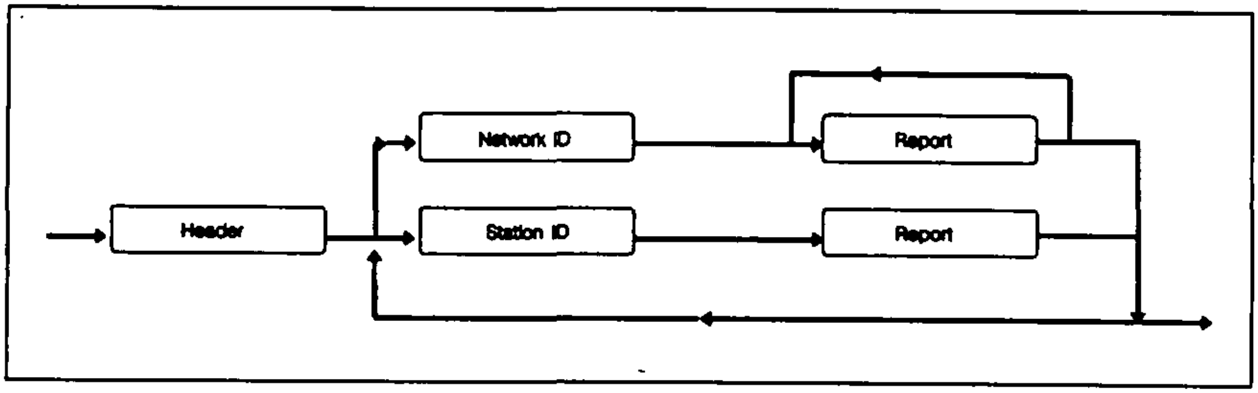


FIGURE 31. Structure of CONEX message.

b. The CONEX message header contains a 14-bit Control field, followed by the name of the sending station, as shown on figure 32. The first bit of the Control field is set to 1 to request CONEX from responding stations, or to 0 to suppress such responses. The second bit is set to 1 to indicate that CONEX reports follow the sending station name. If this bit is 0, no reports are included in this message. The next five bits in the Control field contain a count of the characters in the sending station name. The Max Age and Max Relays fields apply to CONEX requests: the responding station shall only return reports whose Age and Relays fields do not exceed these limits (a 7 in a field means no limit). The Control field is followed by the number of 7-bit ASCII characters indicated in the Count field.

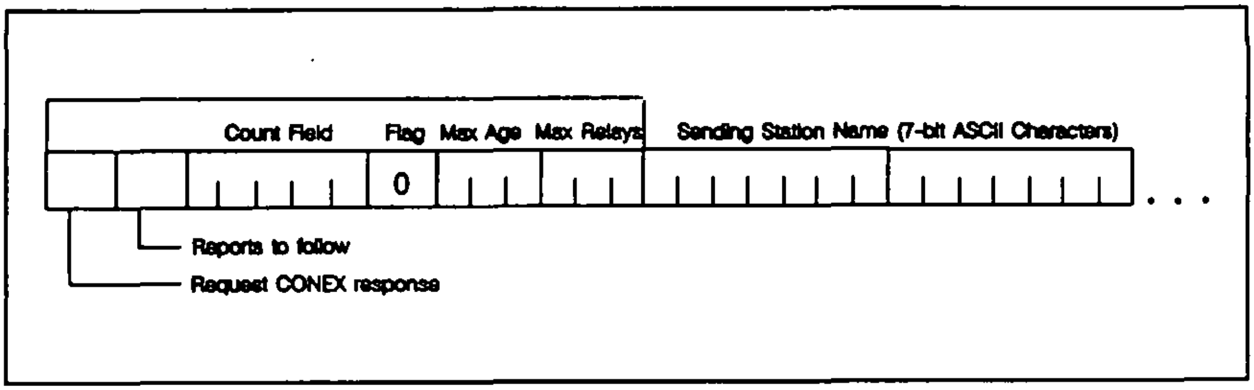


FIGURE 32. CONEX header.

c. Station and network IDs have a similar structure to the CONEX header. Each begins with a 7-bit Control field, which is followed by the 7-bit ASCII characters composing the name of that station or network (figure 33). The first control bit is set to 0 for an individual station identifier, and to 1 for a network identifier. The second bit is set to 0 in the last ID in the CONEX message, and to 1 for all of the preceding station and network IDs. The last five bits in the Control field contain a count of the characters in the station or network name. The Control field is followed by the number of 7-bit ASCII characters indicated in this count.

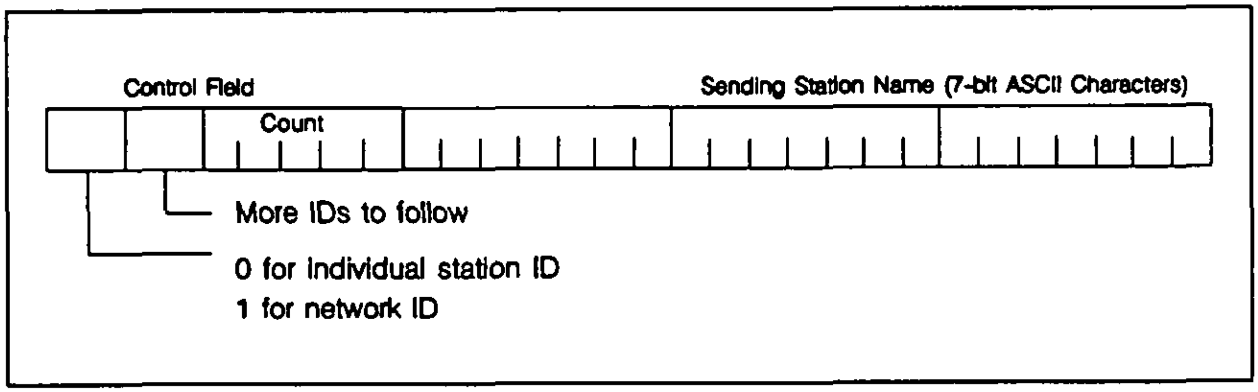


FIGURE 33. CONEX station or network ID.

d. Each report in a CONEX message refers to the best path from the sending station to a specified destination. When the report is preceded by a station ID, the report pertains to the best path to that station. When the report is one of a sequence of reports following a network ID, the destination station is known implicitly from the position of the report in that sequence.

e. Each report contains four fields as shown on figure 34: the minimum number of relays between the sending station and the destination station (3 bits), end-to-end quality of the best path(s) to the destination for voice or data use (4 bits each), and the age of the oldest data used to compute the voice and data path qualities (3 bits).

3	4	3	4
Age	Voice Quality	Relays	Data Quality

FIGURE 34. CONEX report.

f. The Age field uses the same encoding as in the LQA report (5.4.4). For up to six relays in the path, the Relays field contains the number of relays. For six or more relays, the Relays field contains 110 (six). When the number of relays is unknown, the Relays field is set to 111 (seven).

5.8.4.4 CONEX broadcast.

a. Stations may periodically broadcast CONEX messages containing reports of path quality to selected destinations (e.g., net control stations, gateways to other networks, or distant network members that are difficult for some members to reach). The rate of these broadcasts, the channels used, and the stations included in the CONEX report may be selected by the operator, or determined adaptively by the networking controller. A CONEX broadcast will typically use an ALE scanning call to a net or group. The CONEX message may be sent using DTM or DBM with the ALE modem, or by switching to a data modem for reduced channel overhead when long reports are sent.

b. A station receiving a CONEX broadcast shall update its path quality matrix using the data received along with link quality data from the link controller receiving the broadcast, as described above.

5.8.4.5 <u>CONEX handshake</u>. A CONEX handshake is used to exchange connectivity data among networking controllers. The request bit is set to 1 to request connectivity, and the Max Age and Max Relays fields may be used to restrict the number of reports received. ALE is used to establish the link(s) used, as required; the CONEX messages may be conveyed using either the ALE modem (with DTM or DBM) or a data modem.

5.9 <u>Network management</u>. Not yet standardized.

5.10 <u>Multi-media operation</u>. Not yet standardized.

5.11 <u>Special requirements</u>. Not yet standardized.

6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Intended use.

6.1.1 General.

a. The purpose of this document is to provide the technical parameters for the functions and features of advanced adaptive HF radio, and provide logical and cohesive guidelines for both industry and the Government.

b. There is no requirement for linking protection to be a part of a user's acquisition unless the user has an identified need. Optional levels of linking protection are identified and detailed. These options, AL-1 and AL-2, provide an inexpensive, least protected mode and a more sophisticated protection mode. The user should establish their application level based on minimum essential requirements.

c. There is no requirement for ALQA to be a part of a user's acquisition unless the user has an identified need. The user should establish their need based on minimum essential requirements.

d. This document is structured segmentally, with each segment being added as it is developed. The outline of MIL-STD-187-721 used in this document includes areas anticipated to be covered in other segments. These areas are referenced in this document as "not yet standardized."

6.1.2 Interaction matrix. The complexity of the adaptive features and functions may be confusing to the user of this standard. Certain parts of the technical features are dependent on other features defined within this standard and MIL-STD-188-141. This dependency is not always apparent to the user or the acquisition activity. The following matrix provides the interaction dependencies known, as of the publication date.

Interaction matrix

	Function or Feature	Requires:				Benefits From:		
	Basic ALE							
1	Sounding							
2	Basic LQA							
3	Individual calls							
4	Star net calls							
5	Star group calls							
6	Anycalls							
7	AMD							
	ALE Data Modes							
10	DTM							
11	DBM							
	Link Quality Functions							
20	LQA matrix	2						
21	Local noise sound							
22	Individual polling	2	3					
23	Net poll	2	4					
24	Group poll	2	5					
25	Poll before link	2	51			50		
26	LQA scoring algorithm							
27	LQA aging algorithm	20						
28	LQA report	20						
	ALE Addressing and Calling Functions							
30	Multipoint net calls	4						
31	Multipoint group calls	5						
32	ALE indirect addressing							
33	ALE directed query addressing							
34	ALE anycall query addressing	6						
	Additional ALE CMD Types							
40	Data port selection ALE CMD							
41	Software Version ALE CMD	7						

Interaction matrix - continued.

	Function or Feature	Requires:				Benefits From:		
	Other Data Link Layer Functions and Features							
50	Channel designators							
51	Frequency designators							
52	FDX independent operation	51				50		
53	Response to connectivity queries	33	34					
54	Adaptive data link	10	2			11		
55	Tandem data links	32				11	10	
56	Best links report to net control	20				26	27	
57	Connectivity report to net control							
	Network Layer Connectivity Functions							
60	Path quality matrix	56						
61	Conectivity tracking	57						
62	CONEX data format							
63	CONEX handshake	62	61			60		
64	CONEX broadcast (send)	62	61			60		
65	CONEX broadcast (receive)	62						
	Network Layer Routing Functions							
70	Routing matrix					60		
71	Manual routing table maintenance	70						
72	Adaptive routing	70	61			63	65	
73	Indirect calling	70				63	65	
74	Relay calling	70				63	65	
75	Slave router	32				55		
76	Source routing	70				32		
77	Query routing	34				33	70	
	Network Layer Message Handling Functions							
80	Network layer header							
81	AME header	80						
82	Automatic msg exchange	81						
83	Message buffering	82						

Interaction matrix - continued.

	Function or Feature	Requires:				Benefits From:		
	Network Management Functions							
90	Net status message protocol	80						
91	Remote data fill	80						
92	Remote software update	80						
93	Key distribution/management	80						
	Higher-level Functions							
100	Multi-media interface	70	82			83		
101	Mailbox operation	82				83		
102	BBS operation	82				83		

6.2 Tailoring. This document cannot be tailored further than the proper selection made from the intended use paragraph above.

6.3 Subject term (key word) listing.

Adaptive HF radio
ALE
ALQA
Application level
Articulation Index
Automatic link establishment
Channel quality measure
Connectivity exchanges
Epoch
Error-free interval
Forward error correction
Histogram
Link performance measure
Linking protection
Link quality functions
LQA
Networking controller
Networking functions
Polling protocols
Protection interval
SINAD
Spectral distortion
Time protocols

CONCLUDING MATERIAL

Custodians:
- Army - SC
- Navy - EC
- Air Force - 90

Review activities:
- Army - CR
- Navy - MC
- DoD - DC, NS, DI

User activities:
- Army - AC, PT
- Navy - NC, TD, OM, CG
- Air Force - 02,13,21
- DoD - DH, ECAC, MP
- DOT - FAA, OST

Civil agency coordinating activities:
- NCS

Preparing activity:
Army - SC

(Project TCSS-7211)

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER	2. DOCUMENT DATE *(YYMMDD)*

3. DOCUMENT TITLE

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME *(Last, First, Middle Initial)*	b. ORGANIZATION	
c. ADDRESS *(Include Zip Code)*	d. TELEPHONE *(Include Area Code)* (1) Commercial (2) AUTOVON *(If applicable)*	7. DATE SUBMITTED *(YYMMDD)*

8. PREPARING ACTIVITY

a. NAME	b. TELEPHONE *(Include Area Code)* (1) Commercial (2) AUTOVON
c. ADDRESS *(Include Zip Code)*	**IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:** Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340