NOT
MEASUREMENT
SENSITIVE

MIL-STD-188-141D
22 December 2017
SUPERSEDING
MIL-STD-188-141C
27 December 2011

DEPARTMENT OF DEFENSE
INTERFACE STANDARD

INTEROPERABILITY AND PERFORMANCE STANDARDS FOR MEDIUM AND HIGH FREQUENCY RADIO SYSTEMS

AMSC N/A AREA TCSS

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited.

FOREWORD

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

2. In accordance with DoD Instruction 4630.8, it is DoD policy that all forces for joint and combined operations be supported through compatible, interoperable, and integrated Command, Control, Communications, and Intelligence (C3I) systems. Furthermore, all C3I systems developed for use by U.S. forces are considered to be for joint use. The director of the Defense Information Systems Agency (DISA) serves as DoD's single point of contact for developing information technology standards to achieve interoperability and compatibility. All C3I systems and equipment shall conform to technical and procedural standards for interface, interoperability, and compatibility, as recommended by DISA.

3. MIL-STDs in the 188 series (MIL-STD-188-XXX) address telecommunication design parameters based on proven technologies. These MIL-STDs are to be used in all new DoD systems and equipment, or major upgrades thereto, to ensure interoperability. The MIL-STD-188 series is subdivided into a MIL-STD-188-100 series, covering common standards for tactical and long-haul communications; a MIL-STD-188-200 series, covering standards for tactical communications only; and a MIL-STD-300 series, covering standards for long-haul communications only. Emphasis is being placed on the development of common standards for tactical and long-haul communications (the MIL-STD-188-100 series). The MIL-STD-188 series may be based on, or make reference to, Joint Technical Architecture, American National Standards Institute (ANSI) standards, International Telecommunications Union (ITU) recommendations, North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAG), and other standards wherever applicable.

4. This document contains technical standards and design objectives for medium- and high-frequency radio systems. Included are: (1) the basic radio parameters to support both conventional and adaptive radio communications; and (2) technical parameters for automatic link establishment (ALE), linking protection, and other advanced adaptive features and functions.

5. The technical parameters in certain identified paragraphs have not (as of the date of publication) been verified by testing or implementation. These parameters have, however, been subjected to rigorous simulation and computer modeling. The DoD working group and the Technical Advisory Committee (TAC) are confident that these features, functions, and parameters are technically valid. The un-tested portion of the technology are marked (NT) following the title of each paragraph containing un-tested material.

6. Users of this MIL-STD should note that there is no proprietary or otherwise restricted use material in this document. This document is for unrestricted DoD, federal, and industry use.

7. Comments, suggestions, or questions on this document should be addressed Air Force Sustainment Center – Oklahoma City/AFLCMC/LZPES, 3001 Staff Drive, Suite 1AB81A, Tinker AFB, OK 73145, or emailed to ocalc.dsp@us.af.mil. Since contact information can change, you may want to verify the currency of this address information using the ASSIST Online database at https://assist.dla.mil.

CONTENTS

CONTENTS (continued)

TABLES

FIGURES

APPENDICES

1. SCOPE.

1.1 Scope.

The purpose of this document is to establish technical performance and interface parameters in the form of firm requirements and optional design objectives (DO) that are considered necessary to ensure interoperability and interface standardization of new long-haul and tactical radio systems in the medium frequency (MF) band and in the high frequency (HF) band. It is also the purpose of this document to establish a level of performance for new radio equipment that is considered necessary to satisfy the requirements of the majority of users. These technical parameters, therefore, represent a minimum set of interoperability, interface, and performance standards. The technical parameters of this document may be exceeded in order to satisfy certain specific requirements, provided that interoperability is maintained. That is, the capability to incorporate features such as additional standard and nonstandard interfaces is not precluded.

1.2 Applicability.

This standard is approved for use within the Department of Defense (DoD) in the design and development of new MF and HF radio systems. It is not intended that existing equipment and systems be immediately converted to comply with the provisions of this standard. However, this standard establishes requirements for new equipment and systems, and those undergoing major modification or rehabilitation. If deviation from this standard is required, the user should contact the lead standardization activity for waiver procedures.

1.3 Application guidance.

The terms “system standard” and “design objective” are defined in FED-STD-1037. In this document, the word “shall” identifies firm requirements. The word “should” identifies design objectives that are desirable but not mandatory.

2. APPLICABLE DOCUMENTS.

2.1 General.

The documents listed in this section are specified in sections 3 or 4 of this standard. This section does not include documents cited in other sections of this standard, those recommended for additional information, or those used as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in sections 3 or 4 of this standard, whether or not they are listed.

2.2 Government documents.

2.2.1 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 cited in the solicitation or contract.

INTERNATIONAL STANDARDIZATION AGREEMENTS

North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs)

STANAG 4203	Technical Standards for Single Channel HF Radio Equipment
STANAG 4539	Technical Standards for Non-Hopping HF Communications Waveforms
STANAG 5035	Introduction of an Improved System for Maritime Air Communications on HF, LF, and UHF
STANAG 5066	Profile for HF Data Communication

Quadripartite Standardization Agreements (QSTAGs)

QSTAG 733	Technical Standards for Single Channel High Frequency Radio Equipment

FEDERAL STANDARDS

FED-STD-1037	Telecommunications: Glossary of Telecommunications Terms

DEPARTMENT OF DEFENSE STANDARDS

MIL-STD-188-110	Interoperability and Performance Standards for HF Data Modems
MIL-STD-188-148	Interoperability Standard for Anti-Jam (AJ) Communications in the High Frequency (2-30 MHz) Band (U)

(Copies of these documents are available online at http://quicksearch.dla.mil.)

2.2.2 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 of these documents are those cited in the solicitation or contract.

U.S. DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration (NTIA)

NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

(Applications for copies should be addressed to the U.S. Department of Commerce, NTIA, Room 4890, 14th and Constitution Ave. N.W., Washington, DC 20230 or online at http://www.ntia.doc.gov/osmhome/redbook/redbook.html .)

2.3 Non-Government publications. The following documents form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

TELECOMMUNICATIONS INDUSTRIES ASSOCIATION (TIA)

(Formerly Electronic Industries Association (EIA))

TIA/EIA-422	Electrical Characteristics of Balanced Voltage Digital Interface Circuits
TIA/EIA-423	Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits

(Application for copies may be submitted online at: http://www.tiaonline.org/standards/catalog/ should be addressed to the Telecommunications Industries Association (TIA), 2500 Wilson Boulevard, Arlington, VA 22201, ATTN: Standard Sales Office

(Non-Government standards and other publications are normally available from the organizations that prepare or distribute the documents. These documents also may be available in or through libraries or other informational services.)

2.4 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 as specified in the current edition of FED-STD-1037, except where inconsistent with the use in this standard. In addition, the following definitions are applicable for the purpose of this standard.

2-ISB. Two-channel independent sideband operation with one nominal 3-kHz channel in the upper sideband (USB) and one in the lower sideband (LSB); that is two independent 3-kHz channels—one in each sideband.

4-ISB. Four-channel independent sideband operation with two nominal 3-kHz channels in the upper sideband (USB) and two in the lower sideband (LSB); that is four independent 3-kHz channels—two in each sideband.

Assigned frequency. The center of the frequency band assigned to a station. Note: The frequency of the RF carrier, whether suppressed or radiated, is usually given in parentheses following the assigned frequency, and is the frequency appearing in the dial settings of RF equipment intended for single-sideband or independent-sideband transmission.

Assigned frequency band: The frequency band within which the emission of a station is authorized.

Co-sited operation. Multiple radio circuits operating within close proximity of each other, so that their emanations may couple into adjacent antennas or radio equipment, resulting in unexpected intermodulation and other effects.

High-performance HF data modem. High-speed (capable of at least 1200 bits per second) or robust data modes which incorporate sophisticated techniques for correcting or reducing the number of raw (over-the-air induced) errors.

Linking protection (LP). Protection (authentication) of the linking function that establishes, controls, maintains, and terminates the radio link.

Manpack. A radio system, including power source that is intended for use while being carried by an individual.

Necessary bandwidth. For a given class of emission, the width of the frequency band which is just sufficient to ensure the transmission of information at the rate and with the quality required under specified conditions.

Second generation automatic link establishment (2G ALE). ALE as first technically described in Appendix A of this document.

Third generation automatic link establishment (3G ALE). ALE as first technically described in Appendix C of this document.

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

2G ALE	second generation automatic link establishment
2-ISB	two channel independent sideband
3G ALE	third generation automatic link establishment
4G ALE	fourth generation automatic link establishment
4-ISB	four channel independent sideband
ABCA	American, British, Canadian, Australian
AGC	automatic gain control
AJ	Anti-Jam
ALC	automatic level control
ALE	automatic link establishment
ANSI	American National Standards Institute
ARQ	automatic repeat request
b/s	bits per second
Bd	baud
C3I	Command, Control, Communications, and Intelligence
CCIR	International Radio Consultative Committee
dB	decibels
dBc	decibels referenced to full-rated peak envelope power
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAC	Defense Information Systems Agency Circular
DO	design objective
DoD	Department of Defense
EMC	electromagnetic compatibility
FDM	frequency division multiplex
FEC	forward error correction
FSK	frequency-shift keying
HF	high frequency
Hz	Hertz
ICW	interrupted continuous wave
IF	intermediate frequency
IMD	intermodulation distortion
ISB	independent sideband
ITU	International Telecommunications Union
kHz	kilohertz
LP	linking protection
LQA	link quality analysis
LSB	lower sideband
MF	medium frequency
MHz	megahertz
ms	millisecond
NATO	North Atlantic Treaty Organization

NSA	National Security Agency
NT	not tested
NTIA	National Telecommunications and Information Administration
PEP	peak envelope power
PI	protection interval
PTT	push-to-talk
QSTAG	Quadripartite Standard Agreement
RF	radio frequency
SINAD	signal-plus-noise-plus-distortion to noise-plus-distortion ratio
SSB	single-sideband
STANAG	Standard Agreement
TAC	Technical Advisory Committee
TOD	time of day
uncl	unclassified
USB	upper sideband
VSWR	voltage standing wave ratio
WALE	wideband automatic link establishment
WBHF	wideband high frequency

4. GENERAL REQUIREMENTS.

4.1 General.

By convention, frequency band allocation for the MF band is from 0.3 megahertz (MHz) to 3 MHz and the HF band is from 3 MHz to 30 MHz. However, for military purposes, equipment designed for HF band use has been historically designed with frequency coverage extending into the MF band. For new HF equipment, HF band standard parameters shall apply to any portion of the MF band, at 2.0 MHz or above, that is included as extended coverage. Currently there are no known military requirements below 2.0 MHz. Consequently, this portion of the MF band is not standardized.

4.1.1 Equipment parameters.

Equipment parameters will be categorized using functional use groups for radio assemblages/sets. Historically, these groups have been fixed (long-haul) installations and tactical systems. The tactical sets are subgrouped further into vehicle transportable and manpack versions. Although these distinctions still exist in principle, the former lines of distinction have become somewhat blurred. The mobility of current military forces dictates that a significant number of long-haul requirements will be met with transportable systems, and in some cases, such systems are implemented with design components shared with manpack radios. When such “tactical” equipment is used to meet a long-haul requirement, the equipment shall meet long-haul minimum performance standards. (See additional application guidance in section 6.)

4.1.2 Basic HF radio parameters.

Basic HF radio parameters are contained in this section and in section 5. HF technology going beyond the basic radio is contained in the appendices. Figure 1 shows the relationship of the functional aspects of current HF technology in terms of the Internet reference model. The un-

shaded area in Figure 1 indicates coverage in this section and section 5. Corresponding physical layer interface points are depicted in Figure 2.

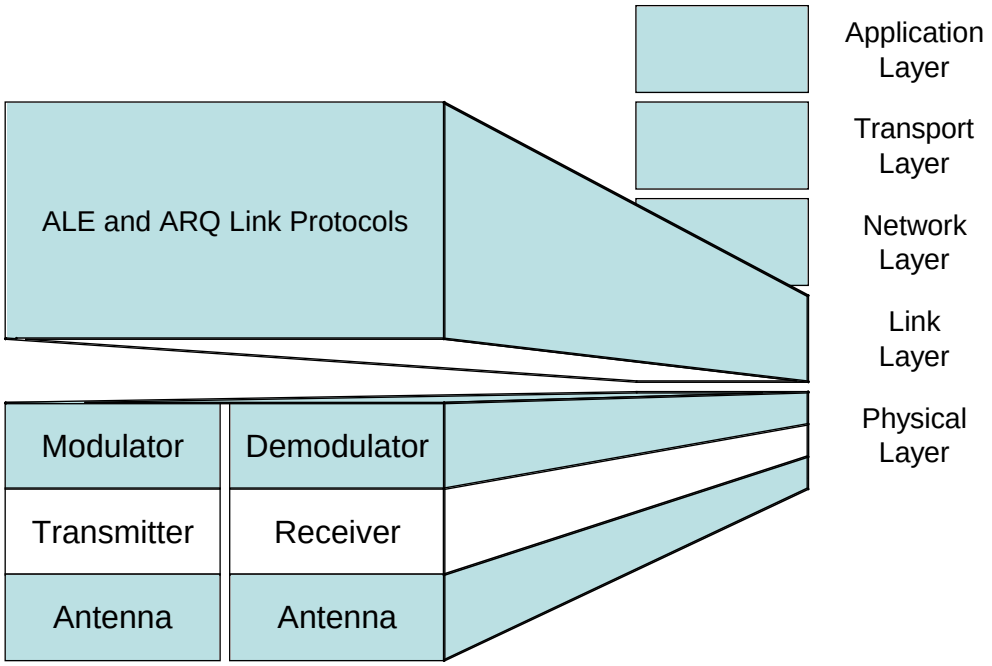


FIGURE 1. Physical layer with transceiver and modem elements.

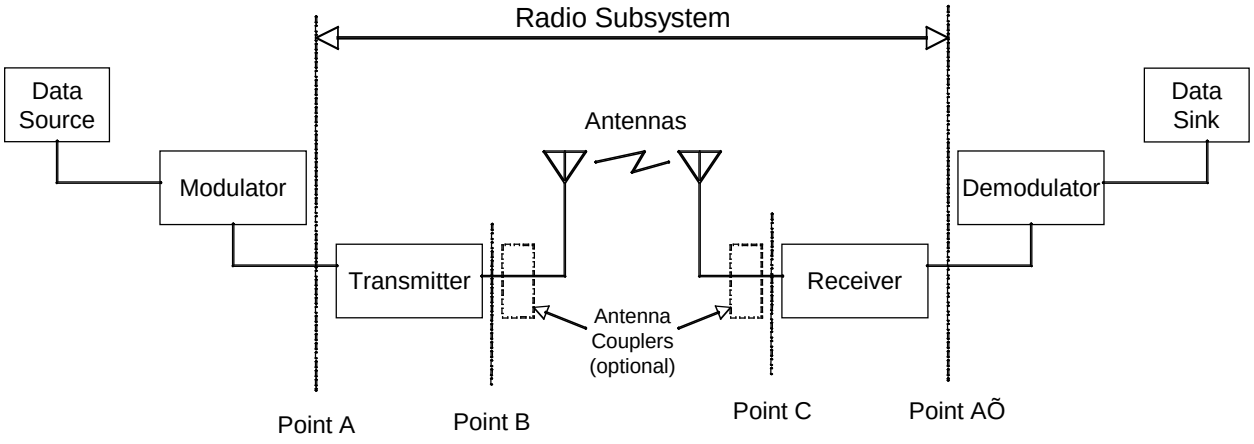


FIGURE 2. Radio subsystems interface points.

4.2 Equipment operation mode.

4.2.1 Baseline mode.
a. Frequency control of all new HF equipment, except manpack, shall be capable of being stabilized by an external standard.

b. Should multiple-frequency (channel) storage be incorporated, it shall be of the programmable memory type and be capable of storing/initializing the operational mode (see paragraphs 4.2.1.1 and 4.2.1.2 below, and paragraph A.4.3.1 of Appendix A) associated with each particular channel.

4.2.1.1 Single-channel.
All new single-channel HF equipment shall provide, as a minimum, the capability for the following one-at-a-time selectable operational modes:

a. One nominal 3-kiloHertz (kHz) channel upper sideband (USB) or lower sideband (LSB) (selectable).

b. One (rate-dependent bandwidth) interrupted continuous wave (ICW) channel.*

*Not mandatory for radio systems that include automatic link establishment (ALE) per Appendix A, Appendix C, or Appendix G.

Optionally a wideband HF (WBHF) mode may be provided, with a nominal channel width of N x 3 kHz, where N may be 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, or 16 (selectable).

4.2.1.2 Multichannel.
Should a multichannel capability be implemented, the multichannel HF equipment shall provide a single channel capability as set forth in paragraph 4.2.1.1 and two-channel independent sideband (2-ISB), as a minimum.

Optionally one or more of the following additional modes may be provided, selectable one at a time:

a. Two nominal 3-kHz channels in the USB or LSB (two independent channels in the same sideband—sideband selectable).

b. Two nominal 3-kHz channels in the USB and two in the LSB (four independent 3-kHz channels, two in each sideband).

4.2.2 Manual mode push-to-talk operation.
Push-to-talk (PTT) operation is a common form of interaction with MF/HF single sideband (SSB) radios, especially for tactical use by minimally trained, “noncommunicator” operators. Manual control with PTT shall be conventional; that is, the operator pushes the PTT button to talk and releases it to listen.

4.2.3 ALE mode.
Should a Second Generation ALE (2G ALE) capability be included, it shall be in accordance with Appendix A. Should Third Generation ALE (3G ALE) be included, it shall be in accordance with Appendix C. Should Fourth Generation ALE (4G ALE) be included, it shall be in accordance with Appendix G. See 4.5 for the list of features required to support this operational mode.

4.2.4 Anti-jam (AJ) mode.
If AJ is to be implemented, the AJ capabilities and features for HF radios shall be in accordance with MIL-STD-188-148.

4.2.5 Linking protection (LP).
If LP is to be implemented, the LP capabilities and features for HF radios shall be in accordance with Appendix B.

4.3 Interface parameters.

4.3.1 Electrical characteristics of digital interfaces.
Any interfaces provided for serial binary data shall be in accordance with the provisions of TIA/EIA-422 and TIA/EIA-423, and any other interface requirements specified by the contracting agencies. Such interfaces shall include provisions for request-to-send and clear-to-send signaling. The capability to accept additional standard interfaces is not precluded.

4.3.2 Electrical characteristics of analog interfaces.
An analog handset interface shall be provided. Line level analog interface(s) are optional if the system includes an internal modem. See 5.3.6 and 5.4.5 for electrical characteristics.

4.4 NATO and Quadripartite interoperability requirements.

4.4.1 Single-channel communications systems.
If interoperation with NATO member nations is required for land, air, and maritime applications, single-channel HF radio equipment shall comply with the applicable requirements of the current edition of STANAG 4203.

4.4.2 Maritime air communications systems.
If interoperation with NATO member nations is required, HF maritime air communications shall comply with the applicable requirements of the current edition of STANAG 5035.

4.4.3 High-performance HF data modems.
If interoperation with NATO member nations is required, land, air, and maritime, single-channel HF radio equipment shall comply with the “Associated communications equipment” requirements of STANAG 4539.

4.4.4 QSTAGs.
If interoperation among American, British, Canadian, Australian (ABCA), and New Zealand Armies is required, HF combat net radio equipment shall comply with the applicable requirements of the current edition of QSTAG 733.

4.5 Adaptive communications.
Adaptive HF describes any HF communications system that has the ability to sense its communications environment, and, if required, to automatically adjust operations to improve communications performance. Should the user elect to incorporate adaptive features, they shall be in accordance with the requirements as follows:

a. Channel (frequency) scanning capability.

b. ALE using an embedded selective calling capability. A disabling capability and a capability to inhibit responses shall be included.

c. Automatic sounding (station-identifiable transmissions). A capability to disable sounding and a capability to inhibit responses shall be included.

d. Limited link quality analysis (LQA) for assisting the ALE function:

(1) Relative data error assessment.

(2) Relative signal-plus-noise-plus-distortion to noise-plus-distortion ratio (SINAD).

(3) Multipath/distortion assessment (DO) (optional).

e. Automatic link maintenance

f. Channel occupancy detection (performed on the entire channel bandwidth to be used)

4.6 Linking protection.
Should linking protection be provided, it shall be in accordance with Appendix B. New designs should employ the HALFLOOP algorithm in Appendix H, rather than the Lattice algorithm in Appendix B.

4.7 HF data link protocol.
Should an HF data link protocol be provided, it shall be in accordance with STANAG 5066.

4.8 Networking functions.
Should adaptive networking be provided, it should follow the recommendations in Appendix D.

4.9 HF e-mail and other application protocols for HF radio networks.
Should HF e-mail or other applications be provided, they should be in accordance with Appendix E, Application Protocols for HF Radio Networks.

5. DETAILED REQUIREMENTS.

5.1 General.

5.1.1 Introduction.
This section provides detailed performance standards for MF and HF radio equipment. These performance standards shall apply over the appropriate frequency range from 2.0 MHz to 29.9999 MHz.

5.1.2 Signal and noise relationships.
The signal and noise relationships are expressed as SINAD, unless otherwise identified. Unless otherwise specified, when the ratio is stated, the noise bandwidth is the channel bandwidth (typically 3 kHz) used by the transmitted waveform of the unit under test..

5.2 Common equipment characteristics.
These characteristics shall apply to each transmitter and to each receiver unless otherwise specified.

5.2.1 Displayed frequency.
When operating in SSB or any ISB mode, the displayed frequency shall be that of the carrier, whether suppressed or not. When operating in WBHF mode, the displayed frequency shall be the center of the occupied portion of the wideband channel (i.e., the center of the energy of the WBHF signal).

5.2.2 Frequency coverage.
The radio equipment shall be capable of operating over the frequency range of 2.0 MHz to 29.9999 MHz in a maximum of 100-Hz frequency increments (DO: 10-Hz) for single-channel equipment, and 10-Hz frequency increments (DO: 1-Hz) for multichannel equipment.

5.2.3 Frequency accuracy.
The accuracy of the radio carrier frequency, including tolerance and long-term stability, but not any variation due to Doppler shift, shall be within $\pm$30 Hz for tactical applications and within $\pm$10 Hz for all others, during a period of not less than 30 days. Tactical systems (manpack and vehicular) that must interoperate with long haul systems shall meet the $\pm$10 Hz radio carrier frequency specification.

5.2.4 Co-sited operation
Radio systems intended for co-sited operation must meet additional requirements as detailed in Appendix F.

5.2.5 Phase noise. Deleted.

5.2.6 Bandwidths.
The bandwidths for high frequency band emissions shall be as shown in Table I. Use of other HF band emissions is optional. However, if selected, they shall be as shown in Table I. Other high frequency band emissions, which may be required to satisfy specific user requirements, can be

found in the NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management.

TABLE I. Bandwidths.

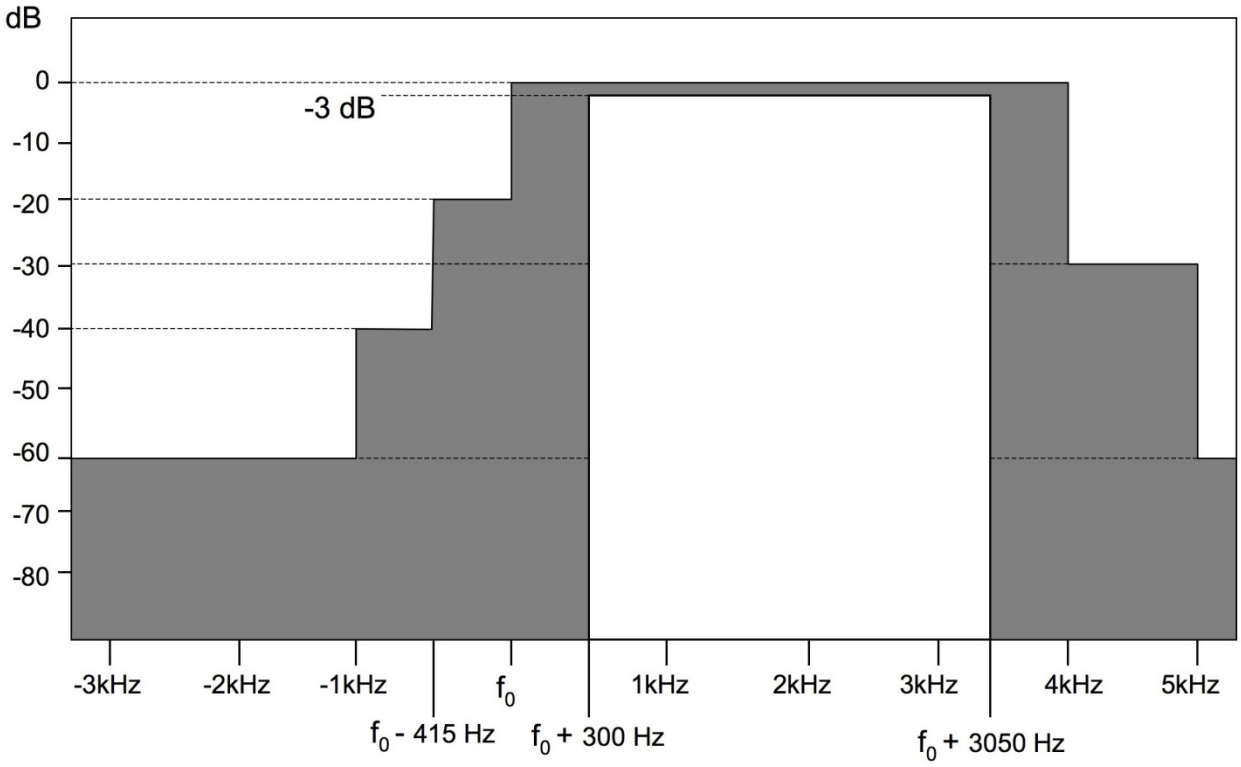
Emission type	Maximum Allowable 3 decibels (dB) Bandwidth (kHz)	Mandatory Requirement
ICW	0.5	Yes*
Single-channel modulation one 3 kHz channel	see 5.2.7.1	Yes
oneWBHF channel	see 5.2.7.2	No
Multi-channel modulation two 3 kHz channels	see 5.2.7.1	No
four 3 kHz channels	see 5.2.7.3	No
* Not mandatory for radio systems that include automatic link establishment (ALE) per Appendix A, Appendix C, or Appendix G.		

5.2.7 Overall channel amplitude responses.

The channel amplitude responses specified here apply to all radio systems. More stringent requirements may be specified elsewhere for certain applications (e.g., for ALE or LINK-11 systems).

5.2.7.1 Single-channel SSB or dual-channel (2-ISB) operation in 3 kHz channels.
The amplitude vs. frequency response between (f_0 + 300 Hz) and (f_0 + 3050 Hz) shall be within 3 dB (total) where f_0 is the carrier frequency. The attenuation shall be at least 20 dB from f_0 to (f_0 - 415 Hz), at least 40 dB from (f_0 - 415 Hz) to (f_0 - 1000 Hz), and at least 60 dB below (f_0 - 1000 Hz). Attenuation shall be at least 30 dB from (f_0 + 4000 Hz) to (f_0 + 5000 Hz) and at least 60 dB above (f_0 + 5000 Hz). See Figure 3.

NOTE: Although the response values given are for single-channel USB operation, an identical shape, but inverted channel response, is required for LSB or the inverted channel of a dual-channel independent sideband operation.



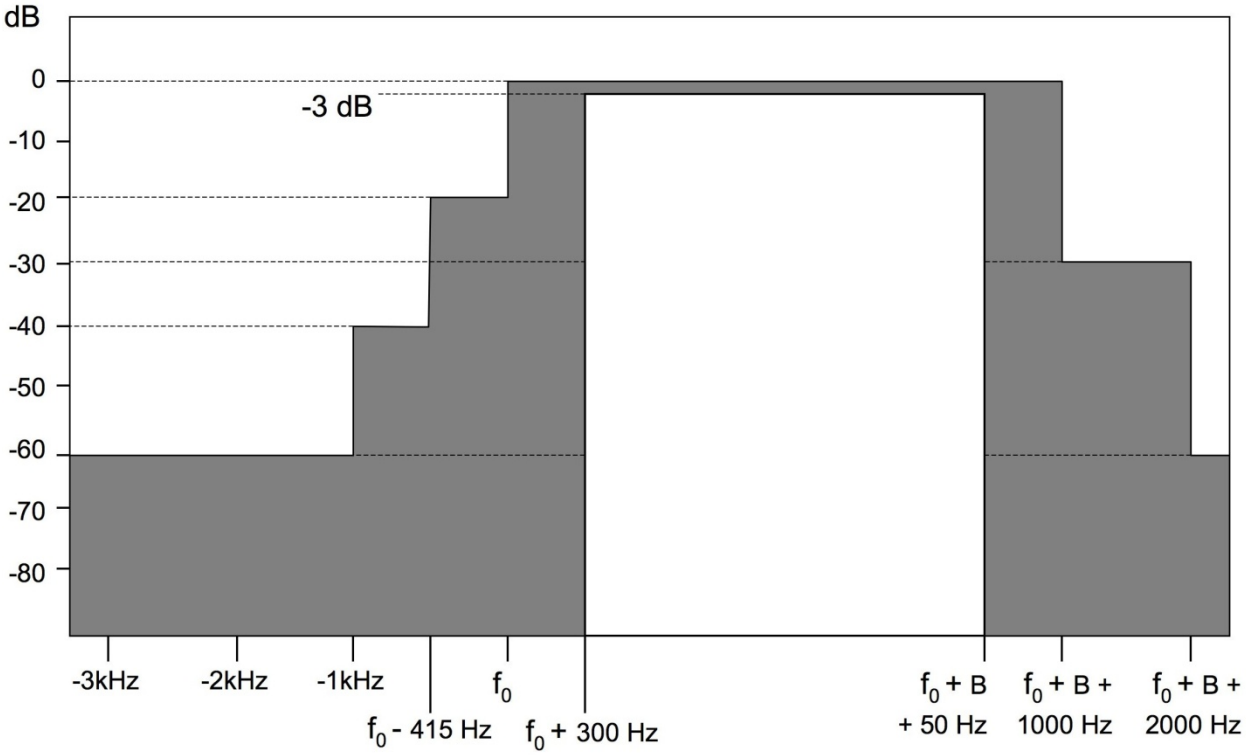
NOTES:

1. Channel response shall be within shaded portion of curve.
2. f_0 for a single channel is the carrier frequency.
3. f_0 for 2-channel ISB is the center frequency.

FIGURE 3. Overall channel response for single or dual 3kHz channel equipment.

5.2.7.2 Operation in channels wider than 3 kHz.
When operating in WBHF channels, the amplitude vs. frequency response shall be in accordance with figure 4, where the allocated bandwidth B is N x 3 kHz per channel, N may be 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, or 16. Between (f_0 + 300 Hz) and (f_0 + B + 50 Hz) the amplitude vs. frequency response shall be within 3 dB (total) where f_0 is the carrier frequency. The attenuation shall be at least 20 dB from f_0 to (f_0 - 415 Hz), at least 40 dB from (f_0 - 415 Hz) to (f_0 - 1000 Hz), and at least 60 dB below (f_0 - 1000 Hz). Attenuation shall be at least 30 dB from (f_0 + B + 1000 Hz) to (f_0 + B + 2000 Hz) and at least 60 dB above (f_0 + B + 2000 Hz).

NOTE: WBHF signals shall always be transmitted as USB, i.e., a higher frequency in the baseband shall always produce a higher frequency at RF.



NOTES:

1. Channel response shall be within shaded portion of curve.
2. f_0 for a single channel is the carrier frequency.
3. f_0 for 2-channel ISB is the center frequency.
4. B is the nominal channel bandwidth (N x 3 kHz)

FIGURE 4. Overall channel response for single or dual channel WBHF equipment.

5.2.7.3 Four-channel operation.
When four-channel independent sideband (4-ISB) operation is employed, the four individual 3-kHz channels shall be configured as shown in figure 5, which also shows the amplitude response for these four channels. Channels A2 and B2 shall be inverted and displaced with respect to channels A1 and B1 as shown on the figure. This can be accomplished by using subcarrier frequencies of 6290 Hz above and below the center carrier frequency, or by other suitable techniques that produce the required channel displacements and inversions.

The suppression of any subcarriers used shall be at least 40 dB (DO: 50 dB) below the level of a single tone in the A2 or B2 channel modulating the transmitter to 25 percent of peak envelope power (PEP). See Figure 5. The radio frequency (RF) amplitude versus frequency response for each ISB channel shall be within 2 dB between 250 Hz and 3100 Hz, referenced to each channel's carrier (either actual or virtual). Referenced from each channel's carrier, the channel attenuation shall be at least 40 dB at 50 Hz and 3250 Hz, and at least 60 dB at -250 Hz and 3550 Hz.

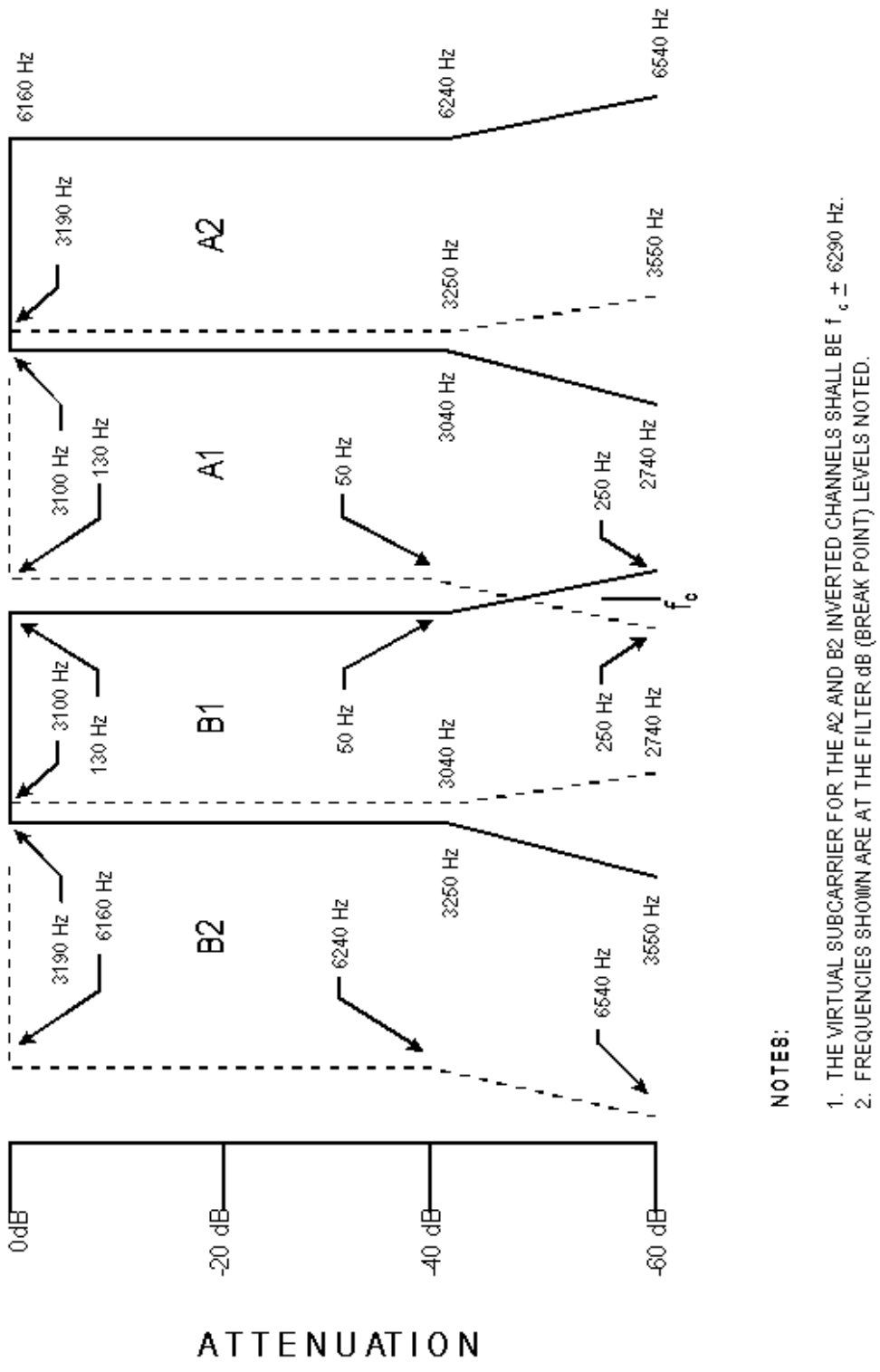


FIGURE 5. Overall channel characteristics (four-channel equipment).

5.2.8 Channel Delay
Measurements shall be performed from audio input to RF output (for transmitters) and from RF input to audio output (for receivers).

5.2.8.1 Absolute delay.
The absolute delay shall not exceed 5 ms (DO: 2.5 ms) over the frequency range of 300 Hz to 3050 Hz.

5.2.8.2 Group Delay
In each channel of single-channel and 2-ISB systems, over the following portion of the passband, group delay shall not vary by more than 500 microseconds, and group delay variation shall not exceed 150 microseconds for any 100-Hz frequency increment.

3 kHz channel: 575 to 2775 Hz
WBHF channel: 575 to (B – 225) Hz, where B = N x 3 kHz and N may be 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, or 16.

In each channel of 4-ISB systems,

- Group delay shall not exceed 750 microseconds over the ranges 370 Hz to 750 Hz and 3000 Hz to 3100 Hz.
- Group delay shall not exceed 500 microseconds over the range 750 Hz to 3000 Hz.
- Group delay variation shall not exceed 150 microseconds for any 100-Hz frequency increment between 570 Hz and 3000 Hz.

5.3 Transmitter characteristics.

5.3.1 Noise and distortion.

5.3.1.1 In-band noise.
Broadband noise in a 1-Hz bandwidth within the selected sideband shall be at least 65 decibels referenced to full-rated peak envelope power (dBc) below the level of the rated PEP of the HF transmitter for tactical application and 75 dBc below the level of the rated PEP of the HF transmitter for long-haul applications. See Appendix F for co-sited installations.

5.3.1.2 Intermodulation distortion (IMD).
The IMD products of HF transmitters produced by any two equal-level signals within the 3 dB bandwidth (a single-frequency audio output) shall be at least 24 dB (DO 30 dB) below either tone for tactical applications and 30 dB (DO 40 dB) below either tone for long-haul applications when the transmitter is operating at rated PEP. The frequencies of the two audio test signals shall not be harmonically related and shall have a minimum separation of 300 Hz.

NOTE: For high-data-rate applications (greater than 2400 bps), transmitter linearity should be 36 to 40 dB. This exceeds the requirement and DO for tactical applications above, and exceeds the requirement and approaches the DO for long-haul applications.

5.3.2 Spectral purity.

5.3.2.1 Broadband emissions.
When the transmitter is driven to rated PEP with a single tone in the center of the necessary bandwidth, the power spectral density of the transmitter broadband emission shall not exceed the level established in Table II and as shown in Figures 6 and 7. Discrete spurs shall be excluded from the measurement, and the measurement bandwidth shall be 1 Hz. In cases where the necessary bandwidth causes a conflict with limits based on percentage offset from f_c, the less stringent limit shall apply.

TABLE II. Broadband emissions power spectral density limits for radio transmitters.

Measurement Frequency (Hz)	Power Spectral Density Limit (dBc/Hz)	
	Tactical Transmitter	Long-haul* Transmitters
$f_m = f_c \pm (0.5\ B + 500)$	–65	–75
$f_m = f_c \pm 1.0\ B$	–70	–80
$f_m = f_c \pm 2.5\ B$	–85	–95
$(f_c + 4.0\ B) \leq f_m < 1.05\ f_c$ $0.95\ f_c < f_m \leq (f_c - 4.0\ B)$	–95	–105
$f_m \leq 0.95\ f_c$ $f_m \geq 1.05\ f_c$	–125	–125 (DO –140)
Where f_m = frequency of measurement (Hz) f_c = center frequency of bandwidth (Hz) B = necessary bandwidth (Hz)		

* See Appendix F for special requirements for co-sited installations.

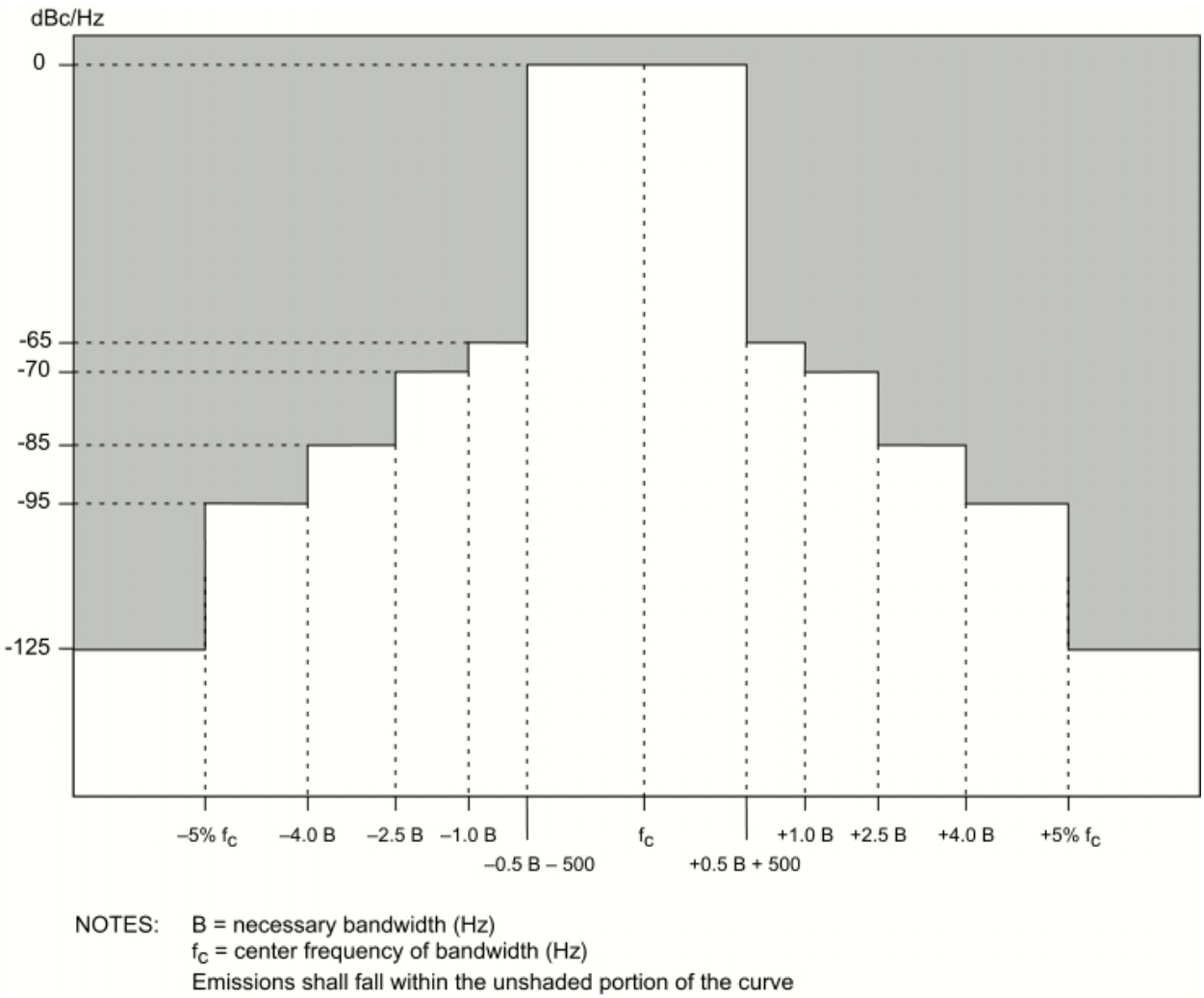
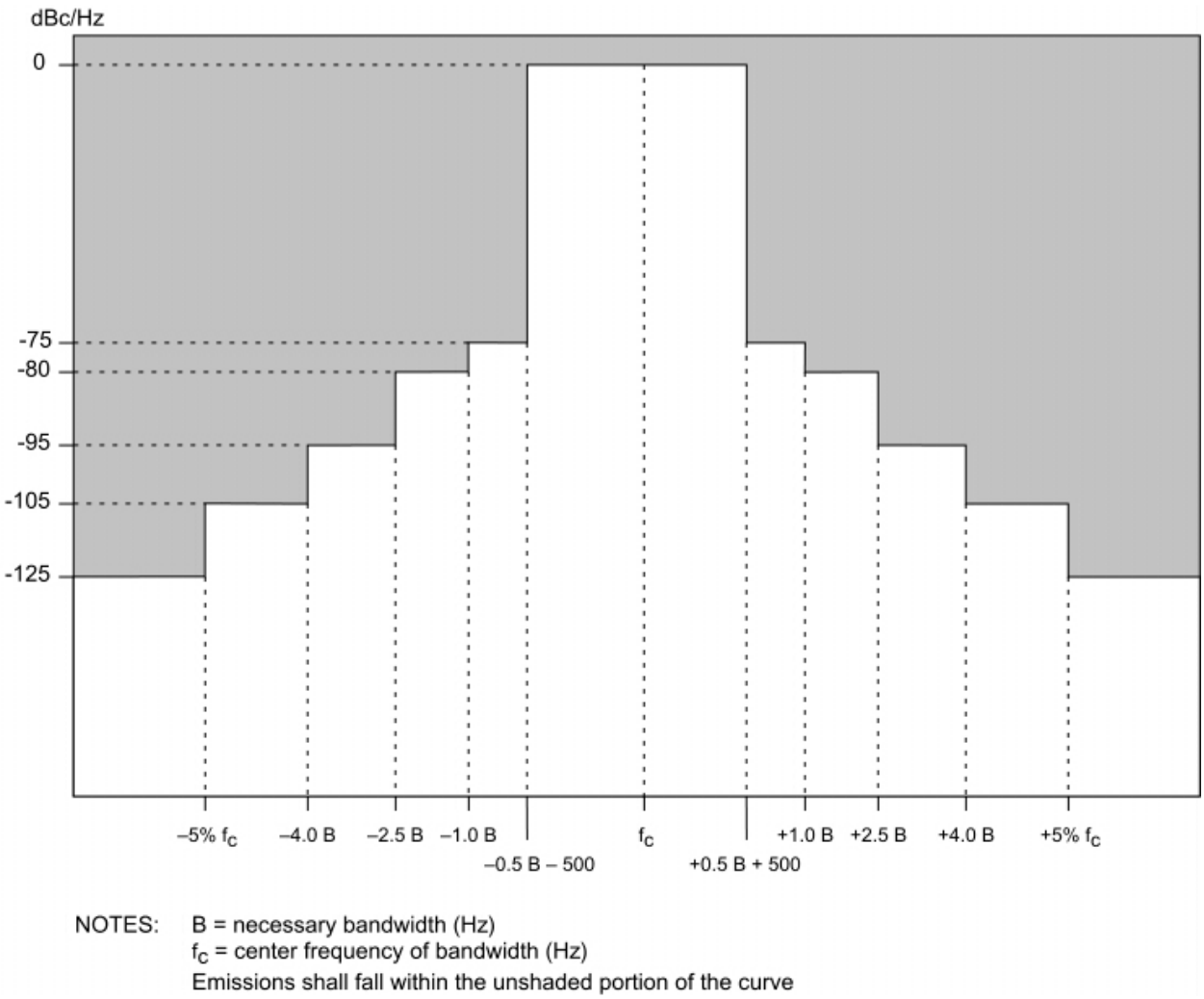


FIGURE 6. Broadband emissions power spectral density for tactical HF transmitters.



NOTES: B = necessary bandwidth (Hz)
f_c = center frequency of bandwidth (Hz)
Emissions shall fall within the unshaded portion of the curve

FIGURE 7. Broadband emissions power spectral density for long-haul HF transmitters.

5.3.2.2 Discrete frequency spurious emissions.
For HF transmitters, when driven with a single tone to produce an RF output of 25 percent rated PEP, all discrete frequency spurious (non-harmonic) emissions shall be suppressed as follows:

a. For tactical applications (see Figure 8)
   - Between the carrier frequency f_c and $f_c \pm 4B$ (where B = bandwidth), at least 40 dBc.
   - Beyond $f_c \pm 4B$ at least 50 dBc.

b. See Appendix F for shipboard applications.

c. For long-haul applications (see Figure 9)
   - Between the carrier frequency fc and fc $\pm$ 4B (where B = bandwidth), at least 40 dBc.
   - Between fc $\pm$ 4B and $\pm$ 5 percent of fc removed from the carrier frequency, at least 60 dBc.
   - Beyond $\pm$5 percent removed from the carrier frequency, at least 80 dBc.

5.3.2.3. Discrete frequency harmonic emissions.
For HF transmitters, when driven with a single tone to produce an RF output of 25 percent rated PEP, all discrete frequency harmonic emissions shall be suppressed as follows:

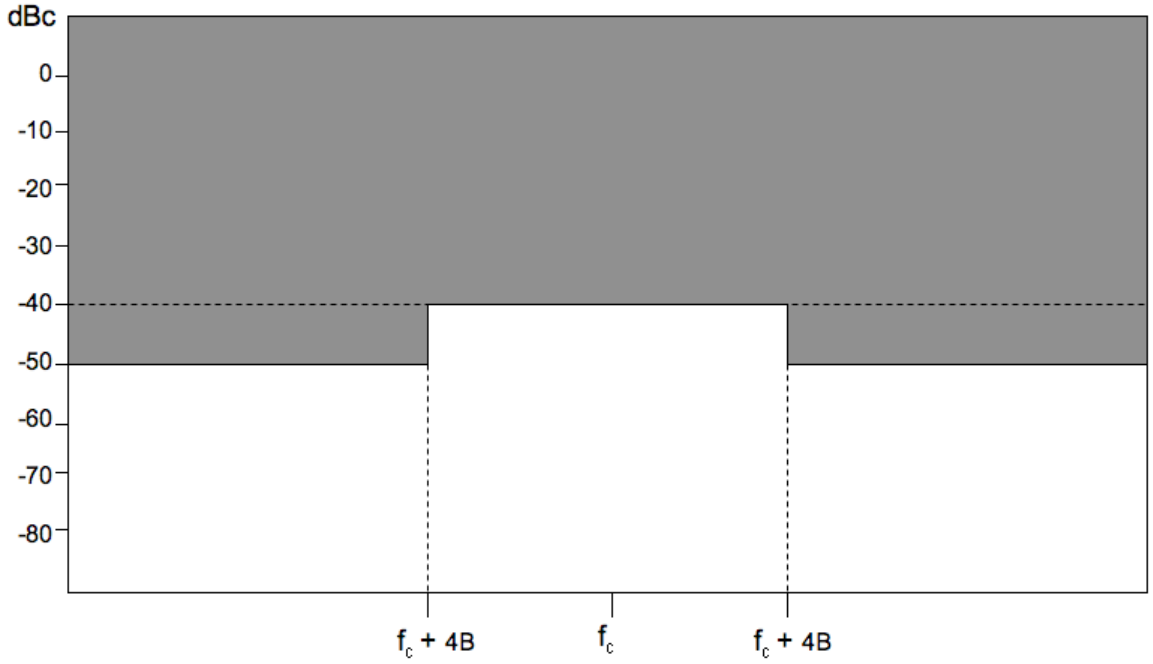
a. For tactical applications, harmonic emission levels shall not exceed -40 dBc.

b. See Appendix F for shipboard applications.

c. For long-haul applications, harmonic emissions shall be attenuated below Px (the rated PEP) by [40 + 10log(Px in watts)] or 80 dB, whichever is the lesser attenuation.

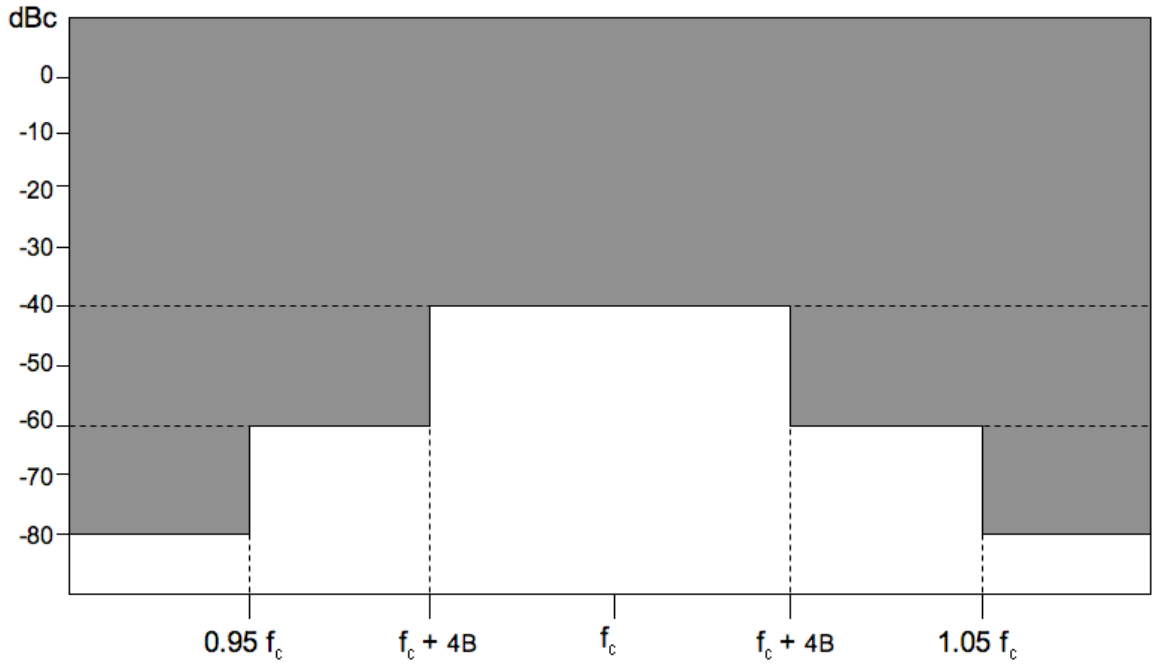
5.3.3 Carrier suppression.
The suppressed carrier for tactical applications shall be at least 40 dBc (DO: 60 dBc) below the output level of a single tone modulating the transmitter to rated PEP. The suppressed carrier for long-haul applications shall be at least 50 dBc (DO: 60 dBc) below the output level of a single tone modulating the transmitter to rated PEP.

5.3.4 Automatic level control (ALC).
Starting at ALC threshold, an increase of 20 dB in a single-tone audio input shall result in less than a 1 dB increase in average RF power output.



Notes:
1. Emissions shall fall within the unshaded portion of the graph.
2. Harmonic emissions for tactical transmitters shall not exceed -40 dBc

FIGURE 8. Discrete frequency spurious emissions limit for tactical HF transmitters.



Notes:
1. Emissions shall fall within the unshaded portion of the graph.
2. Harmonic emissions for long-haul transmitters shall not exceed -63 dBc

FIGURE 9. Discrete frequency spurious emissions limit for long-haul HF transmitters.

5.3.5 Attack and release time delays.

5.3.5.1 Attack-time delay.
The time interval from keying-on a transmitter until the transmitted RF signal amplitude has increased to 90 percent of its steady-state value shall not exceed 25 ms (DO: 10 ms). This delay excludes any necessary time for automatic antenna tuning.

5.3.5.2 Release-time delay.
The time interval from keying-off a transmitter until the transmitted RF signal amplitude has decreased to 10 percent of its key-on steady-state value shall be 10 ms or less.

5.3.6 Signal input interface characteristics.

5.3.6.1 Input signal power.
Input signal power for microphone or handset input is not standardized. When a line-level input is provided (see paragraph 5.3.6.2), rated transmitter PEP shall be obtainable for single tone amplitudes from -17 dBm to +6 dBm (manual adjustment permitted).

5.3.6.2 Input audio signal interface.

5.3.6.2.1 Unbalanced interface.
When an unbalanced interface is provided, it shall have an audio input impedance of a nominal 150 ohms, unbalanced with respect to ground,.

5.3.6.2.2 Balanced interface.
When a balanced interface is provided, the audio input impedance shall be a nominal 600 ohms, balanced with respect to ground.

5.3.7 Transmitter output load impedance.
The nominal RF output load impedance of the transmitter shall be 50 ohms, unbalanced with respect to ground. Transmitters shall survive any voltage standing wave ratio (VSWR) at the output, while derating the output power as a function of increasing VSWR. However, the transmitter shall deliver full rated forward power into a 1.3:1 VSWR load.

Figure 10 shows the design objective for the maximum derating in the presence of high VSWR.

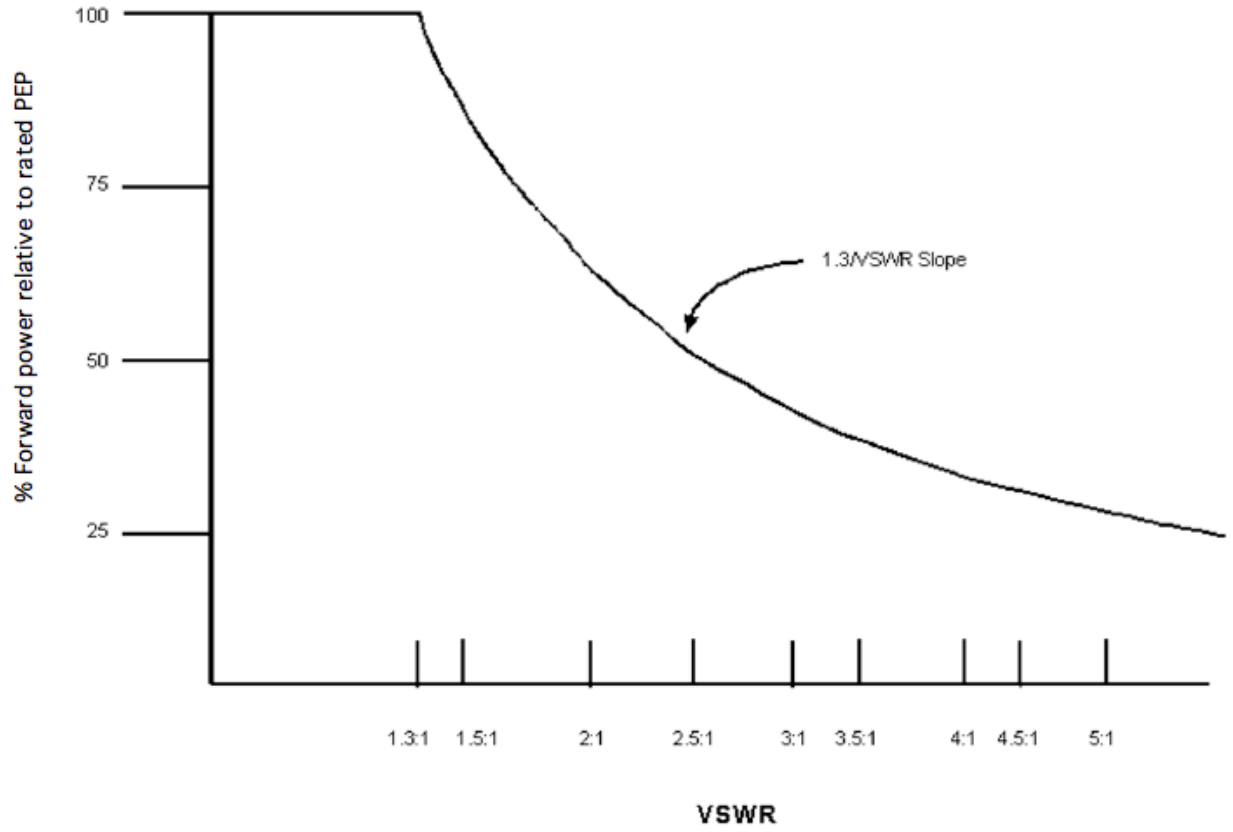


FIGURE 10. <u>Output power vs. VSWR for transmitters with broadband output impedance networks</u>.

NOTE: The full-rated output power of a transmitter over the operating frequency range is defined to be (a) the rated PEP when the transmitter is driven by a two-tone signal consisting of equal amplitude tones, and (b) the rated average power when driven by a single tone. The output rating shall be determined with the transmitter operating into a 50-ohm load.

5.4 Receiver characteristics.

5.4.1 Receiver RF characteristics.
All receiver input amplitudes are in terms of available power in dBm from a 50-ohm source impedance signal generator.

5.4.1.1 Image rejection.
The rejection of image signals shall be at least 70 dB for tactical HF receivers and 80 dB for long-haul HF receivers (DO: 100 dB).

5.4.1.2 Intermediate frequency (IF) rejection.
The rejection of signals at the IF (frequencies) shall be at least 70 dB for tactical HF receivers and 80 dB for long-haul HF receivers (DO: 100 dB).

5.4.1.3 Adjacent-channel rejection.
With AGC active, the receiver shall reject any signal in the undesired sideband and adjacent channel in accordance with Figure 3 or 4 as appropriate for 3 kHz or wider channels, respectively.

5.4.1.4 Other signal-frequency external spurious responses.
Receiver rejection of spurious frequencies, other than IF and image, shall be at least 65 dB (55 dB for tactical application) for frequencies from +2.5 percent to +30 percent, and from -2.5 percent to -30 percent of the center frequency, and at least 80 dB (70 dB for tactical application) for frequencies beyond $\pm$30 percent of the center frequency.

5.4.1.5 Receiver protection.
The receiver, with primary power on or off, shall be capable of survival without damage with applied signals of up to +43 dBm (DO: +53 dBm) available power delivered from a 50-ohm source for a duration of 5 minutes (1 minute for tactical applications).

5.4.1.6 Desensitization dynamic range.
The following requirement shall apply to the receiver in an SSB mode of operation with an IF passband setting providing at least 2750 Hz (nominal 3 kHz bandwidth) at the 2 dB points. With the receiver tuning centered on a sinusoidal input test signal and with the test signal level adjusted to produce an output SINAD of 10 dB, a single interfering sinusoidal signal, offset from the test signal by an amount equal to $\pm$5 percent of the carrier frequency, is injected into the receiver input. The output SINAD shall not be degraded by more than 1 dB as follows:

a. For tactical radios, the interfering signal is equal to or less than 90 dB above the test signal level.

b. See Appendix F for co-sited applications

c. For long-haul radios, the interfering signal is equal to or less than 100 dB above the test signal level.

5.4.1.7 Receiver sensitivity.
The sensitivity of the receiver over the operating frequency range, in the sideband mode of operation (3-kHz bandwidth), shall be such that a -111 dBm (DO: -121 dBm) unmodulated signal at the antenna terminal, adjusted for a 1000 Hz audio output, produces an audio output with a SINAD of at least 10 dB over the operating frequency range.

5.4.1.8 Receiver out-of-band IMD.
Second-order and higher-order responses shall require a two-tone signal amplitude with each tone at -30 dBm or greater (-36 dBm or greater for tactical applications), to produce an output SINAD equivalent to a single -110 dBm tone. This requirement is applicable for equal-amplitude input signals with the closest signal spaced 30 kHz or more from the operating frequency.

5.4.2 Receiver distortion and internally generated spurious outputs.

5.4.2.1 Overall IMD (in-channel).
The total of IMD products, with two equal-amplitude, in-channel tones spaced 110 Hz apart, present at the receiver RF input, shall meet the following requirements. The requirements shall be met for any RF input amplitude up to 0 dBm PEP (-6 dBm/tone) at rated audio output. All IMD products shall be at least 35 dB (DO: 45 dB) below the output level of either of the two tones.

5.4.2.2 Adjacent-channel IMD.
For multiple-channel equipment, the overall adjacent-channel IMD in each 3 kHz channel being measured shall not be greater than -35 dBm at the 3 kHz channel output with all other channels equally loaded with 0 dBm unweighted white noise.

5.4.2.3 Audio frequency total harmonic distortion.
The total harmonic distortion produced by any single-frequency RF test signal, which produces a frequency within the frequency bandwidth of 300 Hz to 3050 Hz shall be at least 25 dB (DO: 35 dB) below the reference tone level with the receiver at rated output level. The RF test signal shall be at least 35 dB above the receiver noise threshold.

5.4.2.4 Internally generated spurious outputs.
For 99 percent of the available 3 kHz channels, internally generated spurious signals shall not exceed -112 dBm. For 0.8 percent of the available 3 kHz channels, spurious signals may exceed –112 dBm but shall not exceed -100 dBm for tactical applications and -106 dBm for long-haul applications. For 0.2 percent of the available 3 kHz channels, spurious signals may exceed these levels.

5.4.3 Automatic gain control (AGC) characteristic.
The steady-state output level of the receiver (for a single tone) shall not vary by more than 3 dB over an RF input range from -103 dBm to +13 dBm (-103 dBm to 0 dBm for tactical application).

5.4.3.1 AGC attack time (nondata modes).
The receiver AGC attack time from the initial application of a -57 dBm RF signal until audio output reaches steady state shall not exceed 30 ms.

5.4.3.2 AGC release time (nondata modes).
The receiver AGC release time shall be between 800 and 1200 ms for SSB voice and ICW operation. This shall be the period from RF signal downward transition until audio output is within 3 dB of the steady-state output. The final steady-state audio output is simply receiver noise being amplified in the absence of any RF input signal.

5.4.3.3 AGC requirements for data service.
In data service, the receiver AGC attack time shall not exceed 10 ms. The AGC release time shall not exceed 25 ms.

5.4.4 Receiver linearity.
The following shall apply with the receiver operating at maximum sensitivity, and with a reference input signal that produces a SINAD of 10 dB at the receiver output. The output SINAD shall increase monotonically and linearly within $\pm$ 1.5 dB for a linear increase in input signal level until the output SINAD is equal to at least 30 dB (DO: 40 dB). When saturation occurs, the output SINAD may vary $\pm$3 dB for additional increase in signal level. This requirement shall apply over the operating frequency range of the receiver.

5.4.5 Interface characteristics.

5.4.5.1 Input impedance.
The receiver RF input impedance shall be nominally 50 ohms, unbalanced with respect to ground. The input VSWR, with respect to 50 ohms, shall not exceed 2.5:1 over the operating frequency range.

5.4.5.2 Output impedance and power.
When a balanced output is provided, the receiver output impedance shall be a nominal 600 ohms, balanced with respect to ground, capable of delivering 0 dBm to a 600-ohm load. Electrical symmetry shall be sufficient to suppress longitudinal currents at least 40 dB below reference signal level. The receiver output signal power for operation with a headset or handset shall be adjustable at least over the range from -30 dBm to 0 dBm. For operation with a speaker, the output level shall be adjustable at least over the range of 0 dBm to +30 dBm. As a DO, an additional interface can accommodate speakers ranging from 4 to 16 ohms impedance should be provided.

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

6.1 Intended use.
This standard contains requirements to ensure interoperability of new radio equipment with long-haul and tactical application in the MF and HF bands. Appendix F contains additional special requirements for applications in which more than one such radio is installed on a single mobile

platform or fixed location (co-site installations). Table III offers guidance in applying these sets of requirements to various applications.

TABLE III. Application guidance for radio specifications.

Application	Tactical	Long-haul	Co-site	Co-site Shipboard
Manpack	X			
Ground Vehicle	X			
Aircraft (one MF/HF radio)		X		
Aircraft (multiple MF/HF radios)			X	
Ship (one MF/HF radio)		X		
Ship (multiple MF/HF radios)				X
Fixed site (one MF/HF radio)		X		
Fixed site (multiple MF/HF radios)			X	

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. Options AL-1 and AL-2 provide an inexpensive, least protected mode, and AL-3 provides a more sophisticated protection mode. The users should establish their application level based on minimum essential requirements.

There is no requirement for the user to acquire any of the advanced technology defined in the appendices to this document unless the user has an identified requirement.

6.2 Subject term (key word) listing.

Adaptive communications
AJ mode
ALE
ALE control functions
ALE message protocol
ALE mode
Automatic sounding
Baseline mode
Deep interleaving
Forward error correction
Golay coding
Leading redundant word
Linking protection
LQA
Network functions
Network management

Protection interval
Radio frequency scanning
Selective calling
Slotted responses
Star net and group
Triple redundant words
Word phase

6.3 International standardization agreements.
Certain provisions of this standard in paragraphs 4.2, 4.4, 5.2, 5.3, and 5.4 are the subject of international standardization agreements, STANAGs 4203, 4539, and 5035, and QSTG 733. When change notice, revision, or cancellation of this standard is proposed that will modify the international agreement concerned, the preparing activity will take appropriate action through international standardization channels, including departmental standardization offices, to change the agreement or make other appropriate accommodations.

6.4 Electromagnetic compatibility (EMC) requirements.
All services and agencies are responsible for their own EMC programs, which are driven by their user requirements and doctrine.

HF radio has significant inherent EMC implications that require serious consideration by designers, users, and acquisition personnel. It is strongly recommended that all users of this standard refer to the following documents prior to design or acquisition of HF radio systems or equipment:

a. MIL-STD-461, Requirements for the Control of Electromagnetic Interface Emissions and Susceptibility.

b. MIL-STD-462, Measurement of Electromagnetic Interference Characteristics.

c. MIL-HDBK-237, Electromagnetic Compatibility Management Guide for Platform, Systems and Equipment.

The applicable portions of these documents should be included in any acquisition actions for HF radio systems or equipment.

6.6 Change notations.
The margins of this standard are marked with vertical lines to indicate changes from the previous edition (except that Appendices G and H are entirely new and are not so marked). This was done as a convenience only and the Government assumes no liability whatsoever for any inaccuracies in these notations. Bidders and contractors are cautioned to evaluate the requirements of this document based on the entire content irrespective of the marginal notations.

APPENDIX A

AUTOMATIC LINK ESTABLISHMENT SYSTEM

(SECOND GENERATION (2G))

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

TABLES

TABLES (Continued)

FIGURES

FIGURE **PAGE**

FIGURES (Continued)

ANNEXES

AUTOMATIC LINK ESTABLISHMENT SYSTEM

A.1 GENERAL.

A.1.1 Scope.

This appendix provides details of the prescribed waveform, signal structures, protocols, and performance requirements for the second generation (2G) automatic link establishment (ALE) system.

A.1.2 Applicability.

This appendix is a mandatory part of MIL-STD-188-141 whenever ALE is a requirement to be implemented into the high frequency (HF) radio system. The functional capability described herein includes automatic signaling, selective calling, automatic answering, and radio frequency (rf) scanning with link quality analysis (LQA). The capability for manual operation of the radio in order to conduct communications with existing, older generation, non-automated manual radios, shall not be impaired by implementation of these automated features.

A.2 APPLICABLE DOCUMENTS.

A.2.1 General.

The documents listed in this section are specified in A.3, A.4, and A.5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in A.3, A.4, and A.5 of this standard, whether or not they are listed.

A.2.2 Government documents.

A.2.2.1 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 cited in the solicitation or contract.

INTERNATIONAL STANDARDIZATION AGREEMENTS

STANAG 4285	Characteristics of 1200/2400/3600 bps Single Tone Modems for HF Radio Links
STANAG 4529	Characteristics of Single Tone Modulators/Demodulators for Maritime HF Radio Links with 1240 Hz Bandwidth

FEDERAL STANDARDS

FED-STD-1037	Telecommunications: Glossary of Telecommunications Terms

DEPARTMENT OF DEFENSE STANDARDS

MIL-STD-188-110	Interoperability and Performance Standards for Data Modems

(Copies of these documents are available online at http://quicksearch.dla.mil.)

A.3 DEFINITIONS.

A.3.1 Terms.

Definitions of terms used in this document shall be as specified in the current edition of FED-STD-1037 except where inconsistent with the use in this standard. In addition, the following definitions are applicable for the purpose of this standard.

- Available State. An ALE controller is in the available state when it does not currently have a link with any other station, and is not in the process of establishing a link. An ALE controller that is programmed for multichannel scanning operation will be scanning when it is in the available state. Single-channel controllers will remain tuned to the assigned channel regardless of their state.
- Exclusive OR.. Used as a check, the condition that exits 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.
- Linking State. An ALE controller enters the linking state from the available state when it sends or receives an ALE call frame. Scanning controllers stop scanning when they enter the linking state. An ALE controller returns to the available state if the linking attempt does not complete successfully. Upon successful completion of a three-way handshake, controllers in the linking state enter the linked state.
- Linked State. An ALE controller is considered to be in the linked state if it has successfully completed link establishment with one or more stations, and at least one link to which it is party has not been terminated. While in the linked state, a wait-for-activity timer will be running (if not disabled by the operator). Controllers programmed to scan will not be scanning while in the linked state. After link establishment, communication among linked stations normally is carried by additional three-way handshakes, but controllers remain in the linked state during these handshakes.

A.3.2 Abbreviations and acronyms.

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

2G ALE	second generation automatic link establishment
3G ALE	secondthird generation automatic link establishment
ACK	acknowledge character
AGC	automatic gain control
ALE	automatic link establishment
AMD	automatic message display
AQC	Alternative Quick Call
AQC-ALE	Alternative Quick Call Automatic Link Establishment
ARQ	automatic repeat request
ASCII	American Standard Code for Information Interchange
AWGN	Additive white gaussian noise
b/s	bits per second
BCD	binary coded decimal
BER	bit error ratio
CCIR	International Radio Consultative Committee
chps	channels per second
CMD	ALE preamble word COMMAND
CRC	cyclic redundancy check
dB	Decibel
DBM	data block message
dBw	dB referred to 1 W (watt)
DC	data code
DCE	data circuit-terminating equipment
DO	design objective
DoD	Department of Defense
DTE	data terminal equipment
DTM	data text message
e.g.	for example
FCS	frame check sequence
FEC	forward error correction
FSK	frequency shift keying
HF	high frequency
HFNC	high frequency node controller
Hz	hertz
ID	identification
IFF	if and only if
ISDN	Integrated Services Digital Network
ISO	International Organization of Standardization
ITU	International Telecommunications Union
kHz	Kilohertz

LP	linking protection
LQA	link quality analysis
LSB	(1) lower sideband (2) least significant bit
MF	medium frequency
MHz	megahertz
MP	multipath
ms	millisecond
MSB	most significant bit
NAK	negative-acknowledge character
NATO	North Atlantic Treaty Organization
NT	Not Tested
PL	probability of linking
PPM	parts per million
REP	ALE preamble word REPEAT
rf	radio frequency
RX	receive
s	second
SCTY	Security
SINAD	signal-plus-noise-plus-distortion to noise-plus-distortion ratio
SN	Slot Number
SNR	signal to noise ratio
SPS	symbols per second
SSB	single-sideband [transmission]
TDMA	time-division multiple access
TIS	ALE preamble word THIS IS
TOD	time of day
TWAS	ALE preamble word THIS WAS
TX	transmit
UI	unique index
USB	upper sideband
UUF	user unique function
UUT	units under test
WRTT	wait for response and tune timeout
WS	AQC-ALE Word Sync word

A.3.3 Definitions of timing symbols.
The abbreviations and acronyms used for timing symbols are contained in annex A to this appendix.

A.4 GENERAL REQUIREMENTS.

A.4.1 ALE introduction.

The techniques specified in this appendix employ a robust modem and forward error correction coding and constitutes a digital ALE data link. The exchange of such ALE words according to the specified protocols supports channel evaluation, selective calling, and passing data messages and constitutes an ALE data link layer. (The ALE modem, radio, coupler, antenna, and so on constitute the corresponding physical layer.)

The ALE data link layer contains three sublayers, as shown in figure A-1: a lower sublayer concerned with error correction and detection (forward error correction [FEC] sublayer), an upper sublayer containing the ALE protocol (ALE sublayer), and a linking protection (LP) sublayer between. 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 Seven Layer Reference Model. The ALE sublayer specifies protocols for link establishment, data communication, and rudimentary LQA based on the capability of exchanging ALE words. The shaded area of figure A-1 indicates the contents of this appendix.

The following paragraphs specify the general requirements for ALE operation.

A.4.1.1 ALE addresses.

Stations designed to this appendix shall employ the addressing structure specified in A.5.2.4 to identify individual stations and collections of stations (nets and groups).

A.4.1.2 Scanning.

The radio system shall be capable of repeatedly scanning selected channels stored in memory (in the radio or controller) under either manual control or under the direction of any associated automated controller. The radio shall stop scanning and wait on the most recent channel upon the occurrence of any of the following selectable events:

- Automatic controller decision to stop scan (the normal mode of operation)
- Manual input of stop scan
- Activation of external stop-scan line (if provided)

The scanned channels should be selectable by groups (often called “scan lists”) and also individually within the groups, to enable flexibility in channel and network scan management.

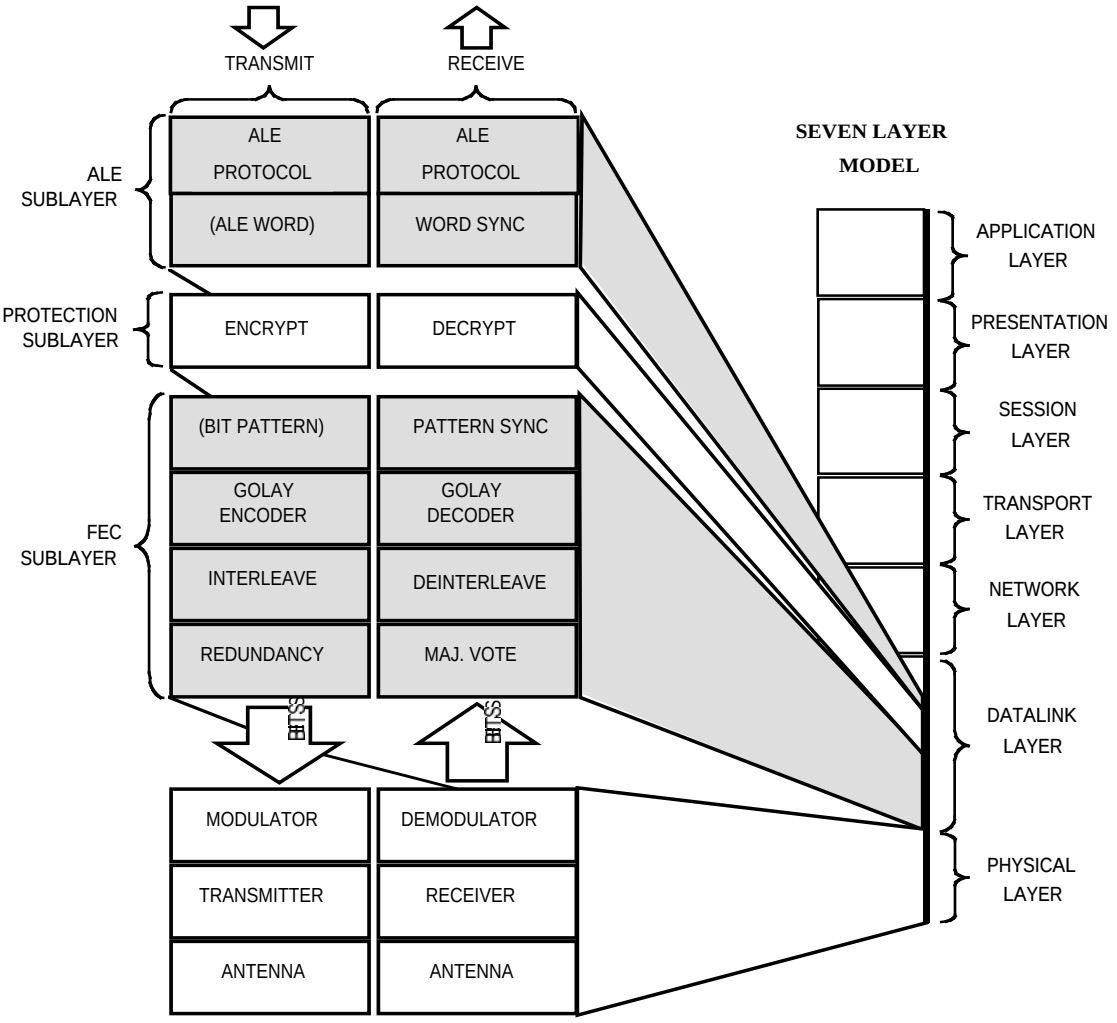


FIGURE A-1. Data link with ALE and FEC sublayers.

A.4.1.3 Calling.
Upon request by the operator or an external automated controller, the radio system shall execute the appropriate calling protocol specified in A.5.5. The operator or external controller shall be able to override automatic channel selection by specifying a channel for the call.

A.4.1.4 Channel evaluation.
The radio system shall be capable of automatically transmitting ALE sounding transmissions in accordance with A.5.3, and shall automatically measure the signal quality of ALE receptions in accordance with A.5.4.1.

.4.1.5 Channel quality display.
If an operator display is provided, the display shall have a uniform scale, 0-30 with 31 being un-known all based on signal-plus-noise-plus-distortion to noise-plus-distortion (SINAD).

A.4.2 System performance requirements.
Stations designed to this appendix shall demonstrate an overall system performance equal to or exceeding the following requirements.

A.4.2.1 Scanning rate.
Stations designed to this appendix shall incorporate selectable scan rates of two and five channels per second, and may also incorporate other scan rates (design objective (DO): 10 channels per second).

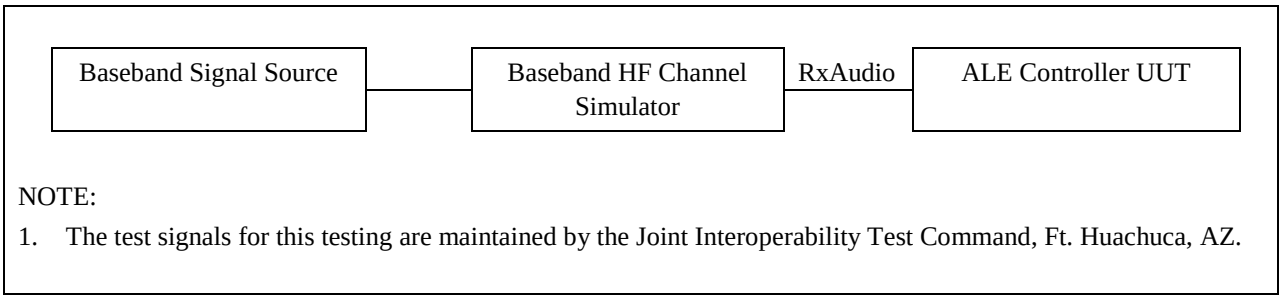
A.4.2.1.1 Alternative Quick Call (AQC) .
In the optional AQC-ALE protocol, the system shall be capable of variable dwell rates while scanning such that traffic can be detected in accordance with table A-II Probability of Linking.

A.4.2.1.2 Recommendation.
Radios equipped with the optional AQC-ALE shall provide scanning at scan rates of two channels per second or five channels per second for backward compatibility to non-AQC-ALE networks.

A.4.2.2 Occupancy detection.
Stations designed to this appendix shall achieve at least the following probability of detecting the specified waveforms (See A.5.4.7) under the indicated conditions, with false alarm rates of no more than 1 percent. The channel simulator shall provide additive white gaussian noise (AWGN) without fading or multipath (MP). See table A-I.

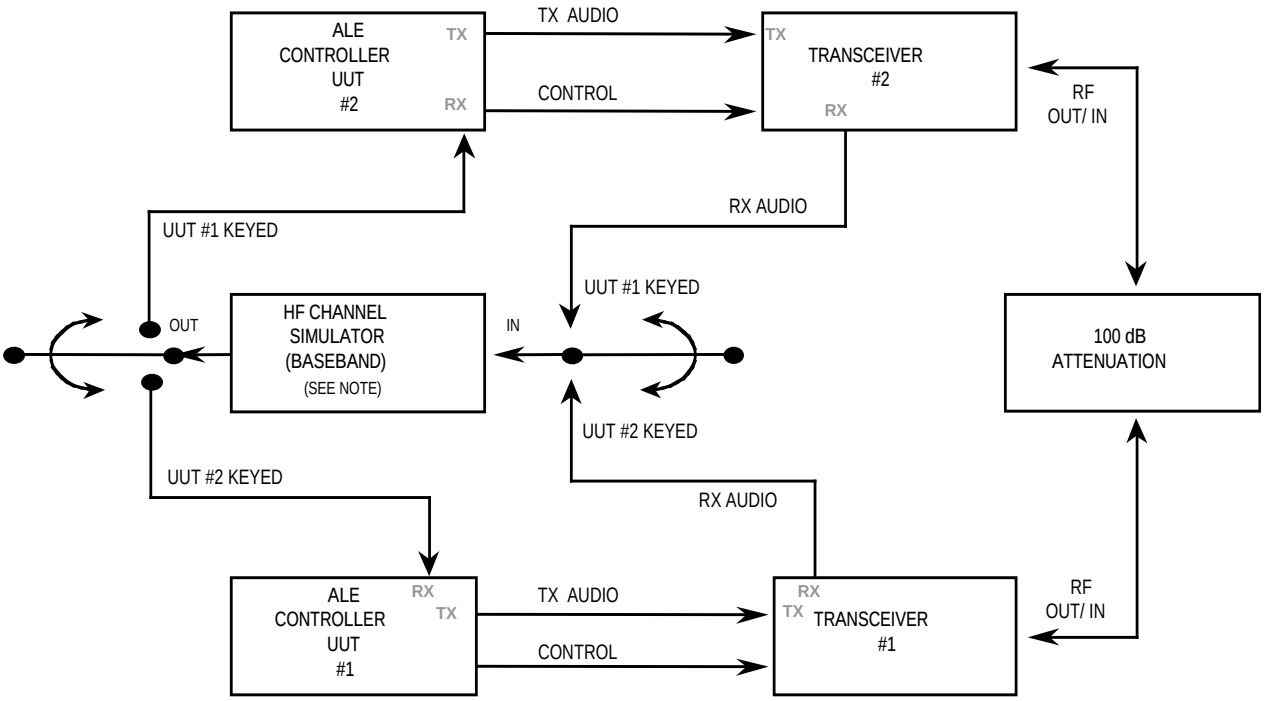
TABLE A-I. Occupancy detection probability (2G and 3G).

Waveform	SNR (dB in 3 kHz)	Dwell Time (s)	Detection Prob
ALE	0	2.0	0.80
	6	2.0	0.99
SSB Voice	6	2.0	0.80
	9	2.0	0.99
MIL-STD-188-110	0	2.0	0.80
(Serial Tone PSK)	6	2.0	0.99
STANAG 4529	0	2.0	0.80
	6	2.0	0.99
STANAG 4285	0	2.0	0.80
	6	2.0	0.99



NOTE:
1. The test signals for this testing are maintained by the Joint Interoperability Test Command, Ft. Huachuca, AZ.

FIGURE A-2. Occupancy detection test setup.



NOTE: THE SIMULATOR INCLUDES EITHER INTERNAL OR EXTERNAL CAPABILITY TO ADJUST/MONITOR SIGNAL/NOISE/DOPPLER-OFFSET SETTINGS AND SHALL INCORPORATE APPROPRIATE FILTERING TO LIMIT THE AUDIO PASSBAND TO 300 - 3050 Hz.

FIGURE A-3. System performance measurements test setup.

A.4.2.3 Linking probability.
Linking attempts made with a test setup configured as shown in figure A-3, using the specified ALE signal created in accordance with this appendix, shall produce a probability of linking as shown in table A-II.

TABLE A-II. Probability of linking.

	Signal-to-noise ratio (dB in 3 kHz)		
Probability of Linking (Pl)	Gaussian Noise Channel	Modified CCIR Good Channel	Modified CCIR Poor Channel
≥ 25%	-2.5	+0.5	+1.0
≥ 50%	-1.5	+2.5	+3.0
≥ 85%	-0.5	+5.5	+6.0
≥ 95%	0.0	+8.5	+11.0
Multipath (millisecond)	0.0	0.52	2.2
Doppler spread (Hertz)	0.0	0.10	1.0

The receive audio input to the ALE controller shall be used to simulate the three channel conditions. The modified International Radio Consultative Committee (CCIR) good channel shall be characterized as having 0.52 millisecond (ms) (modified from 0.50ms) MP delay and a fading (two sigma) bandwidth of 0.1 hertz (Hz). The modified CCIR poor channel, normally characterized as consisting of a circuit having 2.0 ms MP delay with a fading (two sigma) bandwidth of 1.0 Hz, shall be modified to have 2.2 ms MP delay and a fading (two sigma) bandwidth of 1.0 Hz. Doppler shifts of ±60 Hz shall produce no more than a 1.0 decibel (dB) performance degradation from the requirements of table A-II for the modified CCIR good and poor channels.

NOTE: This modification is necessary due to the fact that the constant 2-ms MP delay (an unrealistic fixed condition) of the CCIR poor channel results in a constant nulling of certain tones of the ALE tone library. Other tone libraries would also have some particular MP value, which would result in continuous tone cancellation during simulator testing.

Each of the signal-to-noise (SNR) ratio values shall be measured in a nominal 3-kiloHertz (kHz) bandwidth. Performance tests of this capability shall be conducted in accordance with MIL-STD-188-110 Appendix E “Characteristics of HF Channel Simulators.” This test shall use the individual scanning calling protocol described in A.5.5.3. The time for performance of each link attempt shall be measured from the initiation of the calling transmission until the successful establishment of the link. Performance testing shall include the following additional criteria:

a. The protocol used shall be the individual scanning calling protocol with only TO and TIS preambles.

b. Addresses used shall be alphanumeric, one word (three characters) in length from the 38-character basic American Standard Code for Information Interchange (ASCII) subset.

c. Units under test (UUTs) shall be scanning 10 channels at two channels per second, and repeated at five channels per seconds.

d. Call initiation shall be performed with the UUT transmitter stopped and tuned to the calling frequency.

e. Maximum time from call initiation (measured from the start of UUT rf transmission -- not from activation of the ALE protocol) to link establishment shall not exceed 14.000 seconds, plus simulator delay time. The call shall not exceed 23 redundent words, the response three redundent words and the acknowledgment three redundent words. (See A.5.2.2.4 and Annex A).

NOTE: Performance at the higher scan rates shall also meet the foregoing requirements and shall meet or exceed the probability of linking as shown in table A-II.

A.4.2.3.1 AQC-ALE linking probability.
When the optional AQC-ALE protocol (see details in Section A.5.8) is implemented, the probability of linking shall conform to table A-II with the following additional criteria:

a. The protocol used shall be quick AQC individual calling protocol with no message passing.

b. Addresses shall be one to six characters in the 38-character basic ASCII subset.

c. Units being called shall be scanning 10 channels.

d. Call initiation shall be performed with the UUT transmitter stopped and tuned to the calling frequency.

e. The initial call probe shall not exceed 10 T_{rw}, the call response shall not exceed $4T_{rw}$, and the acknowledgment shall not exceed 2 T_{rw}.

A.4.2.3.2 AQC-ALE linking performance.
AQC-ALE linking performance shall not be degraded in LP level 1 or 2. Scan rates of two or five channels per second may degrade performance because insufficient redundent words are emitted during the call probe.

A.4.3 Required data structures.

A.4.3.1 Channel memory.
The equipment shall be capable of storing, retrieving, and employing at least 100 different sets of information concerning channel data to include receive and transmit frequencies with associated mode information. See table A-III. The channel data storage shall be nonvolatile.

The mode information normally includes:

- transmit power level
- traffic or channel use (voice, data, etc.)

- sounding data
- modulation type (associated with frequency)
- transmit/receive modes
- filter width (DO)
- automatic gain control (AGC) setting (DO)
- input/output antenna port selection (DO)
- input/output information port selection (DO)
- noise blanker setting (DO)
- security (DO)
- sounding self address(es) SA....n(DO)

Any channel (a) shall be capable of being recalled manually or under the direction of any associated automated controller, and (b) shall be capable of having its information altered after recall without affecting the original stored information settings.

A.4.3.2 Self address memory.
The radio shall be capable of storing, retrieving, and employing at least 20 different sets of information concerning self addressing. The self-address information storage shall be nonvolatile.

These sets of information include self (its own personal) address(es), valid channels which are associated for use, and net addressing.

Net addressing information shall include (for each "net member" self address, as necessary) the net address and the associated slot wait time (in multiples of T_w). See table A-IV. (Slotted responses and related concepts are defined in A.5.5.4.1.) The slot wait time values are T_{swt}(slot number (SN)) from the formula, T_{swt} (SN) = T_{sw} x SN .

Stations called by their net call address shall respond with their associated self (net member) address with the specified delay (T_{swt}(SN)). For example, the call is "GUY," thus the response is "BEN."

Stations called individually by one of their self addresses (even if a net member address) shall respond immediately and with that address, as specified in the individual scanning calling protocol.

Stations called by one of their self addresses (even if a net member address) within a group call shall respond in the derived slot, and with that address, as specified in the star group scanning protocol. If a station is called by one of its net addresses and has no associated net member address, it shall pause and listen but shall not respond (unless subsequently called separately with an available self or net member address), but shall enter the linked state.

TABLE A-III. Channel memory example.

Channel	Frequency TX(MHz)	RX (MHz)	Mode TX	Mode RX	T/R	(2) SCAN	(2) SCTY	(3) Next Sound	Sound Interval	(2) SA	(1) AN	(1) PW	(1) US	Example Comments
C-1	17,777.7	17,777.7	USB	USB	T/R	Y	C	14 min	40 min	2	T 1	R LO	E V	Typical simplex channel, low power voice, clear
C-2	22,222.2	22,222.2	USB	USB	R	Y	C	--	--				V	Same, but receive
C-3	10,333.0	10,333.0	USB	LSB	T/R	Y	CS	1 min	60 min	2 2	1 2	LO HI	V	only at this time Half-duplex, uses another antenna, high power, clear
C-4	13,111.0	13,999.0	LSB	LSB	T/R	Y	CS	22 min	60 min	5	1	HI	V, D	and secure Typical voice or data, half-duplex, high power, clear
														and secure Typical, simplex, non-scan, data only,
C-5	9,900.0	9,900.0	USB	LSB	T/R	N	S	--	--	5	2	LO		secure
•	•	•	•	•	•	•	•	•	•	•	•	•	•	
C-100	0.0	5,000.0	--	AM	R	N	C	--	--	-	1	-	V, D	Receive only, non-scan, clear

NOTES:
1. Optional storage of antenna selection(s) "ANT"; power output "PWR"; and usage "USE".
2. Y-yes, N-no, C-clear, S-secure, V-voice, D-data, SA -Self address.
   "next sound" indicates time until next sounding on channel and is periodically decremented until "zero" value triggers sounding.
3. It is reset to "sound interval" value when a sound is sent.
4. Values shown for example only.

TABLE A-IV. Self address memory example.

Index	Self (or Net Member) Address	Net Address	T_{swt}(SN)= Slot Wait Time (T_w)	(4) Valid Channels	Example Comments
SA1	SAM	--	--	All	simple individual address, 1-word, all channels
SA2	BOBBIE	--	--	C1,2,3	simple individual address, 2-word, limited channels
SA3	JIM	--	--	C7	simple individual address, 1-word, single channel
SA4	BEN	GUY	14	All	net and individual addresses, 1-word, all channels, preset slot unit time (slot 1)
SA5	CLAUDETTE	GAL	80	C3-C7	net and 3-word individual addresses, limited channels, preset slot wait-time (slot 4)
SA6	JOE	PEOPLE	17	C1-C9	2-word net and 1-word individual addresses, limited channels preset slot wait-time
×	×	×	×	×	
×	×	×	×	×	
×	×	×	×	×	
SA20	--	PARTY	--	C5-C12	2-word net only address, therefore receive only if called

NOTES:
1. The self address number "SA#" index is included for clarity. Indexes may be useful for efficient memory management.
2. If a net address is associated with a self address, the self address should be referred to as a "net member" address.
3. Addresses and values shown for example only.
4. Valid channels are the channels on which this address is planned, or permitted, to be used.

A.4.3.3 Other station table.
The radio shall be capable of storing, retrieving, and employing at least 100 different sets of information concerning the addresses of other stations and nets, channel quality data to those stations and nets (measurements or predictions), and equipment settings specific to links with each station or net.

DO: any excess capacity which is not programmed with preplanned other station information should be automatically filled with any addresses heard on any of the scanned or monitored channels. When the excess capacity is filled, it should be kept current by replacing the oldest heard addresses with the latest ones heard. This information should be used for call initiation to stations (if needed), and for activity evaluation.

A.4.3.3.1 Other station address storage.
Individual station addresses shall be stored in distinct table entries, and shall be associated with a specific wait for reply time (T_{wr}) if not the default value. Net information shall include own net and net member associations, relative slot sequences, and own net wait for reply times (T_{wrn}) for use when calling. See figure A-4. The storage for addresses and settings shall be nonvolatile.

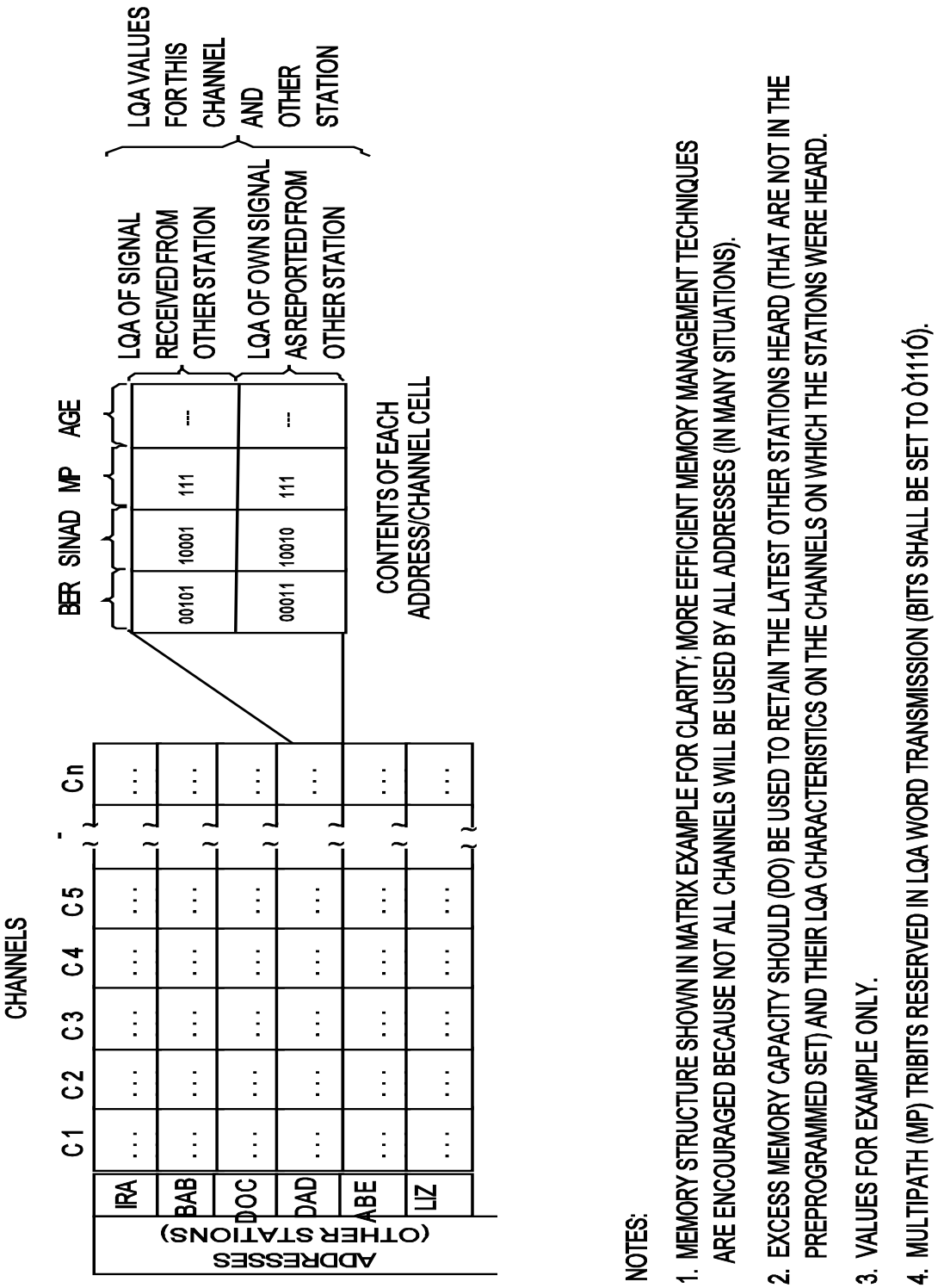


FIGURE A-4. Connectivity and LQA memory example.

A.4.3.3.2 Link quality memory.
The equipment shall be capable of storing, retrieving, and employing at least 4000 (DO: 10,000) sets of connectivity and LQA information associated with the channels and the other addresses in an LQA memory. The connectivity and LQA information storage shall be retained in memory for not less than one hour during power down or loss of primary power. The information in each address/channel "cell" shall include as a minimum, bilateral SINAD values of (a) the signals received at the station, and (b) the station's signals received at, and reported by, the other station. It shall also include either an indicator of the age of the information (for discounting old data), or an algorithm for automatically reducing the weight of data with time, to compensate for changing propagation conditions. (DO: the cells of the LQA memory should also include bilateral bit-error ratio (BER) and bilateral MP information derived by suitably equipped units.) The information within the LQA memory shall be used to select channels and manage networks as stated in this document. See figure A-4.

A.4.3.3.3 Other station settings storage.
DO: Equipment settings for use in linking with specific stations or nets should be stored in non-volatile memory. Such settings may include antenna selection and azimuth, channels authorized for that station or net, power limits for the relevant net, and so on.

A.4.3.4 Operating parameters.
In addition to the Channel memory, Self address memory, and Other station table specified in the preceding paragraphs, the following ALE operating parameters and overrides shall be programmable by the operator or an external automated controller.

Parameter	Reference
Scanning rate	A.4.2.1
Wait time T_{wt}	Table A-XV
Tune time T_t	Table A-XV
Sounding interval T_{ps}	Table A-XV
Wait for activity timer T_{wa}	Table A-XV

Override	Reference
Do not listen before transmit	A.5.4.7.3
Ignore call on channel already in use	A.5.5.3.3
Disable automatic link termination	A.5.5.3.5.2
Ignore AllCall	A.5.5.4.4
Ignore AnyCall	A.5.5.4.5
Ignore Wildcard Call	A.5.5.4.6

If Alternative Quick Call ALE (A.5.8) is implemented, the following shall be programmable:

Parameter	Reference
Automatically derive AQC call duration	A.5.8.2.1
Automatically derive AQC sound duration	A.5.8.2.6

A.4.3.5 Message memory.
Storage for preprogrammed, operator entered, and incoming messages shall be provided in the equipment. This storage shall be retained in memory for not less than one hour during power down or loss of primary power. Storage for at least 12 messages (DO: 100 messages), and a total capacity of at least 1000 characters (DO: 10,000 characters) shall be provided.

A.4.4 ALE operational rules.
The ALE system shall incorporate the basic operational rules listed in table A-V. Some of these rules may not be applicable in certain applications. For example, “always listening” is not possible while transmitting with a transceiver or when using a common antenna with a separate transmitter and receiver.

TABLE A-V. ALE operational rules.

1) Independent ALE receive capability (in parallel with other modems and simular audio receivers) (critical).
2) Always listening (for ALE signals) (critical).
3) Always will respond (unless deliberately inhibited).
4) Always scanning (if not otherwise in use).
5) Will not interfere with active channel carrying detectable traffic in accordance with table A-I (unless this listen call function is overridden by the operator or other controller).
6) Always will exchange LQA with other stations when requested (unless inhibited), and always measures the signal quality of others.
7) Will respond in the appropriate time slot to calls requiring slotted responses.
8) Always seek (unless inhibited) and maintain track of their connectivities with others.
9) Linking ALE stations employ highest mutual level of capability.
10) Minimize transmit and receive time on channel.
11) Automatically minimize power used (if capable).
NOTE : Listed in order of precedence.

A.4.5 Alternate Quick Call ALE (AQC-ALE).

A.4.5.1 Introduction.
This feature may be implemented in addition to the basic ALE functionality described in this appendix. The AQC-ALE provides a link establishment technique that requires significantly less

time to link than the baseline ALE system. This is accomplished by some additional technology and trading-off some of the lesser used functions of the baseline system, for a faster linking process. The AQC-ALE shall always be listening for the baseline ALE call and shall automatically respond and operate in that mode when called.

A.4.5.2 General signaling strategies.
The AQC-ALE format employs the following characteristics:

a. Packs three address characters (21 bits) into a 16-bit value

b. Addresses are reduced from a maximum of 15 characters to 6 characters

c. Six (6) address characters are sent in every transaction

d. Replaces two seldom used preambles as follows:
FROM preamble becomes PART2 indicating the 2nd address word
- THRU preamble becomes INLINK indicating a linked transaction

e. Isolates station addresses from message portion of the signaling structure:
- TO, TIS, TWAS, INLINK, PART2 preambles used for addressing
- CMD, DATA, and REP are used for messaging

f. Easy separation of second generation basic ALE and AQC-ALE protocols:
- Fixes 1 bit of any address word
- Prevents legitimate addresses in AQC-ALE from being legitimate addresses in second generation basic ALE.

g. Provides at least eight information bits per transmission

A.4.5.3 Features supported by AQC-ALE.
The following basic ALE features are fully implemented using the AQC-ALE protocol.

NOTE: A station operating in AQC-ALE can respond to any call type, but a station equipped with only second generation basic ALE will not respond to AQC-ALE protocol forms.

a. Linking protection levels 0, 1, 2, 3

b. Unit calls

c. Star Net calls

d. Allcalls

e. AnyCalls

f. LQA Exchange as part of the call handshake

g. Supports Orderwire and Relay features while in a link:

- automatic message display (AMD), data text message (DTM) or DBM
- User Unique Functions (UUF) when in a link
- Call Relay features
- Time of day and Network Management

h. Sounds are shortened to include scan time + 50percent

A.4.5.4 Features not provided by AQC-ALE.

a. Group call. As an alternative, a controller can use the calling protocol to add on additional members. Behavior of the system is more akin to setting up a call and then conferencing in a third party.

b. AMD, DTM, DBM are not provided during link set up. Primary focus of AQC-ALE is to establish a link between two or more stations as rapidly as possible. Once linked, information can be exchanged in the most efficient manner as is common between stations.

c. Early identification of transmitter's address during orderwire traffic or additional addressing identification for relay addresses. The need for this is eliminated because the call setup is significantly reduced. Orderwire messages are not allowed during the call setup.

A.5. DETAILED REQUIREMENTS.

A.5.1 ALE modem waveform.

A.5.1.1 Introduction.

The ALE waveform is designed to pass through the audio passband of standard SSB radio equipment. This waveform shall provide for a robust, low-speed, digital modem capability used for multiple purposes to include selective calling and data transmission. This section defines the waveform including the tones, their meanings, the timing and rates, and their accuracy.

A.5.1.2 Tones.

The waveform shall be an 8-ary frequency shift-keying (FSK) modulation with eight orthogonal tones, one tone (or symbol) at a time. Each tone shall represent three bits of data as follows (least significant bit (LSB) to the right):

- 750 Hz 000
- 1000 Hz 001
- 1250 Hz 011
- 1500 Hz 010
- 1750 Hz 110
- 2000 Hz 111
- 2250 Hz 101
- 2500 Hz 100

The transmitted bits shall be encoded and interleaved data bits constituting a word, as described in paragraphs A.5.2.2 and A.5.2.3. The transitions between tones shall be phase continuous and shall be at waveform maxima or minima (slope zero).

A.5.1.3 Timing.

The tones shall be transmitted at a rate of 125 tones (symbols) per second, with a resultant period of 8 ms per tone. Figure A-5 shows the frequency and time relationships. The transmitted bit rate shall be 375 bits per second (b/s). The transitions between adjacent redundant (tripled) transmitted words shall coincide with the transitions between tones, resulting in an integral 49 symbols (or tones) per redundant (tripled) word. The resultant single word period (T_w) shall be 130.66... ms (or 16.33... symbols), and the triple word (basic redundant format) period (3 T_w) shall be 392 ms.

A.5.1.4 Accuracy.

At baseband audio, the generated tones shall be within $\pm$1.0 Hz. At rf, all transmitted tones shall be within the range of 2.0 dB in amplitude. Transmitted symbol timing, and therefore, the bit and word rates shall be within ten parts per million.

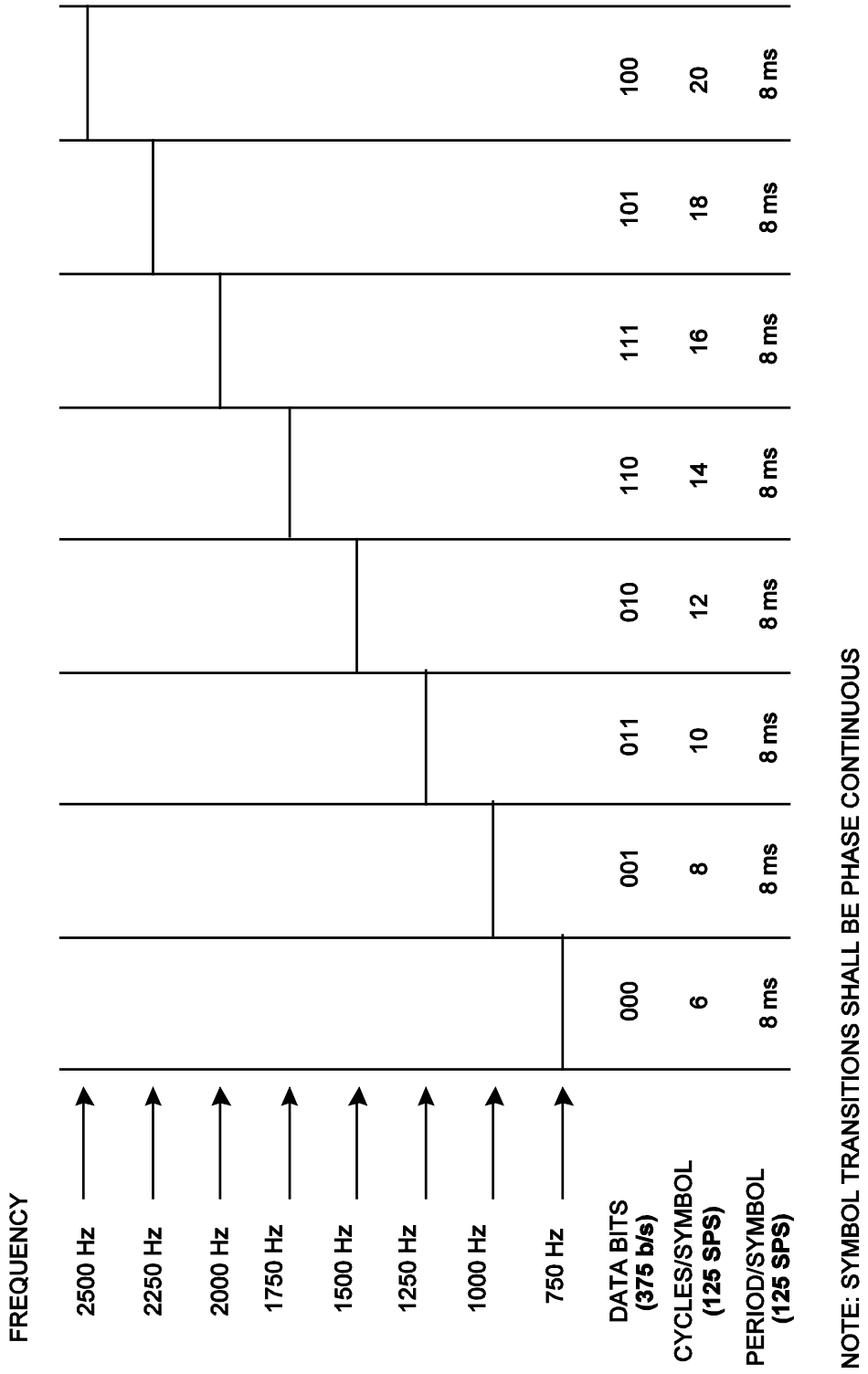


FIGURE A-5. ALE symbol library.

A.5.2 Signal structure.

A.5.2.1 Introduction.
This section provides definition of the ALE signal structure. Included are: forward error correction, word structure, addressing, frame structure, and synchronization. Also described in this section are: addressing, signal quality analysis, and the functions of the standard word preambles associated with the signal structure.

A.5.2.2 FEC.

A.5.2.2.1 General.
The effective performance of stations, while communicating over adverse rf channels, relies on the combined use of forward error correction, interleaving, and redundancy. These functions shall be performed within the transmit encoder and receive decoder.

A.5.2.2.2 Golay coding.
The Golay (24, 12, 3) FEC code is prescribed for this standard. The FEC code generator polynomial shall be:

$$g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

The generator matrix G, derived from g(x), shall contain an identity matrix I_{12} and a parity matrix P as shown in figure A-6. The corresponding parity check matrix H shall contain a transposed matrix p^T and an identity matrix I_{12} as shown in figure A-7.

A.5.2.2.2.1 Encoding.
Encoding shall use the fundamental formula x = uG, where the code word x shall be derived from the data word u and the generator matrix G. Encoding is performed using the G matrix by summing (modulo-2) the rows of G for which the corresponding information bit is a “1.” See figures A-6, A-8, and A-9a.

A.5.2.2.2.2 Decoding.
Decoding will implement the equation

$$s = y H^T$$

where y = x + e is a received vector which is the modulo-2 sum of a code word x and an error vector e, s is a vector of “n - k” bits called the syndrome. See figure A-9. See figure A-7 for the value of H. Each correctable/detectable error vector e results in a unique vector s. Because of this, s is computed according to the equation above and is used to index a look-up of the corresponding e, which is then added modulo-2 to y to give the original code word x. Flags are set according to the number of errors being corrected. The uses of the flags are described in A.5.2.6. If s is not equal to 0 and e contains more ones than the number of errors being corrected by decoding mode, a detected error is indicated and the appropriate flag is set.

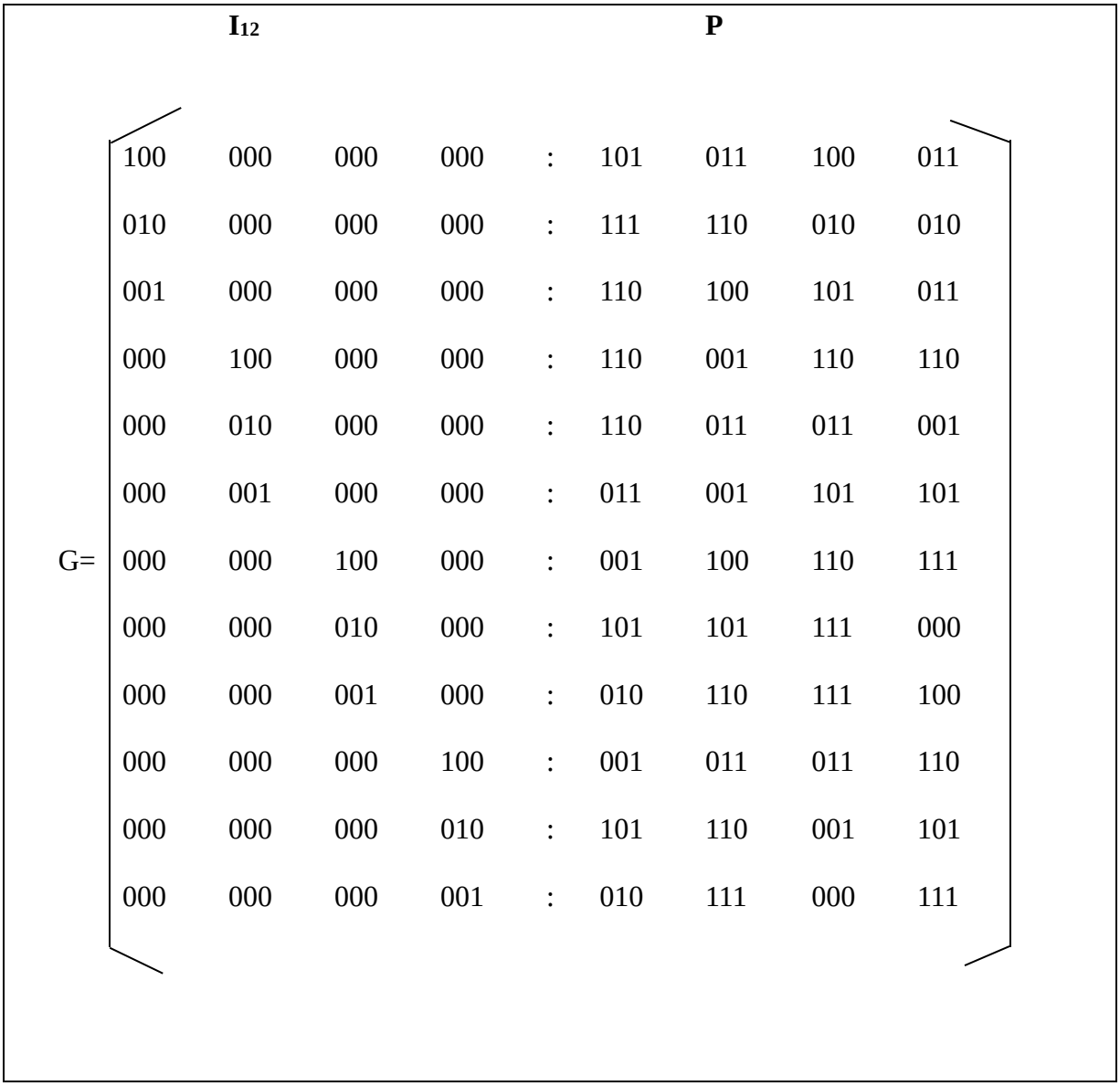


FIGURE A-6. Generator matrix for (24, 12) extended Golay code.

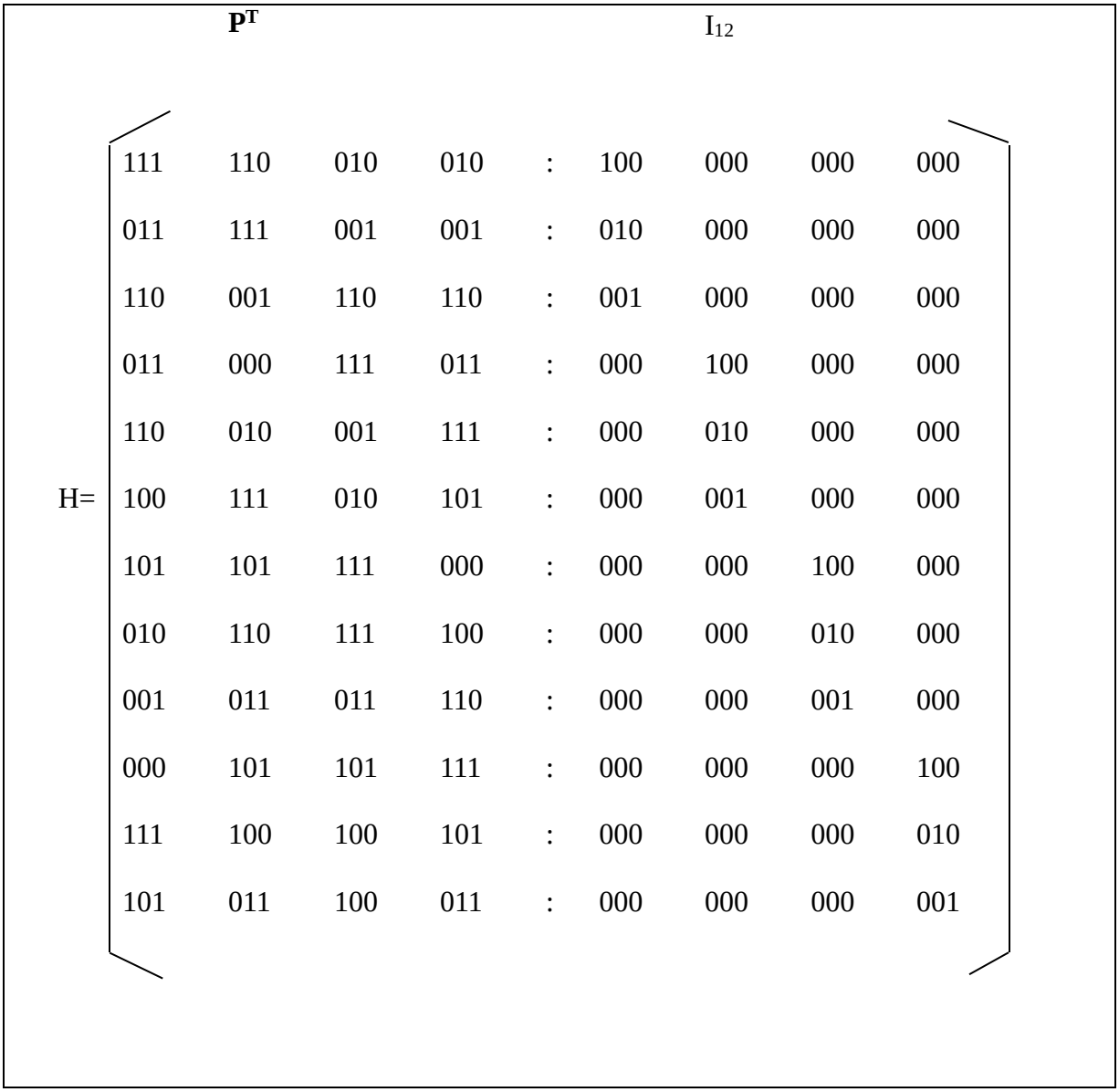


FIGURE A-7. Parity-check matrix for (24, 12) extended Golay code.

12 Bits To Encode	1	1	0	1	0	0	0	1	0	1	0	1
Bit Numbers	1	2	3	4	5	6	7	8	9	10	11	12

'G' MATRIX ROW NUMBERS								
1	100	000	000	000	101	011	100	011
2	010	000	000	000	111	110	010	010
4	000	100	000	000	110	001	110	110
8	000	000	010	000	101	101	111	000
10	000	000	000	100	001	011	011	110
12	000	000	000	001	010	0111	000	011

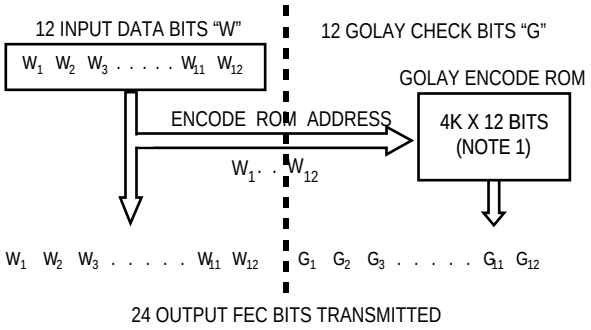
110	100	010	101	010	101	100	110
ENCODED DATA BITS* $W_1 \ldots W_{12}$ (OR $W_{13} \ldots W_{24}$)				GOLAY CHECK BITS $G_1 \ldots G_{12}$ (OR $G_{13} \ldots G_{24}$)			
24 BITS CODE WORD TO SEND							

*See note 2

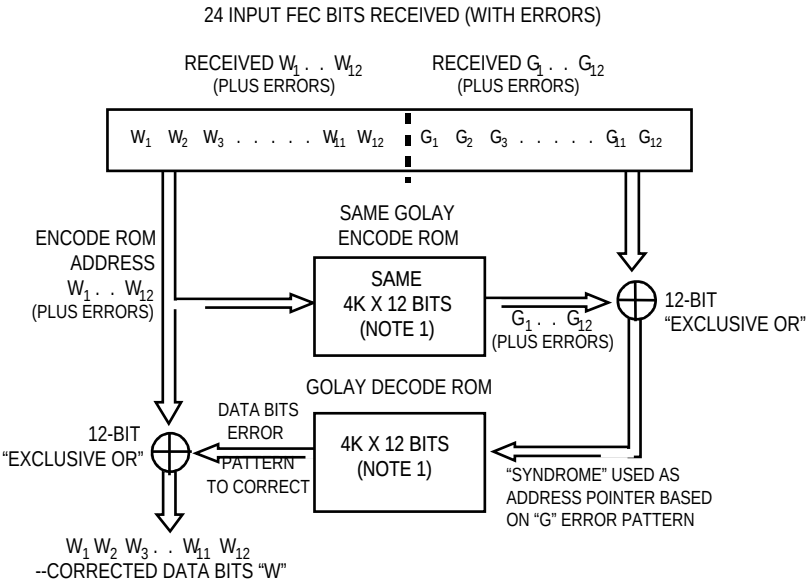
NOTES:

- The "bits" to be encoded determine which rows of the "G" generator matrix are to be "modulo-2" summed. In this example, bits 1, 2, 4, 8, 10, and 12 are "1," so row 1, 2, 4, 8, 10, and 12 are summed.
- Because this is a "systematic" code, the original 12 data bits also appear in the output encoded 24 bits.

FIGURE A-8. Golay word encoding example.



a. GOLAY FEC ENCODING EXAMPLE



b. GOLAY FEC DECODING EXAMPLE

NOTES:

1. ENCODE ROM CONTAINS GOLAY CHECK BITS "G_1. G_{12}" AT EACH ADDRESS, BASED ON DATA BITS "W_1 . . W_{12}" PREVIOUSLY COMPUTED FROM GENERATOR MATRIX "G" AND STORED.
2. DECODE ROM MAY INCLUDE ADDITIONAL BITS (OVER THE BASIC 12 TO CORRECT "W" BITS) TO INDICATE QUANTITY OR DATA ERRORS DETECTED AND CORRECTABILITY.
3. ROM "LOOK UP" HARDWARE FOR EXAMPLE ONLY. SOFTWARE IMPLEMENTATIONS MAY BE PREFERRED.

FIGURE A-9. Golay FEC coding examples.

A.5.2.2.3 Interleaving and deinterleaving.
The basic word bits W1 (most significant bit (MSB)) through W24 (LSB), and resultant Golay FEC bits G1 through G24 (with G13 through G24 inverted), shall be interleaved, before transmission using the pattern shown in figure A-10. The 48 interleaved bits plus a 49th stuff bit S49, (value = 0) shall constitute a transmitted word and they shall be transmitted A1, B1, A2, B2... A24, B24, S49 using 16-1/3 symbols (tones) per word (T_w) as described in A.5.1.3. At the receiver, and after 2/3 voting (see A.5.2.2.4), the first 48 received bits of the majority word (including remaining errors) shall be deinterleaved as shown in figure A-10 and then Golay FEC decoded to produce a correct(ed) 24-bit basic word (or an uncorrected error flag). The 49th stuff bit (S49) is ignored.

A.5.2.2.4 Redundant words.
Each of the transmitted 49-bit (or 16-1/3 symbol) (T_w) words shall be sent redundantly (times 3) to reduce the effects of fading, interference, and noise. An individual (or net) routing word (TO...), used for calling a scanning (multichannel) station (or net), shall be sent redundantly as long as required in the scan call (T_{sc}) to ensure receipt, as described in A.5.5.2. However, when the call is a non-net call to multiple scanning stations (a group call, using THRU and REPEAT (REP) alternately), the first individual routing word (THRU) and all the subsequent individual routing words (REP, THRU, REP,...) shall be sent three adjacent times (T_{rw}). These triple words for the individual stations shall be rotated in group sequence as described in A.5.5.3. See figure A-11. At bit time intervals (approximately $T_w/49$), the receiver shall examine the present bit and past bit stream and perform a 2/3 majority vote, on a bit-by-bit basis, over a span of three words. See tables A-VI and A-VII. The resultant 48 (ignoring the 49th bit) most recent majority bits constitute the latest majority word and shall be delivered to the deinterleaver and FEC decoder. In addition, the number of unanimous votes of the 48 possible votes associated with this majority word are temporarily retained for use as described in A.5.2.6.

A.5.2.3 Word structures.

A.5.2.3.1 ALE word format.
The basic ALE word shall consist of 24 bits of information, designated W1 (MSB) through W24 (LSB). The bits shall be designated as shown in figure A-12.

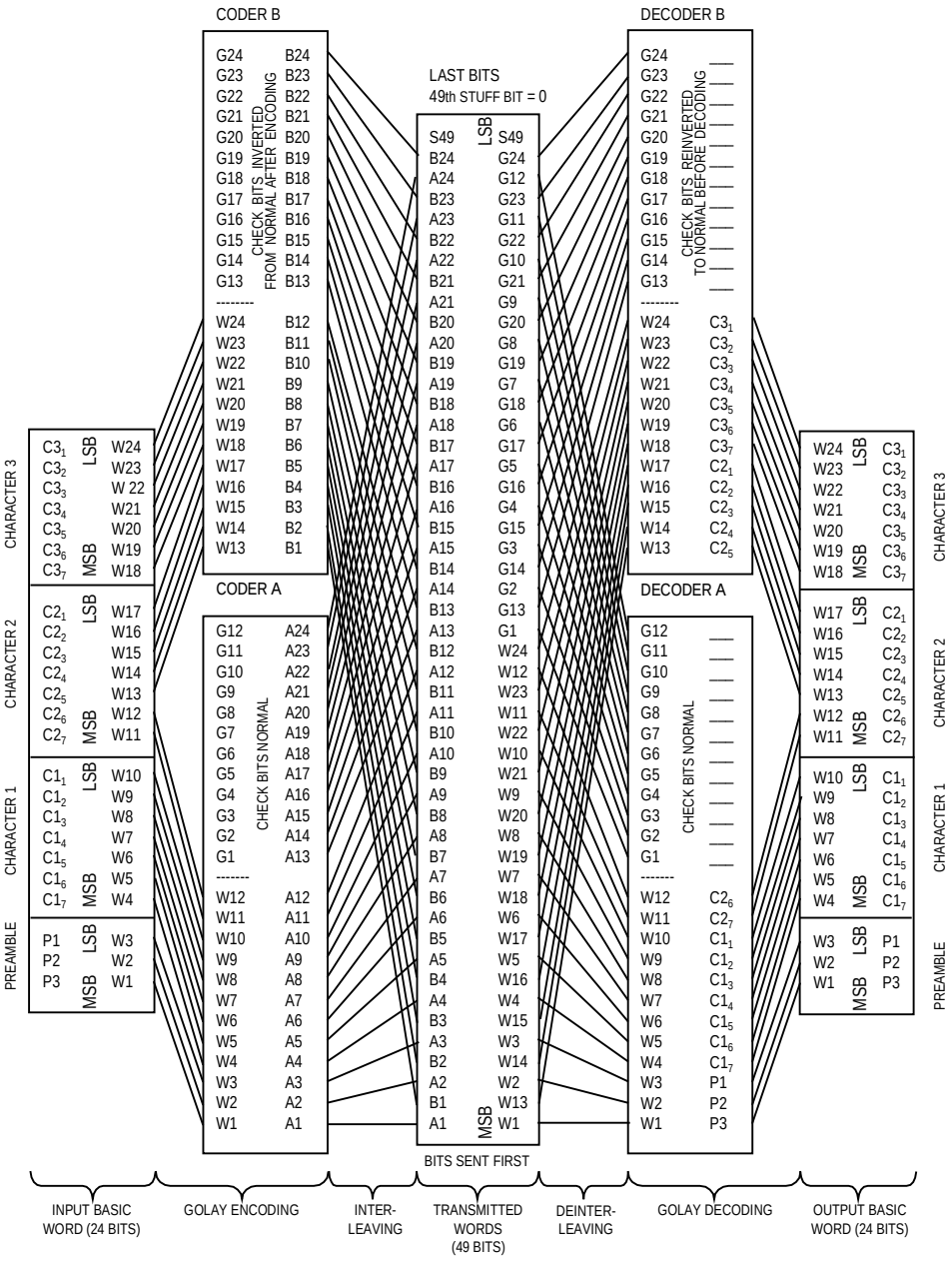
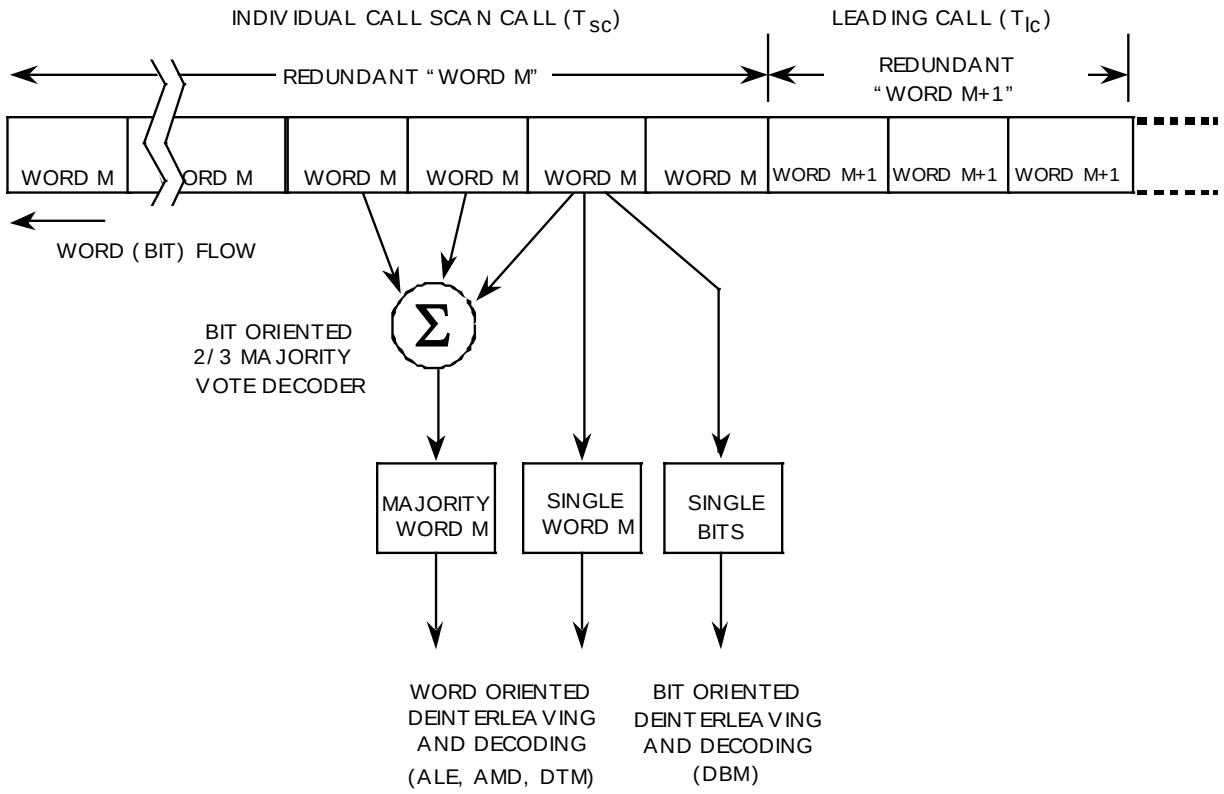


FIGURE A-10. Word bit coding and interleaving.



NOTES:

1. USE OF 2/3 VOTING REQUIRES EACH WORD M TO BE TRANSMITTED AT LEAST THREE ADJACENT TIMES.
2. **AMD** REFERS TO AUTOMATIC MESSAGE DISPLAY;
   DTM REFERS TO DATA TEXT MESSAGE.
   DBM REFERS TO DATA BLOCK MESSAGE;

FIGURE A-11. Bit and word decoding.

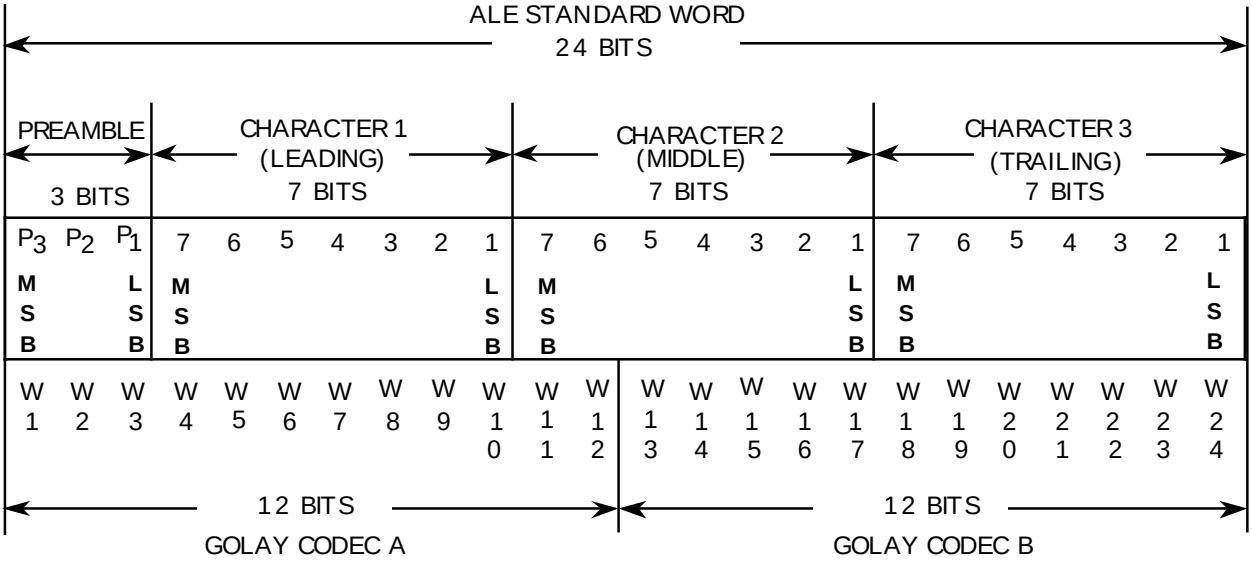
TABLE A-VI. 2/3 Majority vote decoding.

Received Bit R	Received Time	Eight Possible Bit Combinations							
R (n) (now)	T	0	0	0	0	1	1	1	1
R(n-49) (T_w old)	T-130.66... ms	0	0	1	1	0	0	1	1
R(n-98) (2 T_w old)	T-261.33... ms	0	1	0	1	0	1	0	1
Resultant majority bit M:		0	0	0	1	0	1	1	1
Possible error flag:		0	1	1	1	1	1	1	0
0 = error unlikely 1 = error likely									

TABLE A-VII. Majority word construction.

Relative Time	Received Bits R (Time) for 2/3 Voting			Majority Words Bit M	Used as Decoder Bits
Stuff bits	R(n)	R(n-49)	R(n-98)	M(n)	S49 ignored
Recent (LSB)	R(n-1)	R(n-50)	R(n-99)	M(n-1)	B24 (LSB)
	R(n-2)	R(n-51)	R(n-100)	M(n-2)	A24
	R(n-3)	R(n-52)	R(n-101)	M(n-3)	B23
	R(n-4)	R(n-53)	R(n-102)	M(n-4)	A23
	•	•	•	•	•
	•	•	•	•	•
	•	•	•	•	•
	R(n-46)	R(n-95)	R(n-144)	M(n-46)	A2
	R(n-47)	R(n-96)	R(n-145)	M(n-47)	B1
Older (MSB)	R(n-48)	R(n-97)	R(n-146)	M(n-48)	A1 (MSB)

NOTES:
"n" indicates present bit time
"n-m" indicates bit received at "m" bit times earlier



NOTE:
1. THREE 7-BIT ASCII CHARACTERS PER WORD IN DATA FIELD (W4-W10, W11-W17, W18-W24).
2. OPTIONAL 21-BIT UNFORMATTED DATA FIELD (W4-W24). MSB (W1) TRANSMITTED FIRST.

FIGURE A-12. ALE basic word structure.

A.5.2.3.1.1 Structure.
The word shall be divided into two parts: a 3-bit preamble and a 21-bit data field (which often contains three 7-bit characters). The MSB for all parts, and the word, is to the left in figure A-12 and is sent earliest. Before transmission, the word shall be divided into two 12-bit halves (Golay code A and B in figure A-10) for FEC encoding as described in 5.2.2.

The optional AQC-ALE word packs the address data. Details of this can be found in A.5.8.1.1, AQC-ALE Address Word Structure.

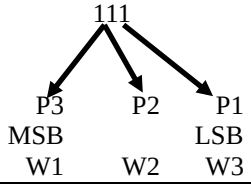
A.5.2.3.1.2 Word types.
The leading three bits, W1 through W3, are designated preamble bits P3 through P1, respectively. These preamble bits shall be used to identify one of eight possible word types.

A.5.2.3.1.3 Preambles.
The word types (and preambles) shall be as shown in table A-VIII and as described herein.

Optional AQC-ALE preambles are defined in A.5.8.1.2.

TABLE A-VIII. ALE word types (preambles).

Word Type	Code Bits	Functions	Significance
THRU	001	multiple (and indirect routing	present multiple direct destinations for group calls (and future indirect relays, reserved)
TO	010	direct routing	present direct destination for individual and net calls
CMD	110	orderwire control and status	ALE system-wide station (and operator) orderwire for coordination, control, status, and special functions
FROM	100	identification (and indirect routing)	identification of present transmitter without termination (and past originator and relayers, reserved)
TIS	101	terminator and identification continuing	identification of present transmitter, signal terminations, protocol continuation
TWAS	011	terminator and identification quitting	identification of present transmitter, signal and protocol termination
DATA	000	extension and information	extension of data field of the previous ALE work, or information defined by the previous CMD
REP	111	duplication and information	duplication of the previous preamble, or information defined by the previous CMD



A.5.2.3.2 Address words.

A.5.2.3.2.1 TO.
The TO word (010) shall be used as a routing designator which shall indicate the address of the present destination station(s) which is (are) to directly receive the call. TO shall be used in the individual call protocols for single stations and in the net call protocols for multiple net-member stations which are called using a single net address. The TO word itself shall contain the first three characters of an address. For extended addresses, the additional address words (and characters) shall be contained in alternating DATA and REP words, which shall immediately follow. The sequence shall be TO, DATA, REP, DATA, and REP, and shall be only long enough to contain the address, up to a maximum capacity of five address words (15 characters).

A.5.2.3.2.2 THIS IS (TIS).
The TIS word (101) shall be used as a routing designator which shall indicate the address of the present calling (or sounding) station which is directly transmitting the call (or sound). Except for the use of TWAS, TIS shall be used in all ALE protocols to terminate the ALE frame and transmission. It shall indicate the continuation of the protocol or handshake, and shall direct, request, or invite (depending on the specific protocol) responses or acknowledgments from other called or receiving stations. The TIS shall be used to designate the call acceptance sound. The TIS word itself shall contain the first three characters of the calling stations address. For extended addresses, the additional address words (and characters) shall be contained in alternating DATA and REP words which shall immediately follow, exactly as described for whole addresses using

the TO word and sequence. The entire address (and the required portion of the TIS, DATA, REP, DATA, REP sequence, as necessary) shall be used only in the conclusion section of the ALE frame (or shall constitute an entire sound). TWAS shall not be used in the same frame as TIS, as they are mutually exclusive.

A.5.2.3.2.3 THIS WAS (TWAS).
The TWAS word (011) shall be used as a routing designator exactly as the TIS, with the following variations. It shall indicate the termination of the ALE protocol or handshake, and shall reject, discourage, or not invite (depending on the specific protocol) responses or acknowledgments from other called or receiving stations. The TWAS shall be used to designate the call rejection sound. TIS shall not be used in the same frame as TWAS, as they are mutually exclusive.

A.5.2.3.2.4 THRU.
The THRU word (001) shall be used in the scanning call section of the calling cycle only with group call protocols. The THRU word shall be used alternately with REP, as routing designators, to indicate the address first word of stations that are to be directly called. Each address first word shall be limited to one basic address word (three characters) in length. A maximum of five different address first words shall be permitted in a group call. The sequence shall only be alternations of THRU, REP. The THRU shall not be used for extended addresses, as it will not be used within the leading call section of the calling cycle. When the leading call starts in the group call, the entire group of called stations shall be called with their whole addresses, which shall be sent using the TO preambles and structures, as described in A.5.2.3.2.1.

NOTE: 1. The THRU word is also reserved for future implementation of indirect and relay protocols, in which cases it may be used elsewhere in the ALE frame and with whole addresses and other information. Stations designed in compliance with this nonrelay standard should ignore calls to them which employ their address in a THRU word in other than the scanning call.

NOTE: 2. The THRU preamble value is also reserved for the AQC-ALE protocol.

A.5.2.3.2.5 FROM.
The FROM word (100) is an optional designator which shall be used to identify the transmitting station without using an ALE frame termination, such as TIS or TWAS. It shall contain the whole address of the transmitting station, using the FROM, and if required, the DATA and REP words, exactly as described in the TO address structure in A.5.2.3.2.1. It should be used only once in each ALE frame, and it shall be used only immediately preceding a command (CMD) in the message section. Under direction of the operator or controller, it should be used to provide a “quick ID” of the transmitting station when the normal conclusion may be delayed, such as when a long message section is to be used in an ALE frame.

NOTE: 1. The FROM word is also reserved for future implementation of indirect and relay protocols, in which cases it may be used elsewhere in the ALE frame and with multiple ad-

dresses and other information. Stations designed in compliance with this nonrelay standard should ignore sections of calls to them that employ FROM words in any other sequence than immediately before the CMD word.

NOTE: 2. The FROM preamble value is also reserved for the AQC-ALE protocol.

A.5.2.3.3 Message words.
All message words (orderwire messages) begin with a word with the CMD preamble. The CMD word (110) is a special orderwire designator which shall be used for system-wide coordination, command, control, status, information, interoperation, and other special purposes. CMD shall be used in any combination between ALE stations and operators. CMD is an optional designator which is used only within the message section of the ALE frame, and it shall have (at some time in the frame) a preceding call and a following conclusion, to ensure designation of the intended receivers and identification of the sender. The first CMD terminates the calling cycle and indicates the start of the message section of the ALE frame. The orderwire functions are directed with the CMD itself, or when combined with the REP and DATA words. See A.5.6 for message words (orderwire messages) and functions.

A.5.2.3.4 Extension words.

A.5.2.3.4.1 DATA.
The DATA word (000) is a special designator which shall be used to extend the data field of any previous word type (except DATA itself) or to convey information in a message. When used with the routing designators TO, FROM, TIS, or TWAS, DATA shall perform address extension from the basic three characters to six, nine, or more (in multiples of three) when alternated with REP words. The selected limit for address extension is a total of 15 characters. When used with CMD, its function is predefined as specified in A.5.6 for message words (orderwire messages) and functions.

A.5.2.3.4.2 REP.
The REP word (111) is a special designator which shall be used to duplicate any previous preamble function or word meaning while changing the data field contents (bits W4 through W24). See table A-VIII. Any change of words or data field bits requires a change of preamble bits (P_3 through P_1) to preclude uncertainty and errors. If a word is to change, even if the data field is identical to that in the previous word, the preamble shall be changed, thereby clearly designating a word change. When used with the routing designator TO, REP performs address expansion, which enables more than one address to be specified. See A.5.2.3.2.4 for use with THRU. With DATA, REP may be used to extend and expand address, message, command, and status fields. REP shall be used to perform these functions, and it may directly follow any other word type except for itself, and except for TIS or TWAS, as there cannot be more than one transmitter for a specific call at a given time.

NOTE 1. REP is used in T_{sc} of group calls directed to units with different first word addresses.

NOTE 2. REP is not used in T_{sc} of calls directed to groups with same first word addresses. Also REP is not used in T_{sc} of calls directed to individuals and nets.

A.5.2.4 Addressing.

A.5.2.4.1 Introduction.
The ALE system deploys a digital addressing structure based upon the standard 24-bit (three character) word and the Basic 38 character subset. As described below, ALE stations have the capability and flexibility to link or network with one or many prearranged or as-needed single or multiple stations. All ALE stations shall have the capacity to store and use at least 20 self addresses of up to 15 characters each in any combination of individual and net calls. There are three basic addressing methods which will be presented:

- Individual station
- Multiple station
- Special modes

NOTE: Certain alphanumeric address combinations may be interpreted to have special meanings for emergency or specific functions, such as “SOS,” “MAYDAY,” “PANPAN,” “SECURITY,” “ALL,” “ANY,” and “NULL.” These should be carefully controlled or restricted.

A.5.2.4.2 Basic 38 ASCII subset.
The Basic 38 ASCII subset shall include all capital alphabetics (A-Z) and all digits (0-9), plus designated utility and wildcard symbols “@” and “?,” as shown in figure A-13. The Basic 38 ASCII subset shall be used for all basic addressing functions. To be a valid basic address, the word shall contain a routing preamble from A.5.2.3.2 (such as TO...), plus three alphanumeric characters (A-Z, 0-9) from the Basic 38 ASCII subset in any combination. In addition, the “@” and “?” symbols shall be used for special functions. Digital discrimination of the Basic 38 ASCII subset shall not be limited to examination of only the three MSBs (b_7 through b_5), as a total of 48 digital bit combinations would be possible (including ten invalid symbols which would be improperly accepted).

BITS b_7 b_6 b_5	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
b_4 b_3 b_2 b_1 COLUMN → / ROW ↓	0	1	2	3	4	5	6	7
0 0 0 0 0	NUL	DLE	SP	0	@	P	`	p
0 0 0 1 1	SOH	DC1	!	1	A	Q	a	q
0 0 1 0 2	STX	DC2	"	2	B	R	b	r
0 0 1 1 3	ETX	DC3	#	3	C	S	c	s
0 1 0 0 4	EOT	DC4	$	4	D	T	d	t
0 1 0 1 5	ENQ	NAK	%	5	E	U	e	u
0 1 1 0 6	ACK	SYN	&	6	F	V	f	v
0 1 1 1 7	BEL	ETB	'	7	G	W	g	w
1 0 0 0 8	BS	CAN	(	8	H	X	h	x
1 0 0 1 9	HT	EM	)	9	I	Y	i	v
1 0 1 0 10	LF	SUB	*	:	J	Z	j	z
1 0 1 1 11	VT	ESC	+	;	K	[	k	{
1 1 0 0 12	FF	FS	,	<	L	\	l	|
1 1 0 1 13	CR	GS	-	=	M	]	m	}
1 1 1 0 14	SO	RS	.	>	N	^	n	~
1 1 1 1 15	SI	US	/	?	O	_	o	DEL

FIGURE A-13. Basic 38 ASCII subset (unshaded areas).

A.5.2.4.3 Stuffing.
The ALE basic address structure is based on single words which, in themselves, provide multiples of three characters. The quantity of available addresses within the system, and the flexibility of assigning addresses, are significantly increased by the use of address character stuffing. This technique allows address lengths that are not multiples of three to be compatibly contained in the standard (multiple of three characters) address fields by "stuffing" the empty trailing positions with the utility symbol "@." See table A-IX. "Stuff-1" and "Stuff-2" words shall only be used in the last word of an address, and therefore should appear only in the leading call (T_{lc}) of the calling cycle (T_{cc}).

NOTE: As an example of proper usage, a call to the address "MIAMI" would be structured "TO MIA," "DATA MI@."

A.5.2.4.4 Individual addresses.
The fundamental address element in the ALE system is the single routing word, containing three characters, which forms the basic individual station address. This basic address word, used primarily for intranet and slotted operations, may be extended to multiple words and modified to provide increased address capacity and flexibility for internet and general use. An address which is assigned to a single station (within the known or used network) shall be termed an "individual" address. If it consists of one word (that is, no longer than three characters) it shall be termed a "basic" size, and if it exceeds one word, it shall be termed an "extended" size.

TABLE A-IX. Use of "@" utility symbol.

Pattern	Function	Guidance
TO A B C	"Standard" three character address structure "ABC"	Any position in address and sequences
TO A B @	"Stuff-1" reduced address fields; adds characters "A, B"	Only last word in address; anywhere in sequences
TO A @ @	"Stuff-2" reduced address fields; adds character "A"	Only last word in address; anywhere in sequences
TO @ ? @	"Allcall" global address; all stop and listen (unless inhibited), none respond	Exclusive member of calling cycle; single TO only
TO @ A @ REP @ B @ (option)	"Selective AllCall;" global address; all with same last character "A" (or "B") stop and listen (unless inhibited), none respond	Alone, or with additional different AllCall selections, for "group selective AllCall;" only in calling cycle; must use TO, REP alternately never DATA, if more than one*
TO @ @ ?	"AnyCall" global address; all stop and respond in PRN slots (unless inhibited), none respond	Exclusive member of calling cycle; single TO only
TO @ @ A REP @ @ B (option)	"Selective AnyCall;" all with same last character(s) "A" (or "B") stop and respond in PRN slots (unless inhibited), using own addresses	Alone or with additional different AnyCall selections, for "group selective AnyCall;" only in calling cycle; must use TO, REP alternately (never DATA), if more than one*
TO @ A B REP @ C D (option)	"Double selective AnyCall;" all with same last characters "AB" (or "CD") stop and respond in PRN slots (unless inhibited), using own addresses	Alone or with additional different AnyCall selections, for "group selective AnyCall;" only in calling cycle; must use TO, REP alternately (never DATA), if more than one*
TO @ @ @	"Null" address; all ignore, test and maintenance use, or extra "buffer" slot	Any position in address sequence (omit from T_{sc} if group call) except never in conclusion (terminator), or REP, only if following TO

NOTES:

1. All patterns not shown here are reserved and shall be considered invalid until standardized.
2. "@" indicates special utility character (1000000); "?" wildcard (0111111).
3. "A," "B," "C," or "D" indicates any alphanumeric member of Basic 38 ASCII subset other than "@," or "?," that is "A-Z" and "0-9."

* THRU, REP in T_{sc} if group call.

A.5.2.4.4.1 Basic size.
The basic address word shall be composed of a routing preamble (TO, or possibly a REP which follows a TO, in T_{lc} of group call, or a TIS or TWAS) plus three address characters, all of which shall be alphanumeric numbers of the Basic 38 ASCII subset. The three characters in the basic individual address provide a Basic 38-address capacity of 46,656, using only the 36 alphanumerics. This three-character single word is the minimum structure. In addition, all ALE stations shall associate specific timing and control information with all own addresses, such as prearranged delays for slotted net responses. As described in A.5.5, the basic individual addresses of various station(s) may be combined to implement flexible linking and networking.

NOTE: All ALE stations shall be assigned at least one (DO: several) single-word address for automatic use in one-word address protocols, such as slotted (multi-station type) responses. This is a mandatory user requirement, not a design requirement. However, nothing in the design shall preclude using longer addresses.

A.5.2.4.4.2 Extended size.
Extended addresses provide address fields which are longer than one word (three characters), up to a maximum system limit of five words (15 characters). See table A-X. This 15-character capacity enables Integrated Services Digital Network (ISDN) address capability. Specifically, the ALE extended address word structure shall be composed of an initial basic address word, such as TO or TIS, as described above, plus additional words as necessary to contain the additional characters in the sequence DATA, REP, DATA, REP, for a maximum total of five words. All address characters shall be the alphanumeric members of the Basic 38 ASCII subset.

NOTE 1: All ALE stations shall be assigned at least one (DO: several) two-word address(es) for general use, plus an additional address(es) containing the station's assigned call sign(s). This is a mandatory user requirement, not a design requirement. However, nothing in the design shall preclude using longer addresses.

NOTE 2: The recommended standard address size for intranet, internet, and general non-ISDN use is two words. Any requirement to operate with address sizes larger than six characters must be a network management decision. As examples of proper usage, a call to "EDWARD" would be "TO EDW," "DATA ARD," and a call to "MISSISSIPPI" would be "TO MIS," "DATA SIS," "REP SIP," "DATA PI@."

TABLE A-X. Basic (38) address structures.

	Words	Address Characters	Types
BASIC	1	1	Stuff-2
	1	2	Stuff-1
	1	3	Basic
EXTENDED	2	4	Basic + Stuff-2
	2	5	Basic + Stuff-1
	2	6	2 Basic
	3	7	2 Basic + Stuff-2
	3	8	2 Basic + Stuff-1
	3	9	3 Basic
	4	10	3 Basic + Stuff-2
	4	11	3 Basic + Stuff-1
	4	12	4 Basic
	5	13	4 Basic + Stuff-2
	5	14	4 Basic + Stuff-1
	5 (limit)	15 (limit)	5 Basic (limit)

NOTES:

1. Basic : ABC
2. Stuff-2: A@@
3. Stuff-1: AB@

A.5.2.4.5 Net addresses.
The purpose of a net call is to rapidly and efficiently establish contact with multiple prearranged (net) stations (simultaneously if possible) by the use of a single net address, which is an additional address assigned to all net members in common. When a net address type function is required, a calling ALE station shall use an address structure identical to the individual station address, basic or extended as necessary. For each net address at a net member's station, there shall be a response slot identifier, plus a slot width modifier if directed by the specific standard protocol. As described in paragraphs A.5.5.3 and A.5.5.4, additional information concerning the assigned response slots (and size) must be available, and the mixing of individual, net, and group addresses and calls is restricted

A.5.2.4.6 Group addresses.
The purpose of a group call is to establish contact with multiple nonprearranged (group) stations (simultaneously if possible) rapidly and efficiently by the use of a compact combination of their own addresses which are assigned individually. When a group address type function is required, a calling ALE station shall use a sequence of the actual individual station addresses of the called stations, in the manner directed by the specific standard protocol. A station's address shall not appear more than once in a group calling sequence, except as specifically permitted in the group calling protocols described in A.5.5.4.

NOTE: The group feature is not available in the AQC-ALE protocol.

A.5.2.4.7 Allcall addresses.
An "AllCall" is a general broadcast that does not request responses and does not designate any specific address. This mechanism is provided for emergencies ("HELP!"), broadcast data exchanges, and propagation and connectivity tracking. The global AllCall address is "@?@." The AllCall protocol is discussed in A.5.5.4.4. As a variation on the AllCall, the calling station can organize (or divide) the available but unspecified receiving stations into logical subsets, using a selective AllCall address. A selective AllCall is identical in structure, function, and protocol to the AllCall except that it specifies the last single character of the addresses of the desired subgroup of receiving stations (1/36 of all). By replacing the "?" with an alphanumeric, the selective AllCall special address pattern is "TO @A@" (or possibly "THRU @A@" and "REP @B@" if more than one subset is desired), where "A" (and "B," if applicable) in this notation represents any of the 36 alphanumerics in the Basic-38 subset. "A" and "B" may represent the same or different character from the subset, and specifically indicate which character(s) must be last in a station's address in order to stop scan and listen.

NOTE: For ACQ-ALE, the Part2 address portion shall contain the same three characters used in the TO word of the call.

A.5.2.4.8 AnyCalls.

An "AnyCall" is a general broadcast that requests responses without designating any specific addressee(s). It is required for emergencies, reconstitution of systems, and creation of new networks. An ALE station may use the AnyCall to generate responses from essentially unspecified stations, and it thereby can identify new stations and connectivities. The global AnyCall address is "@@?." The AnyCall protocol is discussed in A.5.5.4.5. If too many responses are received to an AnyCall, or if the caller must organize the available but unspecified responders into logical subsets, a selective AnyCall protocol is used. The selective AnyCall address is identical in structure, function, and protocol to the global AnyCall, except that it specifies the last single character of the addresses of the desired subset of receiving station (1/36 of all). By replacing the "?" with an alphanumeric, the global AnyCall becomes a selective AnyCall whose special address pattern is "TO @@A." If even narrower acceptance and response criteria are required, the double selective AnyCall should be used. The double selective AnyCall is an operator selected general broadcast which is identical to the selective AnyCall described above, except that its special address (using "@AB" format) specifies the last two characters that the desired subset of receiving stations must have to initiate a response.

NOTE: For ACQ-ALE, the Part2 address portion shall contain the same three characters used in the TO word of the call.

A.5.2.4.9 Wildcards.

A "wildcard" is a special character that the caller uses to address multiple-station addresses with a single-call address. The receivers shall accept the wildcard character as a substitute for any alphanumeric in their self addresses in the same position or positions. Therefore, each wildcard character shall substitute for any of 36 characters (A to Z, 0 to 9) in the Basic 38-character subset. The total lengths of the calling (wildcard) address, and the called addresses shall be the same. The special wildcard character shall be "?" (0111111). It shall substitute for any alphanumeric in the Basic 38-character subset. It shall substitute for only a single-address character position in an address, per wildcard character. See table A-XI for examples of acceptable patterns.

TABLE A-XI. Use of "?" wildcard symbol.

A B C			BASIC "STANDARD," 1 CASE EACH
A B ?	A ? C	? B C	"STANDARD" "WILD-1," 36 CASES EACH
A ? ?	? B ?	? ? C	"STANDARD" "WILD-2," 1296 CASES EACH
? ? ?			"STANDARD" "WILD-3," 46656 CASES EACH
A B @			"STUFF-1," 1 CASE EACH
A ? @	? B @		"WILD-1" "STUFF-1," 36 CASES EACH
? ? @			"WILD-2" "STUFF-2," 1296 CASES EACH
A @ @			"STUFF-2," 1 CASE EACH
? @ @			"WILD-1" "STUFF-2," 36 CASES EACH
@ A B			"DOUBLE SELECTIVE ANYCALL," ("DSA") 1/1296 CASES
@ A ?			"DSA" "WILD-1," 1/36 CASES
@ ? B			NOT PERMITTED. USE "SELECTIVE ANYCALL"
@ ? ?			NOT PERMITTED. USE "GLOBAL ANYCALL"
@ @ A			"SELECTIVE ANYCALL"
@ @ ?			"GLOBAL ANYCALL"
@ A @			"SELECTIVE ALL CALL"
@ ? @			"GLOBAL ALL CALL"
? @ ?			"IN LINK ADDRESS"

A.5.2.4.10 Self addresses.
For self test, maintenance, and other purposes, stations shall be capable of using their own self addresses in calls. When a self-addressing type function is required, ALE stations shall use the following self-addressing structures and protocols. Any ALE calling structures and protocols permissible within this standard, and containing a specifically addressed calling cycle (such as

"TO ABC," but not AllCall or AnyCall), shall be acceptable, except that the station may substitute (or add) any one (or several) of its own calling addresses into the calling cycle.

A.5.2.4.11 Null address.
For test, maintenance, buffer times, and other purposes, the station shall use a null address that is not directed to, accepted by, or responded to by any station. When an ALE station requires a null address type function, it shall use the following null address protocol. The null address special address pattern shall be "TO @@@," (or "REP @@@"), if directly after another TO. The null address shall only use the TO (or REP), and only in the calling cycle (T_{CC}). Null addresses may be mixed with other addresses (group call), in which case they shall appear only in the leading call (T_{LC}), and not in the scanning call (T_{SC}). Nulls shall never be used in conclusion (terminator) (TIS or TWAS). If a null address appears in a group call, no station is designated to respond in the associated slot; therefore, it remains empty (and may be used as a buffer for tune-ups, or overflow from the previous slot's responder, etc.).

A.5.2.4.12 In-link address.
The inlink address feature is used by a system to denote that all members in the established link are to act upon the information sent in the frame containing the inlink address. The inlink address shall be '?@?'. When a radio enters the linked condition with one or more stations, the radio shall expand the set of recognized self addresses to include the inlink address ('?@?'). When a frame is transmitted by any member of the link using the inlink address, all members are thus addressed publicly and are to use the frame information. Thus, if a linked member sent an AMD message, all members would present that message to their user. If the member sent a frame terminated with a TWAS preamble, then all members would note that the transmitting station just 'left' the link. Short messages of 'to-?@?, to-?@?, tis-TALKINGMEMBER' would act as a keep-alive function and cause the receiving radio to extend any link termination timer.

A.5.2.5 Frame structure.
All ALE transmissions are based on the tones, timing, bit, and word structures described in paragraphs A.5.1 and A.5.2.3. All calls shall be composed of a "frame," which shall be constructed of contiguous redundant words in valid sequence(s) as described in figure A-14, as limited in table A-VII, and in formats as described in A.5.5. There are three basic frame sections: calling cycle, message, and conclusion. See A.5.2.5.5 for basic frame structure examples.

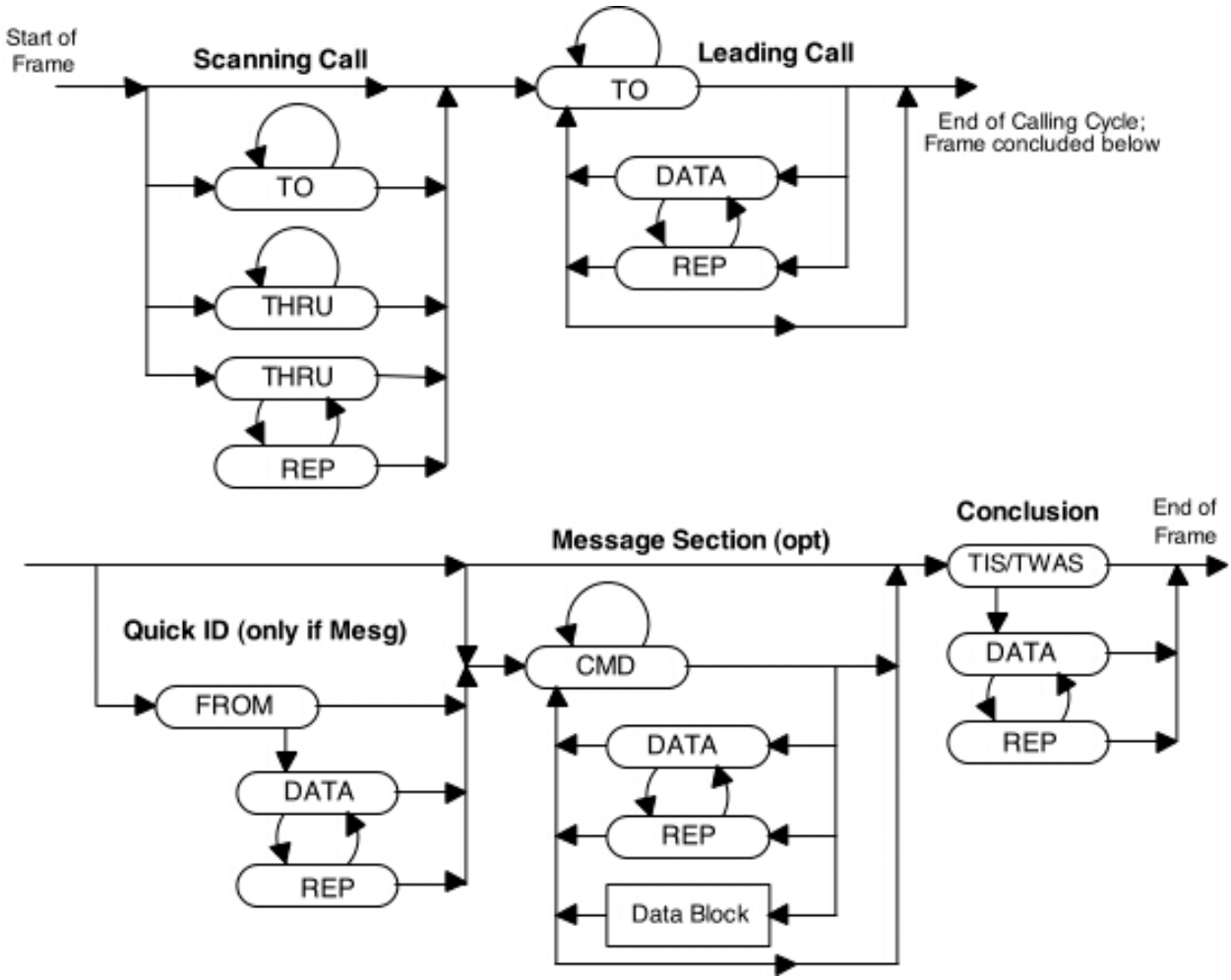


FIGURE A-14. Valid word sequences.

A.5.2.5.1 Calling cycle.
The initial section of all frames (except sounds) is termed a calling cycle (T_{cc}), and it is divided into two parts: a scanning call (T_{sc}) and a leading call (T_{lc}). The scanning call shall be composed of TO words if an individual or net call (or THRU and REP words, alternating, if a group call), which contain only the first word(s) of the called station(s) or net address. The leading call shall be composed of TO (and possibly DATA and REP) words containing the whole address(es) for the called station(s), from initiation of the leading call until the start of the message section or the conclusion (thus the end of the calling cycle). See figure A-15. The use of REP and DATA is described in A.5.2.4. The set of different address first words (T_{cl}) may be repeated as necessary for scanning calling (T_{sc}), to exceed the scan period (T_s). There is no unique "flag word" or "sync word" for frame synchronization (as discussed below). Therefore, stations may acquire and begin to read an ALE signal at any point after the start. The transmitter shall have reached at least 90 percent of the selected rf power within 2.5 ms of the first tone transmission following call initiation. The end of the calling cycle may be indicated by the start of the optional quick-ID, which occupies the first words in the message section, after the leading call and before the start of the rest of the message (or conclusion, if no message) section.

NOTE 1: The frame time may need to be delayed (equipment manufacturer dependent) to avoid loss of the leading words if the transmitter attack time is significantly long. Alternatively, the modem may transmit repeated duplicates of the scanning cycle (set of) first word(s) to be sent (not to be counted in the frame) as the transmitter rises to full power (and may even use the ALE signal momentarily instead of a tuning tone for the tuner), and then start the frame when the power is up.

NOTE 2: The 2.5-ms permissible delay of the first ALE tone, after the transmitter has reached 90 percent of selected power, is in addition to the allowable attack time delay specified in 5.3.5.1.

NOTE 3: Non-compliance with the 90 percent of power parameter will impact the probability of linking. Compliance testing for this can be construed to be met if the probability of linking criteria is met (see table A-I).

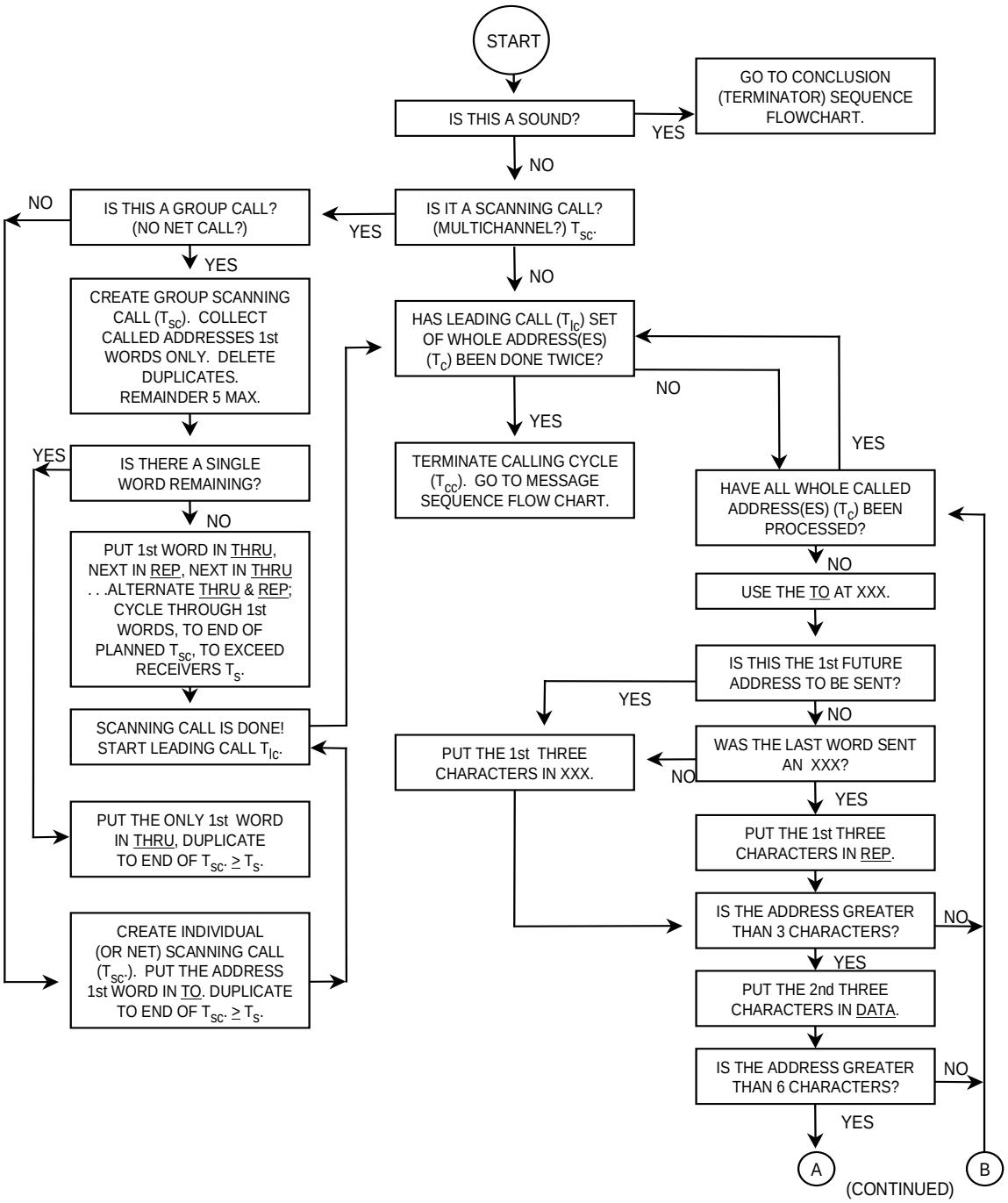


FIGURE A-15. Calling cycle sequence.

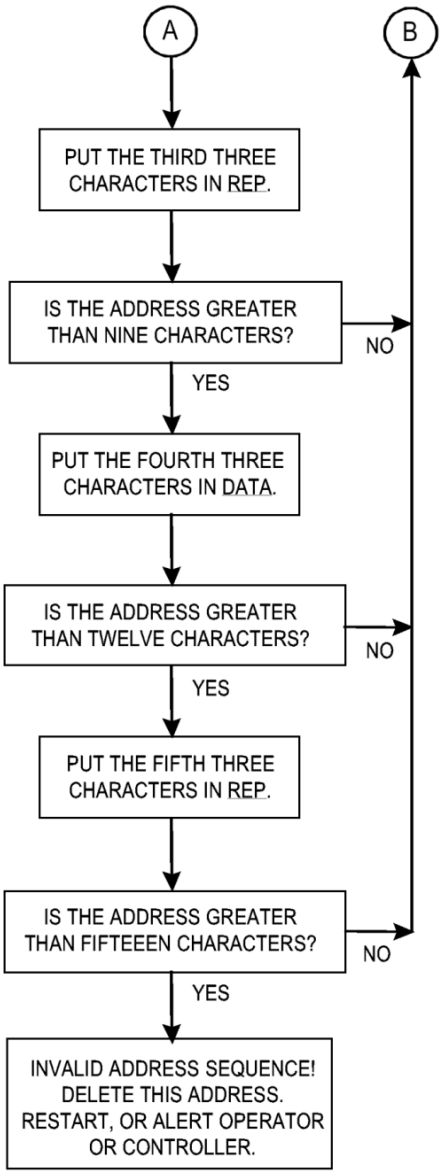


FIGURE A-15. Calling cycle sequence (continued).

A.5.2.5.2 Message section.
The second and optional section of all frames (except sounds) is termed a “message.” Except for the quick-ID, it shall be composed of CMD (and possibly REP and DATA) words from the end of the calling cycle until the start of the conclusion (thus the end of the message). The optional quick-ID shall be composed of FROM (and possibly REP and DATA) word(s), containing the transmitter’s whole address. It shall only be used once at the start of the CMD message section sequences. The quick-ID enables prompt transmitter identification and should be used if the message section length is a concern. It is never used without a following (CMD...) message(s). The message section shall always start with the first CMD (or FROM with later CMD(s)) in the call. See figure A-16. The use of REP and DATA is described in A.5.7.3. The message section is not repeated within the call (although messages or information itself, within the message section, may be).

For AQC-ALE, the message section in AQC-ALE is available when in a link. The acknowledgement leg (third leg) of a call may be used as an inlink entry condition. See A.5.8.2.3.

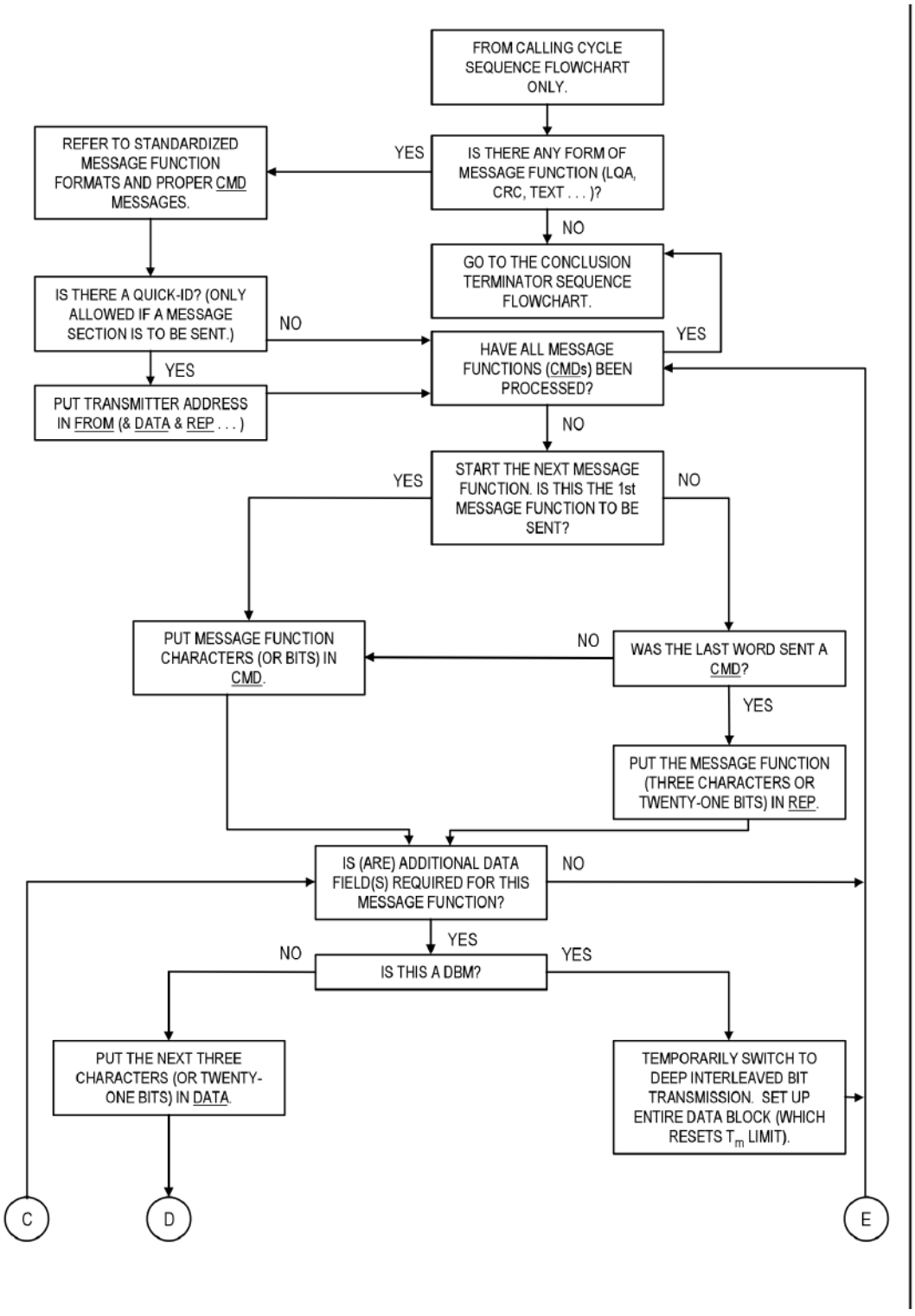


FIGURE A-16. Message sequence.

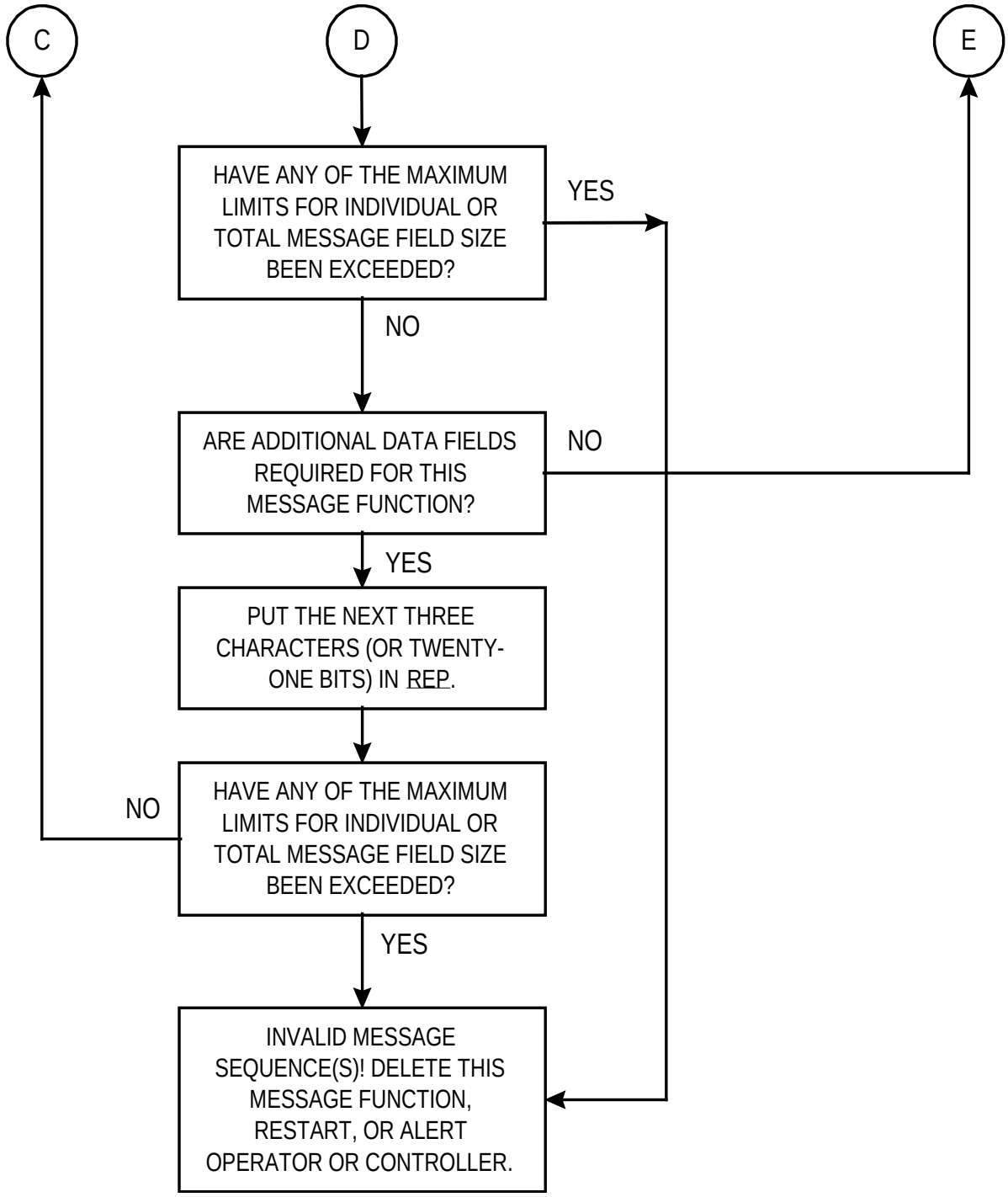


FIGURE A-16. Message sequence (continued).

A.5.2.5.3 Conclusion.
The third section of all frames is termed a “conclusion.” It shall be composed of either TIS or TWAS (but not both) (and possibly DATA and REP) words, from the end of the message (or calling cycle sections, if no message) until the end of the call. See figure A-17. Sounds and exception shall start immediately with TIS (or TWAS) words as described in A.5.3. REP shall not

immediately follow TIS or TWAS. Both conclusions and sounds contain the whole address of the transmitting station.

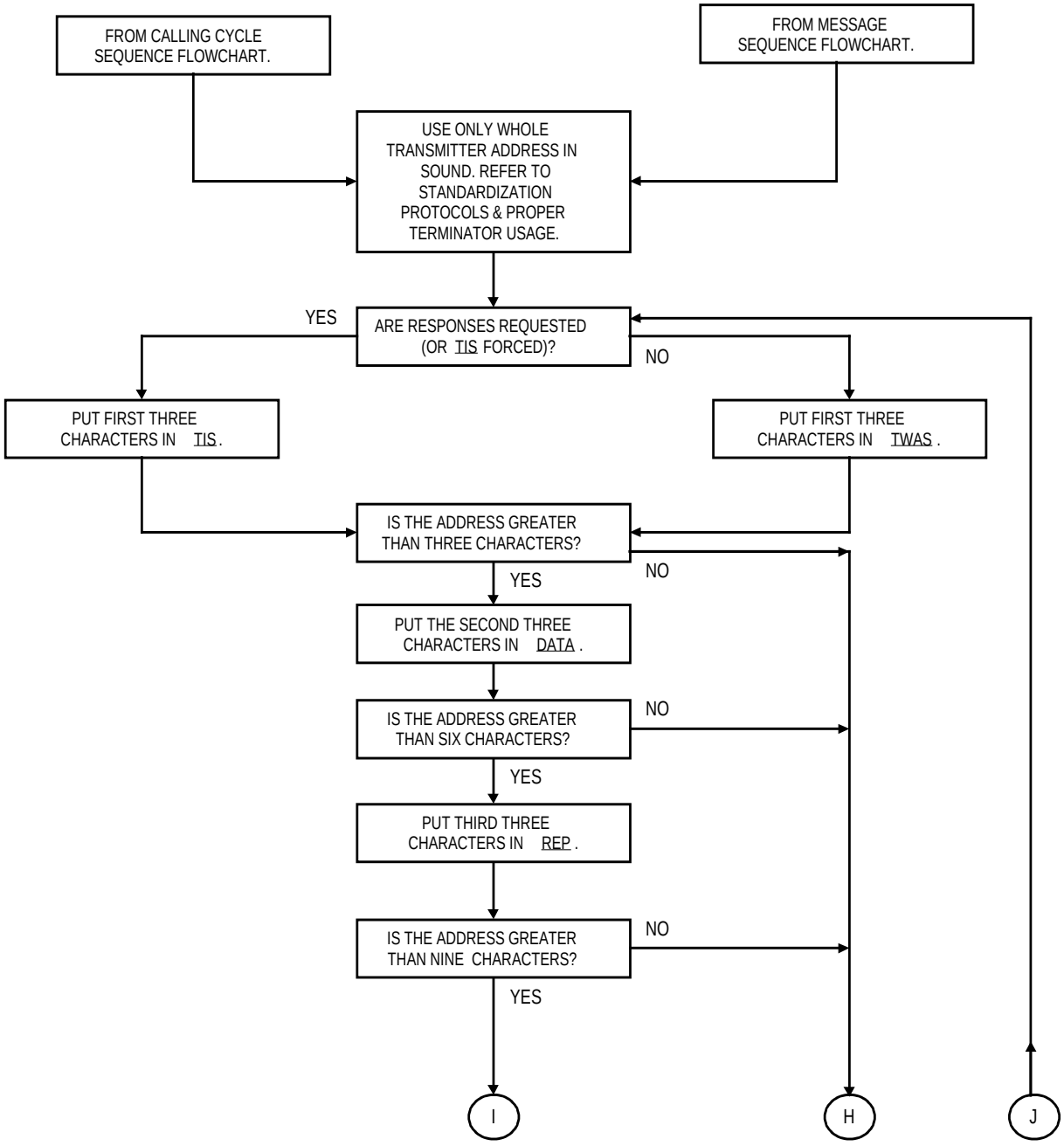


FIGURE A-17. Conclusion (terminator) sequences.

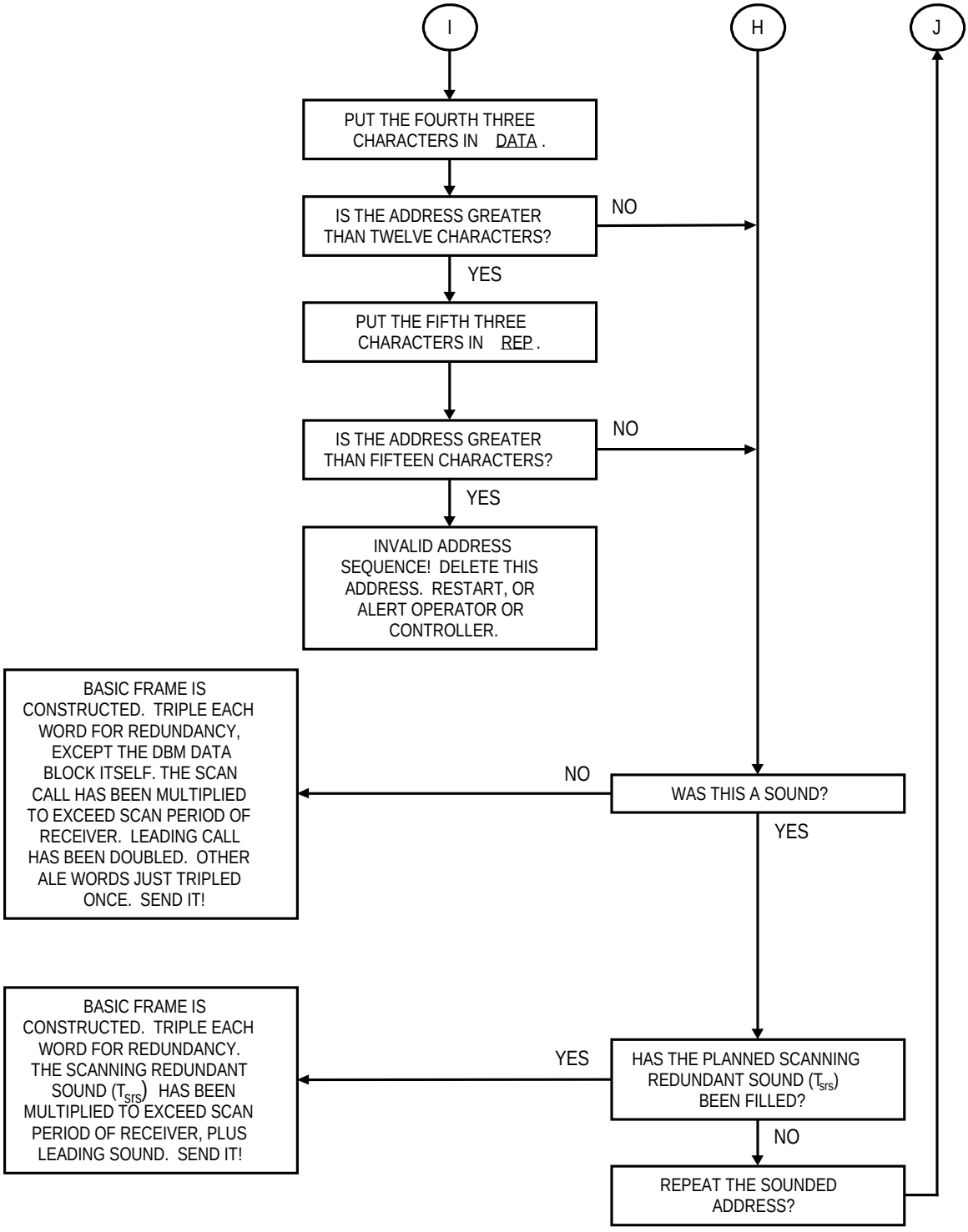


FIGURE A-17. Conclusion (terminator) sequences (continued).

A.5.2.5.4 Valid sequences.
The eight ALE words types that have been described shall be used to construct frames and messages only as permitted in figures A-18, A-19, and A-20. The size and duration of ALE frames, and their parts, shall be limited as described in table A-XII.

TABLE A-XII. Limits to frames.

Calls	Limit
Address size (5 words) ($T_{a\ max}$)	1960 ms
Call time maximum T_c (one-half of T_{lc} = 12 words $_{max}$)	4704 ms
Scan period ($T_{s\ max}$)	50 s
Message section basic time ($T_{m\ \ max}$ basic) (unless modified by AMD extension, or by CMD such as DTM or DBM)	11.76 s
Message section, time limit of AMD (90 characters) ($T_{m\ max}$ AMD)	11.76 s
Message section time, DTM (1053 characters) ($T_{m\ max}$ DTM)	2.29 min (entire data block)
Message section time, DBM (37377 characters) ($T_{m\ max}$ DBM)	23.26 min (entire deeply interleaved block)

A.5.2.5.5 Basic frame structure examples.
Contained in figure A-21 are basic examples (does not include the optional message section) of frame construction. Included are single-word and multiple-word examples of either single or multiple called station address(es) for non-scan (single-channel) and scanning (multiple-channel) use in individual, net, or group calls.

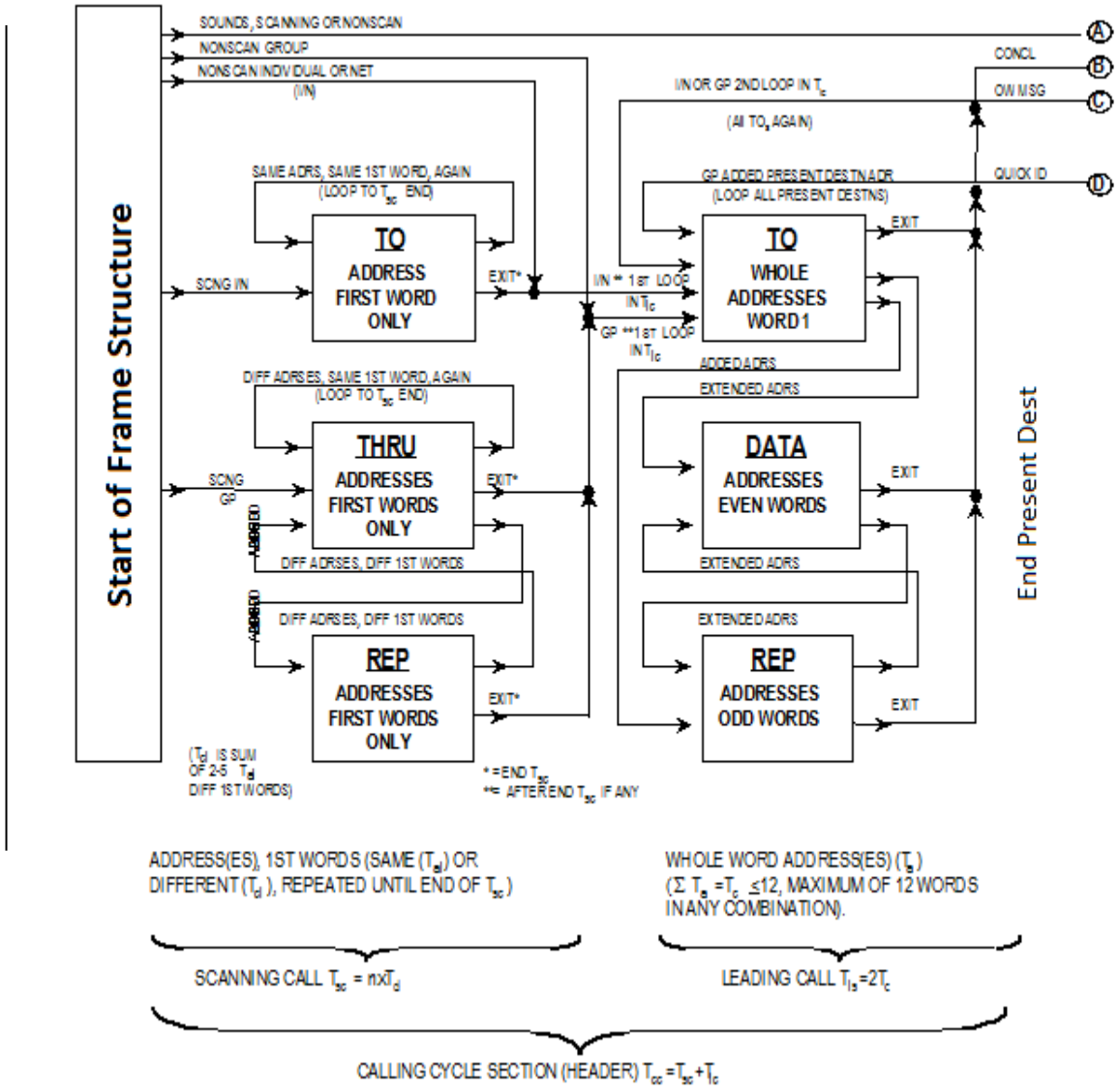


FIGURE A-18. Valid word sequence (calling cycle section).

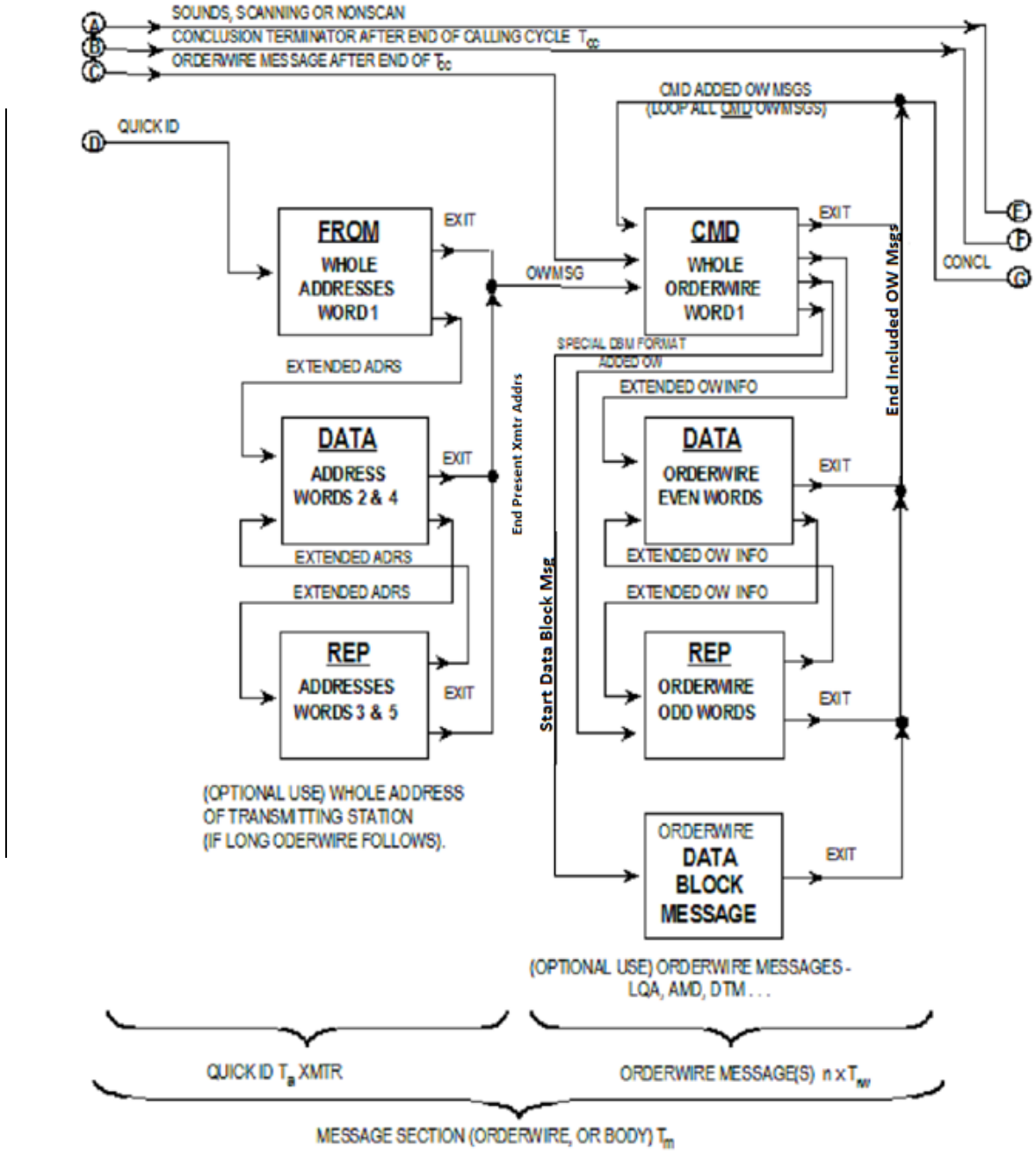


FIGURE A-19. Valid word sequence (message section).

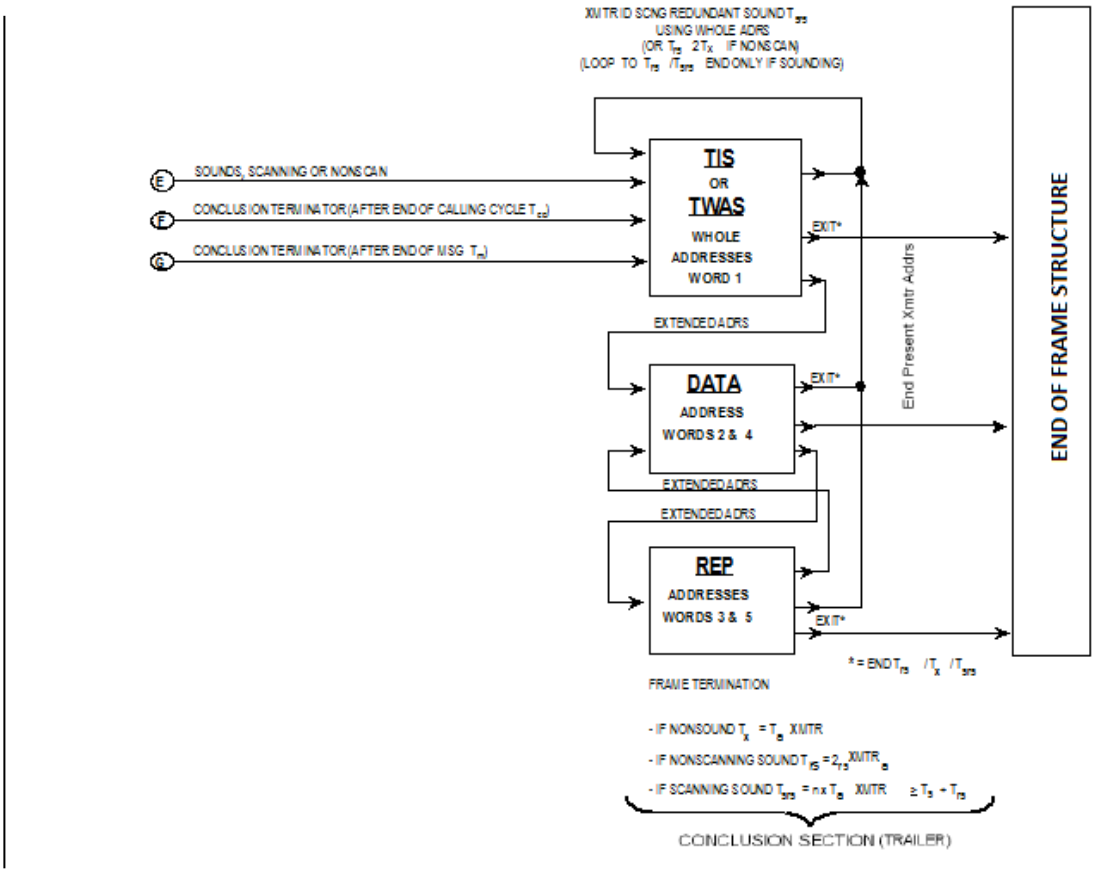
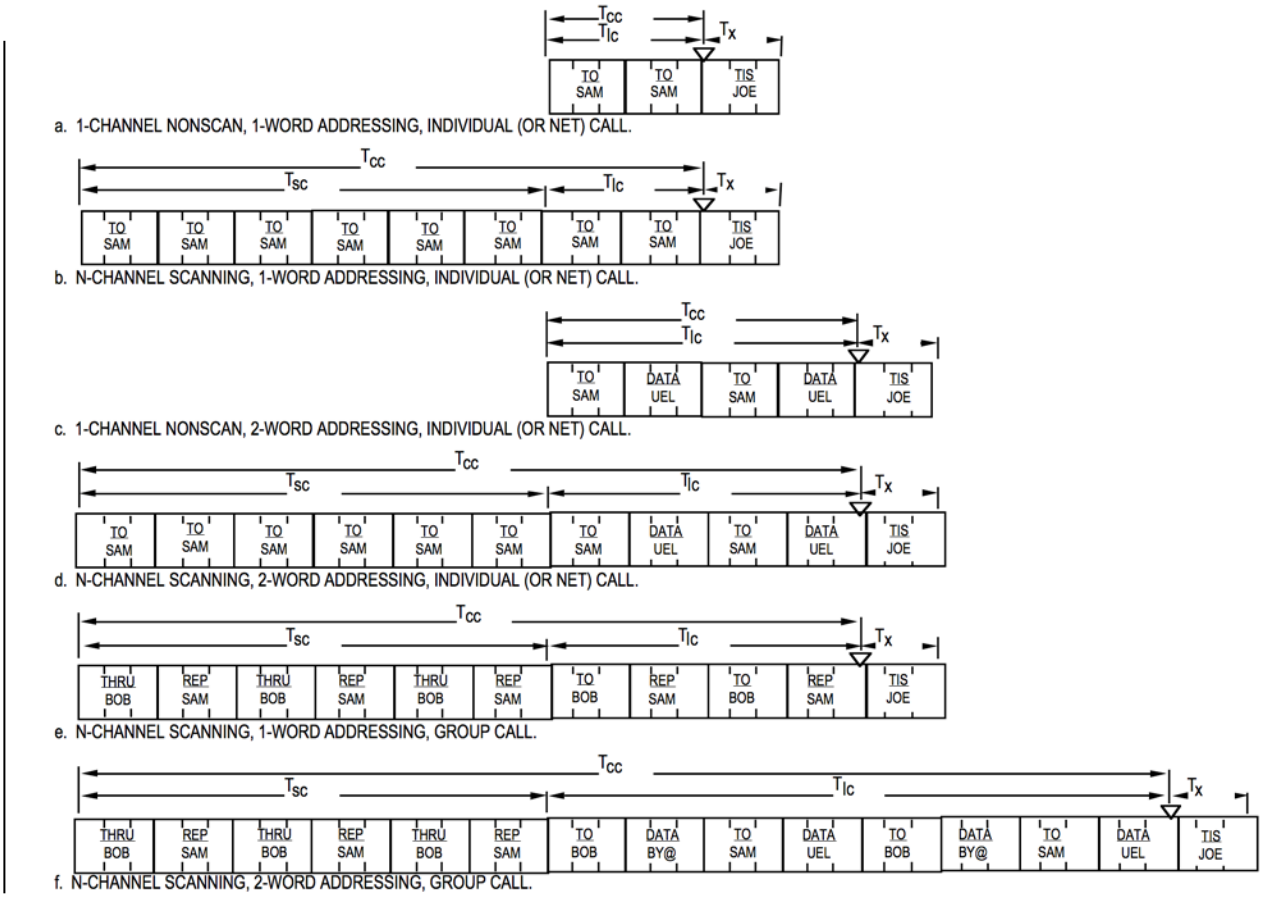


FIGURE A-20. Valid word sequence (conclusion section).



NOTE: ▽ denotes position of optional message section.

FIGURE A-21. Basic frame structure examples.

A.5.2.6 Synchronization.
The ALE system is inherently asynchronous and does not require any form of system synchronization, although it is compatible with such techniques. Within a frame, the imbedded timing and structure of the system provide the necessary “hooks” for achieving and maintaining word synchronization (word sync) during linking, orderwire, and anti-interference functions, as described herein.

A.5.2.6.1 Transmit word phase.
The ALE transmit modulator accepts digital data from the encoder and provides modulated baseband audio to the transmitter. The signal modulation is strictly timed as described in A.5.1.3 and A.5.1.4. After the start of the first transmission by a station, the ALE transmit modulator shall maintain a constant phase relationship, within the specified timing accuracy, among all transmitted triple redundant words at all times until the transmission is terminated. Specifically,

$$T_{(\text{later triple redundant word})} - T_{(\text{early triple redundant word})} = n \times T_{rw}$$

where $T_{(\ )}$ is the event time of a given triple redundant word within any frame, T_{rw} is the period of three words (392 ms), and n is any integer.

NOTE: Word phase tracking will only be implemented within a transmission and not between transmissions.

The internal word phase reference of the transmit modulator shall be independent of the receiver (which tracks incoming signals) and shall be self timed (within its required accuracy). See A.5.1.4.

A.5.2.6.2 Receiver word sync.
The receive demodulator accepts baseband audio from the receiver; acquires, tracks, and demodulates ALE signals; and provides the recovered digital data to the decoders. See figure A-11. In data block message (DBM) mode, the receive demodulator shall also be capable of reading single data bits for deep deinterleaving and decoding.

A.5.2.6.3 Synchronization criteria.
The decoder accepts digital data from the receive demodulator and performs deinterleaving, decoding, FEC, and data checking. During initial and continuing synchronization, all of the following criteria should be used to discriminate and read every ALE word:

- Must meet or exceed a threshold of unanimous votes in the 2/3 majority voter decoder
- Successful Golay decode of "A" word bits
- Successful Golay decode of "B" word bits
- Acceptable preamble according to valid word sequences as shown in figure A-14
- Acceptable first character bits (of Basic 38 ASCII subset)
- Acceptable second character bits (of Basic 38 ASCII subset)
- Acceptable third character bits (of Basic 38 ASCII subset)
- History, status, expectations, and protocol
- Correct triple redundant word phase

The number of unanimous votes provides an easily adjustable BER signal quality discrimination, and the threshold should be chosen by the manufacturer to optimize performance. A successful Golay decode indicates that all detected bit errors were corrected within the power of the FEC code; that is, the errors were within correctable limits and therefore, the uncorrectable error flag(s) did not occur. The correction power (mode) of the Golay code should be chosen by the manufacturer to optimize performance using any of the four modes: (3/4, 2/5, 1/6, 0/7) where n/m indicates up to "n" errors detected and corrected, or up to "m" errors detected but not correctable. Acceptable preambles, as described here and defined in A.5.2.3.1.3, refer to those preambles which are within the limits of this standard. As a DO, automatic adjustment of the unanimous vote threshold and Golay mode should be provided to optimize performance under varying conditions.

NOTE: The application of each preamble is dependent on the recent signaling history of the stations heard, the active status of the machine, the handshake(s) expected, and the protocol being used, if any. For example, an uncommitted station, awaiting calls, would accept TO if individual or net call (and possibly THRU or REP if group call) as valid preambles for calls to it. It would reject CMD as being irrelevant (because it missed the preceding and required calling cycle T_{CC}). It might also reject TIS or TWAS (unless collecting sounding information). Acceptable characters mean that each character is within the appropriate ASCII subset. Note that all criteria, together, must be satisfied to accept a word. For example, all three characters would have to be within the Basic 38 ASCII subset if a routing preamble

such as a TO was decoded. Likewise, any bit combination would be conditionally acceptable if an initial REP was received, but in most cases, without the necessary knowledge of the previous word, it would be considered irrelevant and should be rejected.

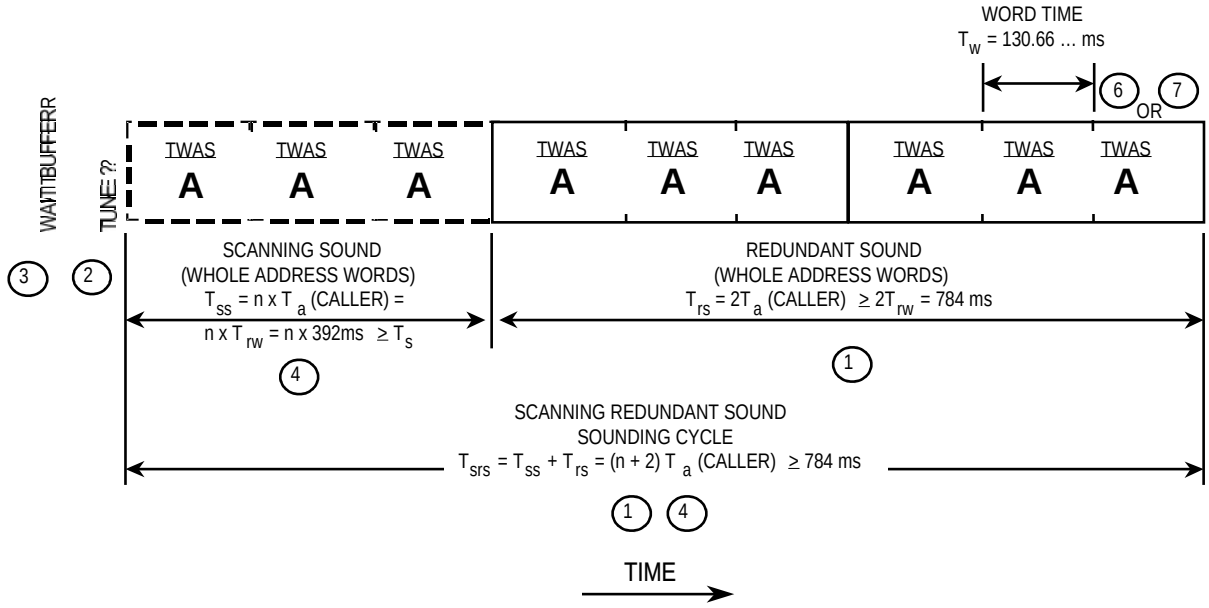
A.5.3 Sounding.

A.5.3.1 Introduction.
The sounding signal is a unilateral, one-way transmission performed at periodic intervals on unoccupied channels. To implement, a timer is added to the controller to periodically initiate sounding signals (if the channel is clear). Sounding is not an interactive, bilateral technique, such as polling. However, the identification of connectivity from a station by hearing its sounding signal does indicate a high probability (but not guarantee) of bilateral connectivity and it may be done passively at the receiver. Sounding uses the standard ALE signaling, any station can receive sounding signals. As a minimum, the signal (address) information shall be displayed to the operator and, for stations equipped with connectivity and LQA memories, the information shall be stored and used later for linking. If a station has had recent transmissions on any channels that are to be sounded on, it may not be necessary to sound on those channels again until the sounding interval, as restarted from those last transmissions, has elapsed. In addition, if a net (or group) of stations is polled, their responses shall serve as sounding signals for the other net (or group) receiving stations. All stations shall be capable of performing periodic sounding on clear prearranged channels. The sounding capability may be selectively activated by, and the period between sounds shall be adjustable by the operator or controller, according to system requirements. When available, and not otherwise committed or directed by the operator or controller, all ALE stations shall automatically and temporarily display the addresses of all stations heard, with an operator selectable alert.

The structure of the sound is virtually identical to that of the basic call; however, the calling cycle is not needed and there is no message section. It is only necessary to send the conclusion (terminator) that identifies the transmitting station. See figure A-22. The type of word, either TIS or TWAS (but never both), indicates whether potential callers are encouraged or ignored, respectively. The minimum redundant sound time (T_{rs}) is equal to the standard one-word address leading call time (T_{lc})=784 ms. Described below are both single-channel and multiple-channel protocols, plus detailed timing and control information, for designing stations.

A.5.3.2 Single channel.
The fundamental capability to automatically sound on a channel shall be in accordance with the sounding protocol as shown in figure A-22. As an option, stations may employ this protocol for single-channel sounding, connectivity tracking, and the broadcast of their availability for calls and traffic. The basic protocol consists of only one part: the sound. The sound contains its own address (“TIS A”). If “A” is encouraging calls and receives one, “A” shall follow the sound with the optional handshake protocol described in A.5.3.4. If “A” plans to ignore calls, it shall use the TWAS, which advises “B” and the others not to attempt calls, and then “A” shall immediately return to normal “available.” In some systems it is necessary for a multichannel station “A” to periodically sound to a single-channel network, usually to inform them that he is active and available on that channel, although scanning. Upon receipt of “A’s” sound, “B” (see figure A-23) and the other stations shall display “A’s” address as a received sound and, if they have an LQA and connectivity memory, they shall store the connectivity information.

A.5.3.3 Multiple channels.
Sounding must be compatible with the scanning timing. All stations shall be capable of performing the scanning sounding protocols described herein, even if operating on a fixed frequency. See figures A-22, A-23, and A-24. These protocols establish and positively confirm unilateral connectivity between stations on any available mutually scanned channel, and they assist in establishment of links between stations waiting for contact. Stations shall employ these protocols for multichannel sounding, connectivity tracking, and the broadcast of their availability for calls and traffic.



1. SINGLE-CHANNEL (AND MULTIPLE-CHANNEL) EXAMPLES SHOWN WITH ONE WORD ADDRESSES.
2. TUNING REQUIRED INITIALLY (T_t).
3. WAIT (LISTEN TIME) (T_{wt}).
4. SOUNDING CYCLE (T_{srs}) DEPENDS ON SCAN PERIOD (T_s).
   - T_{srs} -USE WHOLE ADDRESS ONLY.
   - T_{ss} (OPTIONAL IF NONSCAN).
6. TWAS INDICATES CALL REJECTION.
7. TIS INDICATES CALL ACCEPTANCE (A WILL PAUSE AFTERWARDS).

NOTE: 5 DOES NOT APPLY TO THIS FIGURE.

FIGURE A-22. Basic sounding structure.

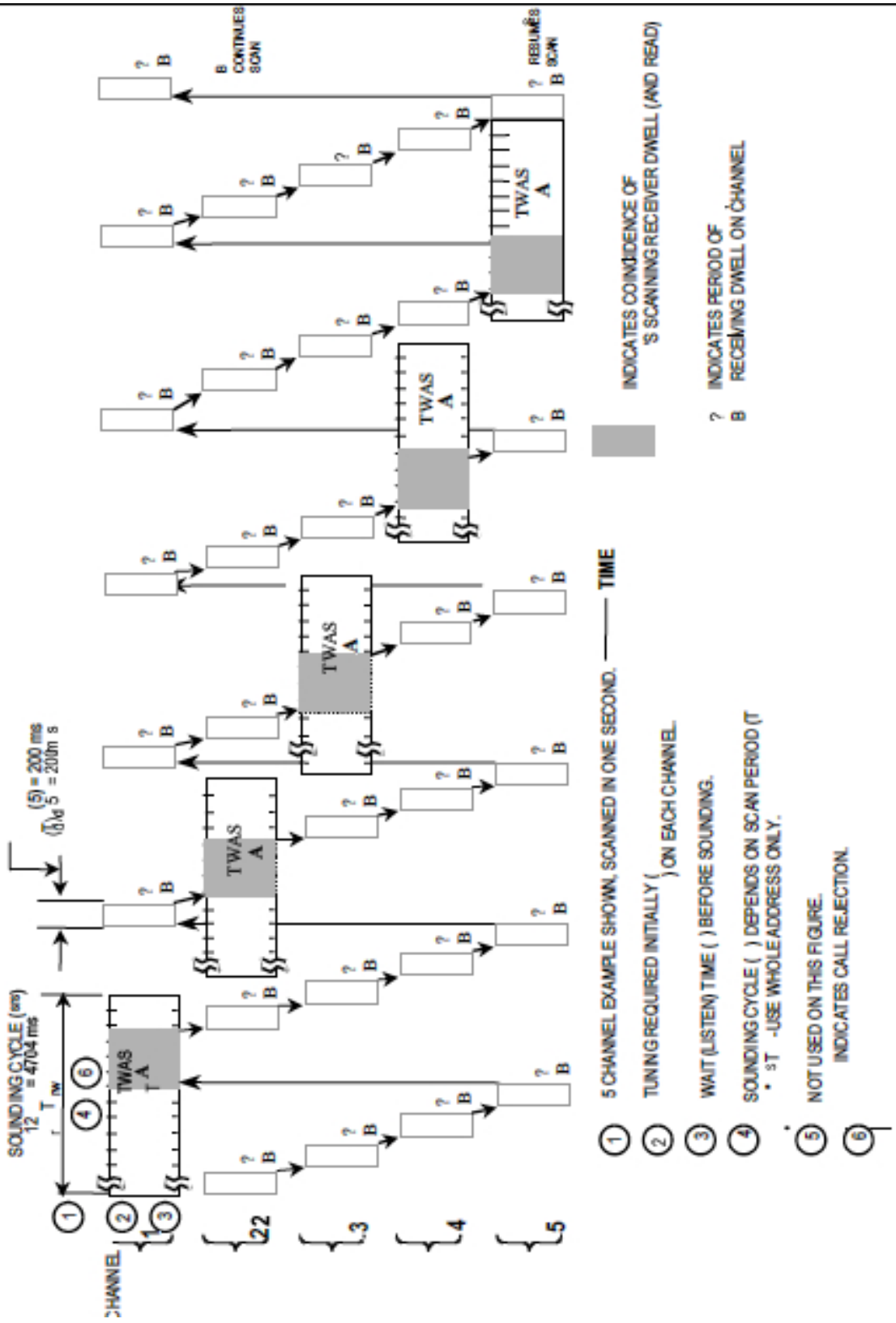


FIGURE A-23. Call rejection scanning sounding protocol.

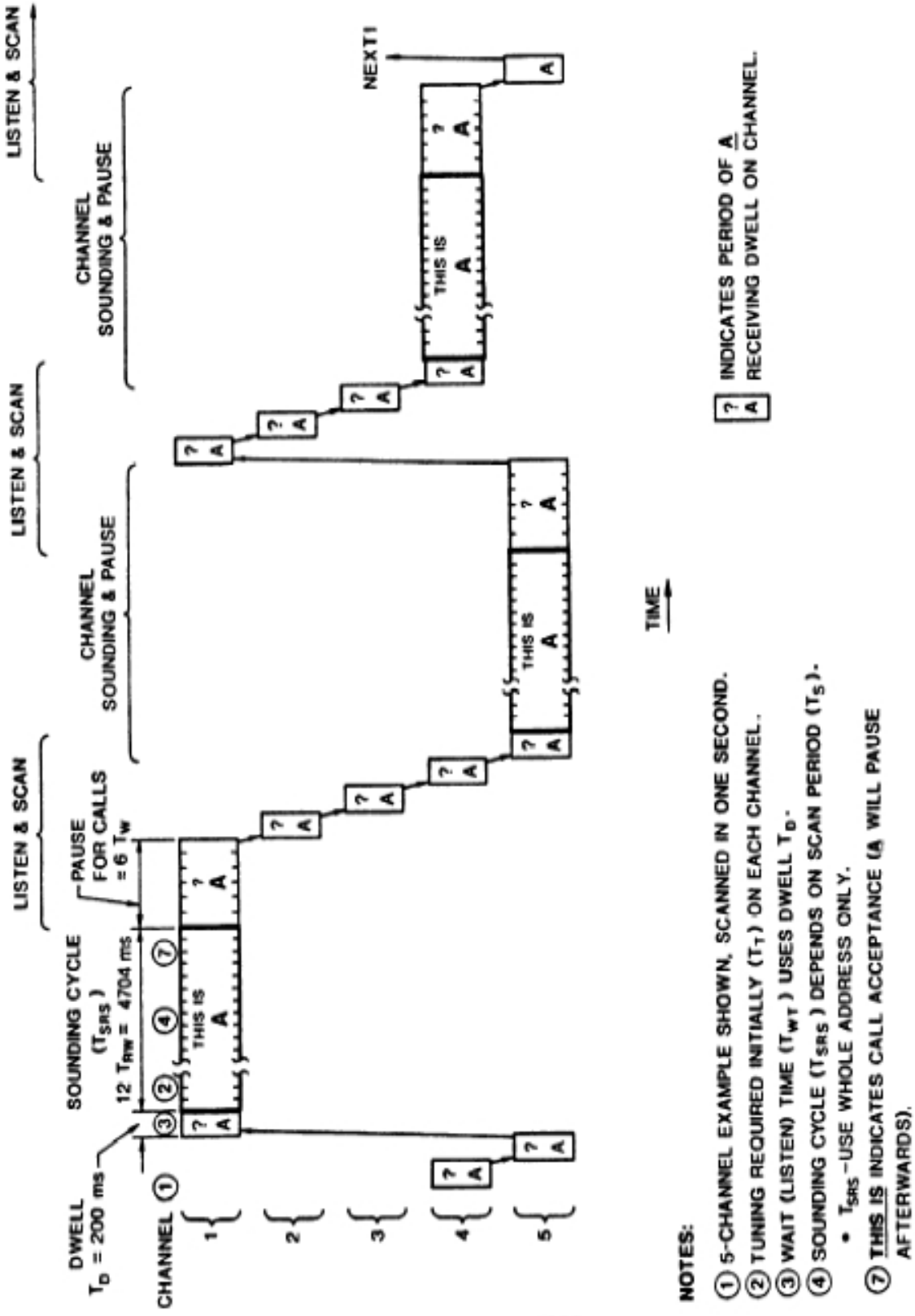


FIGURE A-24. Call acceptance scanning sounding protocol.

All timing considerations and computations for individual scanning calling shall apply to scanning sounding, including sounding cycle times and (optional) handshake times.

NOTE: The scanning sound is identical to the single-channel sound except for the extension of the redundant sound time (T_{rs}) by adding words to the scan sounding time (T_{ss}) to form a scanning redundant sound time (T_{srs}); that is $T_{srs} = T_{ss} + T_{rs}$. The scan sounding time (T_{ss}) is identical in purpose to the scan calling time (T_{sc}) for an equivalent scanning situation, but it only uses the whole address of the transmitter.

The channel-scanning sequences and selection criteria for individual scanning calling shall also apply to scanning sounding. The channels to be sounded are termed a "sound set," and usually are identical to the "scan set" used for scanning. See figure A-23. In this illustration, station "A" is sounding and station "B" is scanning normally. If a station "A" plans to ignore calls (from "B"), which may follow "A's" sound, the following call rejection scanning sounding protocol shall be used. In a manner identical to the previously described individual scanning call, "A" lands on the first channel in the scan set (1), waits (T_{wt}) to see if the channel is clear (3), tunes (T_t) its coupler, comes to full power, and initiates the frame of the scanning redundant sound times (T_{srs}). This scanning sound is computed to exceed "B's" (and any others) scan period (T_s) by at least a redundant sound time (T_{rs}), which will ensure an available detection period exceeding T_{drw} = 784 ms. In this five-channel example, with "B" scanning at 5 chps, "A" sounds for at least 12 T_{rw} (4704 ms). "A" also uses "TWAS A," redundantly to indicate that calls are not invited. Upon completion of the scanning sounding frame transmission, "A" immediately leaves the channel and goes to the next channel in the sound set. (DO: "A" should perform a complete channel scan, listening for incoming calls, between sending sounds. This improves the ability for other stations to reach "A" during what would otherwise be an extended period of unavailability.) This procedure repeats until all channels have been sounded, or skipped if occupied. When the calling ALE station has exhausted all the prearranged sound set channels, it shall automatically return to the normal "available" receive scan mode. As shown in figure A-23, the timing of both "A" and "B" have been prearranged to ensure that "B" has at least one opportunity, on each channel, to arrive and "capture" "A's" sound. Specifically, "B" arrives, detects sounds, waits for good words, reads at least three (redundant) "TWAS A" (in 3 to 4 T_w), stores the connectivity information (if capable), and departs immediately to resume scan.

There are several specific protocol differences when station "A" plans to welcome calls after the sound. See figure A-24. In this illustration, "A" is sounding and "B" is scanning normally. If station "A" plans to welcome calls (from "B"), which may follow his sound, the following call acceptance scanning sounding protocol shall be used. In this protocol, "A" sounds for the same time period as before. However, since "A" is receptive to calls, he shall use his normal scanning dwell time (T_d) or his preset wait before transmit time (T_{wt}), whichever is longer, to listen for both channel activity and calls before sounding. If the channel is clear, "A" shall initiate the scanning sound identically to before, but with "TIS A." At the end of the sounding frame, "A"

shall wait for calls identically to the wait for reply and tune time (T_{wrt}) in the individual scanning calling protocol, in this case shown to be 6 T_w (for fast-tuning stations). During this wait, "A" shall (as always) be listening for calls that may coincidentally arrive even though unassociated with "A's" sound, plus any other sound heard, which "A" shall store as connectivity information if polling-capable. If no calls are received, "A" shall leave the channel.

A.5.3.4 Optional handshake.

In the previous descriptions, one alternative action is the implementation of an optional handshake with a station immediately after its sound. This protocol is identical in all regards to the single channel individual call protocol, except that it is manually or automatically (operator or controller) triggered by acquisition of connectivity from the station that is to be called. See figure A-25. In this illustration, "A" is scanning sounding and is receptive to calls, and "B" is receive scanning (or waiting in ambush on a channel) and requires contact with "A" if heard. "A" uses the standard call acceptance scanning sound, including the "TIS A" and the pause for calls. In this case "B" calls "A." When ALE stations are scanning sounding and receptive to calls, or required contact with such a station, the optional handshake protocol should be used. The calling station should immediately initiate the call upon the determination that the station to be called has terminated its transmission. A wait time before transmit time is not required. Therefore, if "B" hears "A's" sound and is seeking "A," "B" calls immediately using the simple single-channel call. Also, if "B's" operator or controller identifies "A's" address it can attempt the optional handshake.

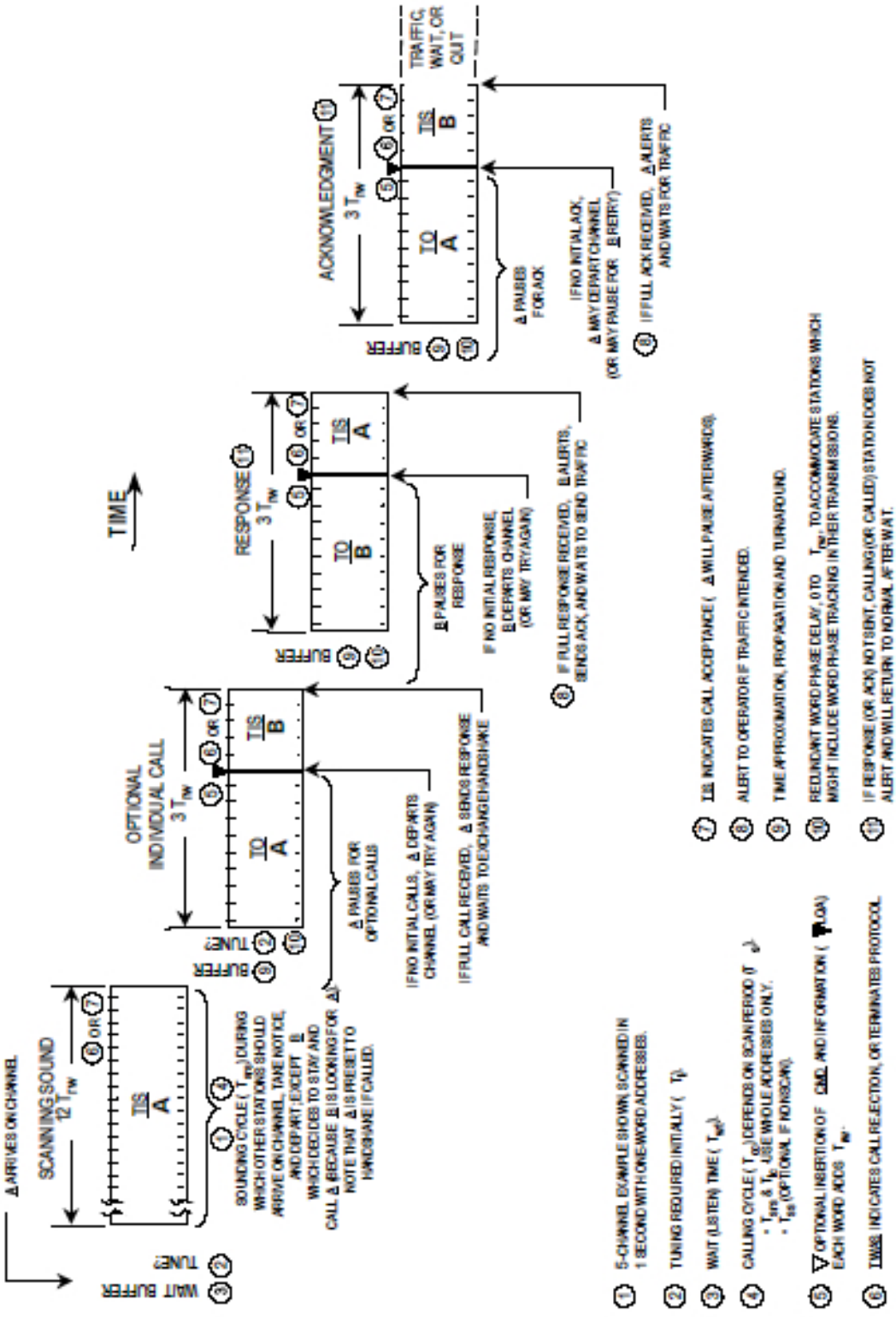


FIGURE A-25. Scanning sounding with optional handshake protocol.

A.5.4 Channel selection.
Channel selection is based on the information stored within the LQA memory (such as BER, SINAD, and MP) and this information is used to speed connectivity and to optimize the choice of quality channels. When initiating scanning (multichannel) calling attempts, the sequence of channels to be tried shall be derived from information in the LQA memory with the channel(s) with the "best score(s)" being tried first (unless otherwise directed by the operator or controller) until all the LQA scored channels are tried. However, if LQA or other such information is unavailable (or it has been exhausted and other valid channels remain available and untried) the station shall continue calling on those channels until successful or until all the remaining (untried valid) channels have been tried.

A.5.4.1 LQA.
LQA data shall be used to score the channels and to support selection of a "best" (or an acceptable) channel for calling and communication. LQA shall also be used for continual monitoring of the link(s) quality during communications that use ALE signaling. The stored values shall be available to be transmitted upon request, or as the network manager shall direct. Unless specifically and otherwise directed by the operator or controller, all ALE stations shall automatically insert the CMD LQA word (□) in the message section of their signals and handshakes when requested by the handshaking station(s), when prearranged in a network, or when specified by the protocol. See A.5.4.2. If an ALE station requires, and is capable of using LQA information (polling-capable), it may request the data from another station by setting the control bit KA1 to "1" in the CMD LQA word. If an ALE station, which is sending CMD LQA in response to a request is incapable of using such information itself (not polling-capable), it shall set the control bit KA1 to "0." It will be a network management decision to determine if the LQA is to be active or passive. For human factor considerations, LQA scores that may be presented to the operator should have higher (number) scores for better channels.

A.5.4.1.1 BER.
Analysis of the BER on rf channels, with respect to poor channels and the 8-ary modulation, plus the design and use of both redundancy and Golay FEC, shows that a coarse estimate of BER may be obtained by counting the number of non-unanimous (2/3) votes (out of 48) in the majority vote decoder. The range of this measure is 0 through 48. Correspondence to actual BER values is shown in table A-XIII.

After an ALE receiver achieves word synchronization (see A.5.2.6.2), all received words in a frame shall be measured, and a linear average BER/LQA shall be computed as follows:

- If the Golay decoder reports no uncorrectable errors in both halves of the ALE word, the number of non-unanimous votes detected in the word shall be added to the total.
- If at least one half of the ALE word contained uncorrectable errors, the number of non-unanimous votes detected shall be discarded, and 48 (the maximum value) shall be added to the total.

At the end of the transmission, the total shall be divided by the number of words received, and the total shall be stored in the Link Quality Memory as the most current BER code for the station sending the measured transmission and the channel that carried it.

A.5.4.1.2 SINAD.
The signal to noise and distortion measurement shall be a SINAD measurement ((S+N+D)/(N+D)) averaged over the duration of each received ALE signal. The SINAD values shall be measured on all ALE signals.

A.5.4.1.3 MP (optional).
Measurement of MP using received ALE signals is optional.

A.5.4.1.4 Operator display (optional).
Display of SINAD values shall be in dB.

A.5.4.2 Current channel quality report (LQA CMD).
This mandatory function is designed to support the exchange of current LQA information among ALE stations. The CMD LQA word shall be constructed as shown in table A-XIV The preamble shall be CMD (110) in bits P3 through P1 (W1 through W3). The first character shall be "a" (1100001) in bits C1-7 through C1-1 (W4 through W10), which shall identify the LQA function "analysis." It carries three types of analysis information (BER, SINAD, and MP) which are separately generated by the ALE analysis capability. Note that when the control bit KA1 (W11) is set to "1," the receiving station shall respond with an LQA report in the handshake. If KA1 is set to "0," the report is not required.

A.5.4.2.1 BER field in LQA CMD.
Measurement and reporting of BER is mandatory. The BER field in the LQA CMD shall contain five bits of information, BE5 through BE1 (W20 through W24). Refer to table A-XIII for the assigned values.

A.5.4.2.2 SINAD.
SINAD shall be reported in the CMD LQA word as follows. The SINAD is represented as five bits of information SN5 through SN1 (W15 through W19). The range is 0 to 30 dB in 1-dB steps. 00000 is 0 dB or less, and 11111 is no measurement.

A.5.4.2.3 MP.
If implemented, MP measurements shall be reported in CMD LQA words in the three bits, MP3 through MP1 (W12 through W14). The measured value in ms shall be reported rounded to the nearest integer, except that values greater than 6 ms shall be reported as 6 (110). When MP is not measured, the reported MP value shall be 7 (111).

TABLE A-XIII. Approximate BER values.

LQA Transmission Bits						
Average 2/3 Votes Counted	**MSB**				**LSB**	**Approximate BER**
	BE5	BE4	BE3	BE2	BE1	
0	0	0	0	0	0	0.0
1	0	0	0	0	1	0.006993
2	0	0	0	1	0	0.01409
3	0	0	0	1	1	0.02129
4	0	0	1	0	0	0.02860
5	0	0	1	0	1	0.03602
6	0	0	1	1	0	0.04356
7	0	0	1	1	1	0.05124
8	0	1	0	0	0	0.05904
9	0	1	0	0	1	0.06699
10	0	1	0	1	0	0.07508
11	0	1	0	1	1	0.08333
12	0	1	1	0	0	0.09175
13	0	1	1	0	1	0.1003
14	0	1	1	1	0	0.1091
15	0	1	1	1	1	0.1181
16	1	0	0	0	0	0.1273
17	1	0	0	0	1	0.1368
18	1	0	0	1	0	0.1464
19	1	0	0	1	1	0.1564
20	1	0	1	0	0	0.1667
21	1	0	1	0	1	0.1773
22	1	0	1	1	0	0.1882
23	1	0	1	1	1	0.1995
24	1	1	0	0	0	0.2113
25	1	1	0	0	1	0.2236
26	1	1	0	1	0	0.2365
27	1	1	0	1	1	0.2500
28	1	1	1	0	0	0.2643
29	1	1	1	0	1	0.2795
30 (or more)	1	1	1	1	0	0.3 (or more)
- -	1	1	1	1	1	no value available

TABLE A-XIV. Link quality analysis structure.

	LQA Bits		Word Bits	
CMD Preamble	MSB	P3=1	MSB	W1
		P2=1		W2
		P1=0		W3
First Character "a"	MSB	C1-7=1		W4
		C1-6=1		W5
		C1-5=0		W6
		C1-4=0		W7
		C1-3=0		W8
		C1-2=0		W9
	LSB	C1-1=1		W10
Control		KA1		W11
MP Bits	MSB	MP3		W12
		MP2		W13
	LSB	MP1		W14
SINAD Bits	MSB	SN5		W15
		SN4		W16
		SN3		W17
		SN2		W18
	LSB	SN1		W19
BER Bits	MSB	BE5		W20
		BE4		W21
		BE3		W22
		BE2		W23
	LSB	BE1	LSB	W24

NOTES:
1. Command LQA first character is "a" (1100001) for "analysis."
2. Control bit KA1 (W11) requests an LQA within the handshake from the called station, if set to "1," and suppresses LQA if set to "0."

A.5.4.4 Local noise report CMD (optional).

The Local Noise Report CMD provides a broadcast alternative to sounding that permits receiving stations to approximately predict the bilateral link quality for the channel carrying the report. An example application of this optional technique is networks in which most stations are silent but need to have a high probability of linking on the first attempt with a base station. A station receiving a Local Noise Report can compare the noise level at the transmitter to its own local noise level, and thereby estimate the bilateral link quality from its own LQA measurement of the received noise report transmission. The CMD reports the mean and maximum noise power measured on the channel in the past 60 minutes.

The Local Noise Report CMD shall be formatted as shown in figure A-26. Units for the Max and Mean fields are dB relative to 0.1 µV 3 KHz noise. 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 1s) is sent when no report is available for a field. 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 that destination.

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

FIGURE A-26. Local noise report (optional).

A.5.4.5 Single-station channel selection.
All stations shall be capable of selecting the (recent) best channel for calling or listening for a single station based on the values in the LQA memory.

A.5.4.5.1 Single-station channel selection for link establishment.
When selecting a channel for a two-way link, link quality measurements for both directions on each frequency must be considered. Figure A-27 represents a simple LQA memory example. For each address/channel cell, the measured LQA (upper section) and reported LQA values (lower section) are stored. Bilateral (handshake) scores in this example are the sum of the two LQA values.

NOTE 1: For operator viewing, LQA values for better channels should be displayed as higher numbers, and values for poorer channels should be displayed as lower numbers.

NOTE 2: In the example shown in figure A-27, if a handshake is required with station "B," channel C3 would be the best because the "round trip" (bilateral) score would be 5 (1+4), thus the lowest, channel C4 is next best with a score of 6 (3+3), the C5 with 7, C2 with 12, and C6 with 18. Linking attempts should be made in that order (C3, C4, C5, C2, and C6).

C1 is left until last because of the "x", which indicates that a recent attempted handshake on that channel failed to link. Similarly, an attempt to call "A" would yield the sequence C3(3), C5(12), C2(12), C1(24), C6(26), and C4(x). In this case, C5 was equal to C2 (both are 12), but C5 was chosen first because the paths were more balanced (LQA values were more equal).

ADDRESSES (OTHER STATIONS)			CHANNELS					
			C1	C2	C3	C4	C5	C6
	A	FROM	10	4	1	0	5	15
		TO	14	8	2	X	7	11
	B	FROM	9	5	1	3	2	6
		TO	X	7	4	3	5	12
	C	FROM	30	22	13	8	3	18
		TO	X	-	17	6	2	-
	D	FROM	1	2	5	12	20	-
		TO	-	4	7	15	21	-
	E	FROM	-	2	6	7	10	-
		TO	X	14	6	9	12	X

LQA SCORE

NOTES:
1. Upper value is LQA measurement on received signal from other stations.
2. Lower value is LQA measure on transmitted signal to other station as received and reported back.
3. Example shows range of 0 to 30 for LQA "scores," with a smaller value being better.
   - •LQA = "0" is excellent, ranging down to "30" which is very poor.
   - •LQA = "x" indicates none available after handshake attempt.
   - •LQA = "-" indicates none available but handshake not tried.

FIGURE A-27. LQA memory example.

A.5.4.5.2 Single-station channel selection for one-way broadcast.
If only a one-way transmission to a station is required instead of a handshake, the scores reported by the destination station (TO section in figure A-27) should be given greater weight than the scores measured on transmissions from that station.

NOTE: In the example, to reach "B," the sequence would be C4(3), C3(4), C5(5), C2(7), C6(12), and C1(x) as a last resort.

A.5.4.5.3 Single-station channel selection for listening.
When selecting a channel to listen for another station, the scores measured on transmissions from that station (FROM section in figure A-27) should be given greater weight than the scores reported by the destination station.

NOTE: In the example, to listen for "A," channel C4(0) would be best, and if only three channels were to be scanned, they should be C4, C3, and C2.

A.5.4.6 Multiple-station channel selection.
A station shall also be capable of selecting the (recent) best channel to call or listen for multiple stations, based on the values in the LQA memory.

NOTE: In the example shown in figure A-27, if a multiple-station handshake is required with stations "B" and "C," C5 is the best choice as the total score is 12 (2+5+3+2), followed by C4 (20) and C3 (35). Next would be C2 (34+) and C6 (36+), this ranking being due to their unknown handshake capability (which had not been tried). C1(x) is the last to be tried because recent handshake attempts had failed for both "B" and "C." To call the three stations "A," "B," and "C," the sequence would be C5 (24), C3 (38), C2 (46+), C6 (62+), C4 (one x) (recently failed attempt), and finally C1 (two x).

If an additional selection factor is used, it will change the channel selection sequence.

NOTE: In the example, to call "D" and "E," the sequence would be C2, C3, C4, C5, C1, and C6. If a maximum limit of LQA $\leq$ 14 is imposed on any path (to achieve a minimum circuit quality), only C2 and C3 would be initially selected for the linking attempt. Further, if the LQA limit was "lowered" to 10, C3 would be selected before C2 for the linking attempt.

If a broadcast to multiple stations is required, the TO section ("to" the station) scores are given priority.

NOTE: In the example, to broadcast to "B" and "C," the sequence would be C5(7), C4(9), C3(21), C2(7+), C6(12+), and C1(two x).

To select channels for listening for multiple stations, the FROM section ("from" the station) scores are given priority.

NOTE: In the example, to listen for "A" and "B," channel C2 (2) would be best, and if only four channels could be scanned, they should be C2, C3, C4, and C5.

A.5.4.7 Listen before transmit.
Before initiating a call or a sound on a channel, an ALE controller shall listen for a programmable time (T_{wt}) for other traffic, and shall not transmit on that channel if traffic is detected. Normally, a sound aborted due to detected traffic will be rescheduled, while for a call another channel shall be selected.

A.5.4.7.1 Listen-before-transmit duration.
The duration of the listen-before-transmit pause shall be programmable by the network manager. When the selected channel is known to be used only for ALE transmissions, the listen-before-transmit delay need be no longer than 2 T_{rw}. For other channels, at least 2 seconds shall be used. When an ALE controller was already listening on the channel selected for a transmission, the time spent listening on the channel may be included in the listen-before-transmit time.

A.5.4.7.2 Modulations to be detected.
The listen-before-transmit function shall detect traffic on a channel in accordance with A.4.2.2. This may be accomplished using any combination of internal signal detection and external devices that provide a channel busy signal to the ALE controller.

A.5.4.7.3 Listen before transmit override.
The operator shall be able to override both the listen-before-transmit pause and the transmit lockout (for emergency use).

A.5.5 Link establishment protocols.
An ALE controller shall control an attached HF SSB radio to support both manual and automatic link operation as described in the following paragraphs.

A.5.5.1 Manual operation.
The ALE controller shall support emergency control by the operator. Each ALE controller shall provide a manual control capability to permit an operator to directly operate the basic SSB radio in emergency situations. At all other times, the radio shall be under automated control, and the operator should operate the radio through its associated controller. The ALE controller's receiving and passive collection capability to be "always listening," such as monitoring for sounding signals or alerting the operator, shall not be impaired.

NOTE: This does not abrogate the manual push-to-talk operation required by 4.2.2.

A.5.5.2 ALE.
The fundamental protocol exchange for link establishment shall be the three-way handshake. A three-way handshake is sufficient to establish a link between a calling station and a responding station. With the addition of slotted responses (described in A.5.5.4.2), the same call/response/acknowledgment sequence can also link a single calling station to multiple responding stations.

A.5.5.2.1 Timing.
The ALE system depends on a selection of timing functions for optimizing the efficiency and effectiveness of ALE. The primary timing functions and values as listed in table A-XV. Annex A defines the timing symbols and Annex B explains the timing analysis and computation.

A.5.5.2.2 ALE states.
An ALE controller may be referred to as being in one of three conceptual "states." See figure A-28.

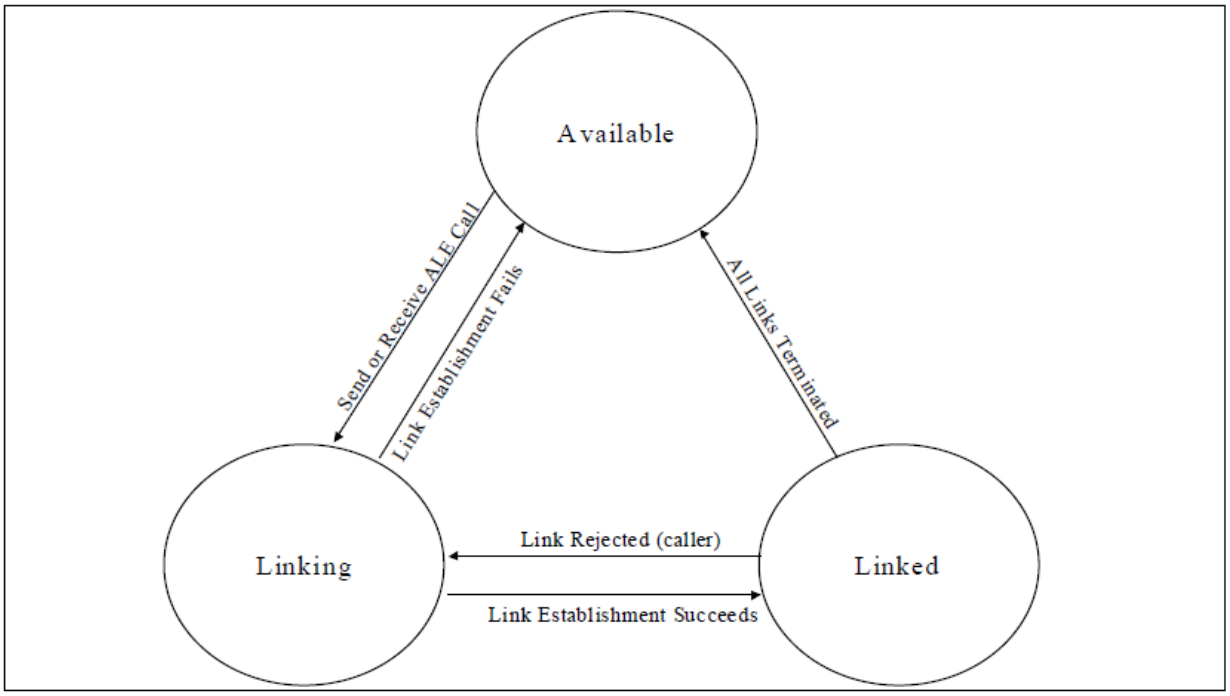


FIGURE A-28. Link establishment states.

A.5.5.2.3 ALE channel selection.
A scanning calling station shall send ALE calls on its scanned channels in the order dictated by its channel selection algorithm. It shall link on the first channel it tries that supports a handshake with the called station(s).

A.5.5.2.3.1 Rejected channel.
If a channel is rejected after linking by the operator or controller as unsuitable, the ALE controller shall terminate the link in accordance with A.5.5.3.5 and shall update LQA data using measurements obtained during linking.

A.5.5.2.3.2 Busy channel.
During the scanning-calling cycle, a caller may encounter occupied channels and shall skip them to avoid interference to traffic and activity. After all available channels have been tried, if no contact has been successful, the caller should revisit the previously occupied channels and, if they are free, attempt to call.

A.5.5.2.3.3 Exhausted channel list.
If a calling station has exhausted all of its prearranged scan set channels and failed to establish a link, it shall immediately return to normal receive scanning (the available state). It shall also alert the operator (and networking controller if present) that the calling attempt was unsuccessful.

A.5.5.2.4 End of frame detection.
ALE controllers shall identify the end of a received ALE signal by the following methods. The controller shall search for a valid conclusion (TIS or TWAS, possibly followed by DATA and REP for a maximum of five words, or $T_{x\ max}$). The conclusion must maintain constant redundant word phase within itself (if a sound) and with associated previous words. The controller shall examine each successive redundant word phase (T_{rw}) following the TIS (or TWAS) for the first (of up to four) non-readable or invalid word(s). Failure to detect a proper word (or detection of an improper word) or detection of the last REP, plus the last word wait delay time, (T_{lww} or T_{rw}), shall indicate the end of the received transmission. The maximal acceptable terminator sequence is TIS (or TWAS), DATA, REP, DATA, REP.

TABLE A-XV. Timing.

NOTE: Refer to annex A and annex B for details and for timing symbols not defined here.

Basic system timing

- Tone rate = 125 symbols per second (sps)
- Tone period = Ttone = 8 ms
- On-air rate = 375 b/s
- On-air word: T_w = 130.66... ms
- On-air redundant word: $T_{rw} = 3\ T_w$ = 392 ms
- On-air leading redundant words: $T_{lrw} = 2\ T_{rw}$ = 784 ms
- On-air individual (net) address time: $T_a = m \times T_{rw}$ for m = 1 to 5 $_{max}$ words. T_a = 392 ms to 1960 ms
- Propagation: T_p = 0 to 70 ms

System timing limits

- Address size limit 5 words: $T_{a\ max}$ = 1960 ms
- Address first word limit: T_{al} = 392 ms
- Call time maximum: T_c = 4704 ms (one-half of T_{lc} = 12 words $_{max}$)
- Group addresses first word limit: T_{cl} = 1960 ms
- Maximum scan period: $T_{s\ max}$ = 50 s
- Message section basic time (unless modified by AMD extension, or by CMD (such as DTM or DBM)): $T_{m\ max}$ basic = 11.76s
- Message section time limit, AMD (90 characters): $T_{m\ max}$ AMD = 11.76s
- Message section time limit, DTM (1053 characters): $T_{m\ max}$ DTM = 2.29 min (entire data block)
- Message section time limit, DBM, (37377 characters): $T_{m\ max}$ DBM = 23.26 min (entire deeply interleaved block with CMD)
- Termination time limit: $T_{x\ max}$ = 1960 ms

If an ALE (orderwire) protocol such as AMD, DTM, or DBM is used to extend the basic message section, it shall start no later than the start of the 30th word (11.368 s). Such extension of the message section shall be determined by the length of the extended ALE protocol, and the message section shall terminate at the end of the orderwire without additional extension. The conclusion shall start at the end of the message section.

Individual calling

- Minimum dwell time: T_d (5) $_{min}$ = 200 ms, basic receive scanning (5 channels per second)
- Minimum dwell time: T_d (2) $_{min}$ = 500 ms minimum receive scanning (2 channels per second (chps))
- Probable maximum dwell per channel, for channel, for T_s computations, let $T_d = T_{drw}$ =784 ms
- Number of channels: C
- Scan period: $T_s \leq C \times T_{drw}$
- Call time: $T_c = T_a$ (one or more whole addresses as required $\Sigma\ T_a$) in T_{lc}
- Call time (Group Call): $T_{cl} = T_{a1}$ (one or more different first words, $\Sigma\ T_{al}$) in T_{sc}
- Leading call time: $T_{lc} = 2\ T_c$
- Redundant call time: $T_{rc} = T_{lc} + T_x$

TABLE A-XV. Timing (continued).

- Scanning call time: $T_{sc} = n \times T_{cl} \geq T_s$
- Calling cycle time: $T_{cc} = T_{sc} + T_{lc} \geq T_s + T_{lc}$
- Scanning redundant call time: $T_{src} = T_{sc} + T_{rc}$
- Last word wait delay: $T_{lww} = T_{rw} = 392$ ms
- Wait for calling cycle end time: $T_{wce} = 2 \times$ own T_s (default)
- Tune time: T_t (as required by slowest tuner)
- Wait for reply and tune time: $T_{wrt} = T_{wr} + T_t$
- Detect signaling period: $T_{ds} \leq (T_d(5) = 200$ ms)
- Detect redundant word period: $T_{drw} = T_{rw}$ + spare $T_{rw} = 784$ ms
- Detect rotating redundant word period: $T_{drrw} = 2\ T_{rw}$ + spare $T_{rw} = 1176$ ms

Sounding

- Redundant sound time (similar to T_{lc}): $T_{rs} = 2\ T_a$ (caller)
- Scanning sound time (similar to T_{sc}): $T_{ss} = n \times T_a$ (caller) $\geq T_s$
- Scanning redundant sound time (similar to T_{cc}): $T_{srs} = T_{ss} + T_{rs} \geq T_s + T_{rs}$

Star calling

- Minimum standard slot widths: $T_{sw\ min} = 14, 17\ T_w$ for 1st handshake slots, or 17, 20 for subsequent handshake slots, or other T_w as set by CMD.
- Slot widths: $T_{sw} = 14, 17, 9$, or other T_w
- Slot number: SN
- Slot wait time: $T_{swt} = T_{sw} \times SN$ (uniform case)
  - Slot wait time (delay to start reply): T_{swt} for each slot is the sum of all the previous slot times and so must be different for each slot and is cumulative. $T_{swt}(SN) = T_{sw} \times SN$ for uniform slots or generally $T_{swt}(SN) = SN \times [5\ T_w + 2\ T_a$(caller) + (optional LQA)T_{rw} + (optional message)$T_m] + T_a$ (caller) + (sum of all previous called addresses):

$$\sum_{m=1}^{m=SN-1} T_a(m)\ (called)$$

NOTE: the general formula uses the caller address size for caller *and called* stations in slot 0. See example in A.5.5.4.1.4.

- Number of slots: NS
- Wait for net reply (at calling station): $T_{wrn} = T_{sw} \times (NS+1)$ for uniform slots, or generally $T_{wrn} = T_{swt}(NS+1)$
- Wait for net acknowledgment (at called stations): $T_{wan} = T_{wrn} + T_{drw}$
- Turnaround and tune limits: $T_{ta} + T_t \leq 360$, 2100, or 1500 ms, depending on whether slot 0, 1, or others
- Maximum star group wait for acknowledgment: $T_{wan\ max} = 107\ T_w + 27\ T_a$ (caller) + $13\ T_{rw}$ (optional LQA) + $13\ T_m$ (optional message)
- For late arrival stations, if caller uses one word addresses and no message calling: $T_{wan\ max} = 188\ T_w$, or $227\ T_w$ if LQA

Programmable timing parameters: typical values

- Wait (listen first): $T_{wt} = 2$ seconds, general uses; = 784 ms, ALE/data only channels
- Tune time: $T_t = 8\ T_w = 1045.33...$ms (default), "blind" first call;
  = 20 seconds, next try
- Automatic sounding: $T_{ps} = 30$ minutes
- Wait for activity: $T_{wa} = 30$ seconds

A.5.5.3 One-to-one calling.
The protocol for establishing a link between two individual stations shall consist of three ALE frames: a call, a response, and an acknowledgment. The sequence of events, and the timeouts involved, are discussed in the following paragraphs using a calling station SAM and a called station JOE.

A.5.5.3.1 Sending an individual call.
After selecting a channel for calling, the calling station (SAM) shall begin the protocol by first listening on the channel to avoid "disturbing active channels," and then tuning. If the called station (JOE) is known to be listening on the chosen channel (not scanning), the calling station shall transmit a single-channel call that contains only a leading call and a conclusion (see upper frame in figure A-29). Otherwise, it shall send a longer calling cycle that precedes the leading call with a scanning call of sufficient length to capture the called station's receiver as it scans (lower frame in figure A-29). The duration of this scanning call shall be 2 T_{rw} for each channel that the called station is scanning. The scanning call section shall contain only the first word of the called station address, using a TO preamble, and repeated as necessary until the end of the scanning call section.

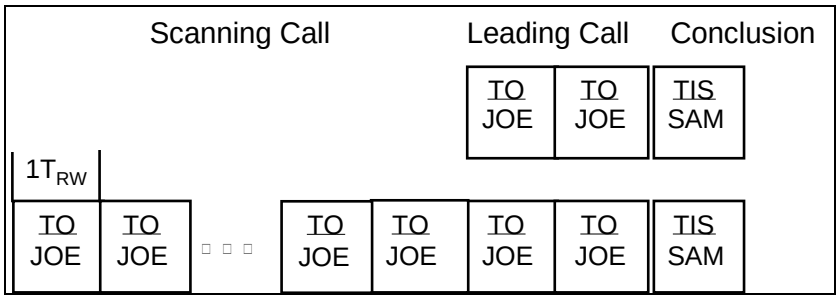


FIGURE A-29. Individual calls.

The entire called station address shall be used in the leading call section, and shall be sent twice (see figure A-29) using a TO preamble each time the first word is sent and DATA and REP as required for additional words.

Any message section CMDs shall be sent immediately following the leading call, followed by a conclusion containing the complete calling station address ("TIS SAM"). The calling station shall then wait a preset reply time to start to receive the called station's response. In the single-channel case, the wait for reply time shall be T_{wr}, which includes anticipated round trip propagation delay and the called station's turnaround time. In the multi-channel case, the calling station shall wait through a wait for reply and tune time (T_{wrt}), which also includes time for the called station to tune up on the chosen channel.

If the expected reply from the called station does not start to arrive within the preset wait for reply time (T_{wr}) or wait for reply and tune time (T_{wrt}), the linking attempt on this channel has failed. At this point, if other channels in the scan set have not been tried, the linking attempt will normally start over on a new channel. Otherwise, the ALE controller shall return to the available state, and the calling station's operator or networking controller shall be notified of the failed linking attempt.

A.5.5.3.2 Receiving an individual call.
When the called station (JOE) arrives on channel, sometime during its scan period T_s, and therefore during the calling station SAM's longer scan calling time T_{sc}, the called station shall attempt to detect ALE signaling within its dwell time. If ALE signaling is detected, and the controller achieves word sync, it shall examine the received word to determine the appropriate action.

If JOE reads "TO JOE" (or an acceptable equivalent according to protocols), the ALE controller shall stop scan, enter the linking state, and continue to read ALE words while waiting a preset, limited time T_{wce} for the calling cycle to end and the message or conclusion to begin.

- If the received word is potentially from a sound or some other protocol, the ALE controller shall process the word in accordance with that protocol.
- Otherwise, the ALE controller shall resume its previous state (e.g., available if it was scanning, linked if it was linked to another station).

While reading a call in the linking state, the called station shall evaluate each new received word. The controller shall immediately abort the handshake and return to its previous state upon the occurrence of any of the following:

- It does not receive the start of a quick-ID, message, or frame conclusion within T_{wce}, or the start of a conclusion within T_{mmax} after the start of the message section;
- Any invalid sequence of ALE word preambles is received, except that during receipt of a scanning call, up to three contiguous words containing uncorrectable errors shall be tolerated without causing rejection of the frame;
- The end of the conclusion is not detected within T_{lww}, (plus the additional multiples of T_{rw} if an extended address) after the first word of the conclusion.

If a quick-ID or a message section starts within T_{wce}, the called station, (JOE) shall attempt to read one or more complete messages within a new preset, limited time T_{mmax}

If a frame conclusion starts "TIS SAM," the called station shall wait and attempt to read the calling station's address (SAM) within a new preset, limited time T_{xmax}.

If an acceptable conclusion sequence with TIS is read, the called station shall start a "last word wait" timeout $T_{lww} = T_{rw}$ while searching for additional address words (if any) and the end of the frame (absence of a detected word), which shall trigger its response. The called station will also expect the calling station to continue the handshake (with an acknowledgment) within the called station's reply window, $T_{wr,}$ after its response. If TWAS is read instead, the called station shall

not respond but shall return to its previous state immediately after reading the entire calling station address.

If all of the above criteria for responding are satisfied, the called station shall initiate an ALE response immediately after detecting the end of the call, unless otherwise directed by the operator or controller.

A.5.5.3.3 Response.
Upon receipt of a call that is addressed to one of its own self addresses (JOE), and which contains a valid calling station address in a TIS conclusion (SAM), the called station shall listen for other traffic on the channel. The nominal listening time is 2 T_{rw} since the channel is known to be in use for ALE. If other traffic is not detected, the station shall tune up, send a response (figure A-30), and start its own reply timer T_{wr}. (The longer T_{wrt} timeout is not necessary unless the calling station will send its acknowledgment on a different channel than the one carrying the call, requiring re-tuning.) The "TO address" in the response shall be identical to the caller's address from the conclusion of the call frame.

If the channel is in use, the ALE controller shall ignore the call and return to its previous state unless otherwise programmed.

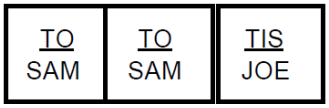


FIGURE A-30. Response frame.

If the calling station (SAM) successfully reads the beginning of an appropriate response ("TO SAM") starting within its timeout (either T_{wr} or T_{wrt}), it shall process the rest of the frame in accordance with the checks and timeouts described above for the call until it either aborts the handshake or receives the appropriate conclusion, which in this example is "TIS JOE."
Specifically, the calling station shall immediately abort the handshake upon the occurrence of any of the following:

- It does not receive an appropriate response calling cycle ("TO SAM") starting within the timeout;
- An invalid sequence of ALE word preambles occurs;
- It does not receive the appropriate conclusion ("TIS JOE") starting within T_{lc} (plus $T_{m\ max}$, if message included);
- The end of the conclusion is not detected within T_{lww}, (plus the additional multiples of T_{rw} if an extended address).

After aborting a handshake for any of the above reasons, the calling station will normally restart the calling protocol, usually on another channel.

If the calling station receives the proper conclusion from the called station ("TIS JOE") starting within T_{lc} (plus $T_{m\ max}$, if message included), it shall set a last word wait timeout as above and prepare to send an acknowledgment. If, instead, "TWAS JOE" is received, the called station has rejected the linking attempt, the calling station ALE controller shall abort the linking attempt and inform the operator of the rejected attempt.

A.5.5.3.4 Acknowledgment.
If all of the above criteria for an acceptable response are satisfied, and if not otherwise directed by the operator or networking controller, the calling station ALE controller shall alert its operator that a correct response has been received, send an ALE acknowledgment (see figure A-31), enter the linked state with the called station (JOE), and unmute the speaker.

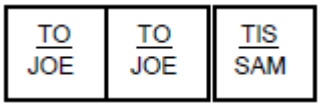


FIGURE A-31. Acknowledgment frame.

A "wait for activity" timer T_{wa} shall be started (with a typical timeout of 30 seconds) that shall cause the link to be dropped if the link remains unused for extended periods (see A.5.5.3.5).

If the called station (JOE) successfully reads the beginning of an appropriate acknowledgment ("TO JOE") starting within its T_{wr} timeout, it shall process the rest of the frame in accordance with the checks and timeouts described above for the response until it either aborts the handshake or receives the appropriate conclusion, which in this example is "TIS SAM" or "TWAS SAM."
Specifically, the calling station shall immediately abort the handshake upon the occurrence of any of the following:

- It does not receive an appropriate response calling cycle ("TO JOE") starting within its T_{wr} timeout;
- An invalid sequence of ALE word preambles occurs;
- It does not receive the appropriate conclusion starting within T_{lc} after the start of the frame (plus $T_{m\ max}$, if message included);
- The end of the conclusion is not detected within T_{lww}, (plus the additional multiples of T_{rw} if an extended address).

If the handshake is aborted for any of the above reasons, the handshake has failed, and the called station ALE controller shall return to its pre-linking state. The called station shall notify the operator or controller of the failed linking attempt.

Otherwise, the called station shall enter the linked state with the calling station ("SAM"), alert the operator (and network controller if present), unmute the speaker, and set a wait-for-activity timeout T_{wa}.

NOTE 1: Although SAM's acknowledgment to JOE appears identical to a single-channel individual call from SAM to JOE, it does not cause JOE to provide another response to the acknowledgment (resulting in an endless "ping-pong" handshake) because SAM's acknowledgment arrives within a narrow time window (T_{wr}) after JOE's response, and an acknowledge (ACK) from SAM is expected within this window. If SAM's acknowledgment arrives late (after T_{wr}), however, then JOE must treat it as a new individual call (and shall therefore send a new response, if SAM concludes the frame with TIS).

NOTE 2: A typical one-to-one scanning call three-way handshake takes between 9 and 14 seconds.

A.5.5.3.5 Link termination.
Termination of a link after a successful linking handshake shall be accomplished by sending a frame concluded with TWAS to any linked station(s) which is (are) to be terminated. For example, "TO JOE, TO JOE, TWAS SAM" (when sent by SAM) shall terminate the link between stations SAM and JOE. JOE shall immediately mute and return to the available state, unless it still retains a link with any other stations on the channel. Likewise, SAM shall also immediately mute and return to the available state, unless it retains a link with any other stations on the channel.

A.5.5.3.5.1 Manual termination.
A means shall be provided for operators to manually reset a station, which shall mute the speaker(s), return the ALE controller to the available state, and send a link terminating (TWAS) transmission, as specified above, to all linked stations, unless this latter feature is overridden by the operator. (DO: provide a manual disconnect feature that drops individual links while leaving others in place.)

A.5.5.3.5.2 Automatic termination.
If no voice, data, or control traffic is sent or received by a station within a preset time limit for activity (T_{wa}), the ALE controller shall automatically mute the speaker, terminate the linked state with any linked stations, and return to the available state. The wait for the activity timer is mandatory, but shall also be capable of being disabled by the operator or network manager. This timed reset is not required to cause a termination (TWAS) transmission, as specified above. However, it is recommended that a termination be sent to reset the other linked stations(s) to immediately return them to the available state.

Termination during a handshake or protocol by the use of TWAS (or a timer) should cause the receiving (or timed-out) station to end the handshake or protocol, terminate the link with that sta-

tion, re-mute, and immediately return to the available state unless it still retains a link with another station.

A.5.5.3.6 Collision detection.
While receiving an ALE signal, it is possible for the continuity of the received signal to be lost (due to such factors as interference or fading) as indicated by failure to detect a good ALE word at a T_{rw} boundary. When one or both Golay words of a received ALE word contain uncorrectable errors, the ALE controller shall attempt to regain word sync, with a bias in favor of words that arrive with the same word phase as the interrupted frame.

If word sync is reacquired but at a new word phase, this indicates that a collision has occurred. The interrupted frame shall be discarded, and the interrupting signal processed as a new ALE frame.

NOTE: Stations should be able to read interfering ALE signals, as they may contain useful (or critical) information, for which the station is "always listening."

A.5.5.4 One-to-many calling.
One station may simultaneously establish a multi-way link with multiple other stations using the protocols described in the following subparagraphs.

A.5.5.4.1 Slotted responses.
The simple three-way handshake used for individual links cannot be used for one-to-many calling because the responses from the called stations would collide with each other. Instead, a time-division multiple access (TDMA) scheme is used. Each responding station shall send its response in an assigned or computed time slot as described later for the particular one-to-many protocol.

At the end of a one-to-many call frame, the following events shall take place:

- The calling station shall set a wait-for-response-and-tune timeout (WRTT) that shall trigger its acknowledgment after the last response slot time has expired. The time allowed is denoted T_{wrn}. The value of T_{wrn} is described later for each one-to-many protocol.
- The called stations shall set their own WRTTs that bound their waiting times for an acknowledgment. To allow time for acquiring word sync during the leading call of the acknowledgment, the waiting time shall be set to $T_{wan} = T_{wrn} + T_{drw}$.
- Each called station shall also set a slot wait timeout T_{swt} that shall trigger its response.
- The called stations shall tune as required during the slot immediately following the end of the call frame, called slot 0.

As each station's slot wait timer expires, it shall send its response and continue to await the expiration of its WRTT. Should that timer expire before the start of an acknowledgment from the calling station, the called station shall abort the linking attempt, and return to its pre-linking state.

A.5.5.4.1.1 Slotted response frames.
Slotted response frames shall be formatted identically to responses in the one-to-one calling protocol (see figure A-32), including a leading call, an optional message section, and a frame conclusion. A responding station shall conclude its response with TIS to accept the call, or TWAS to reject it. When the calling and responding addresses are one-word (as shown), slots are each 14 T_w, or about 1.8 seconds.

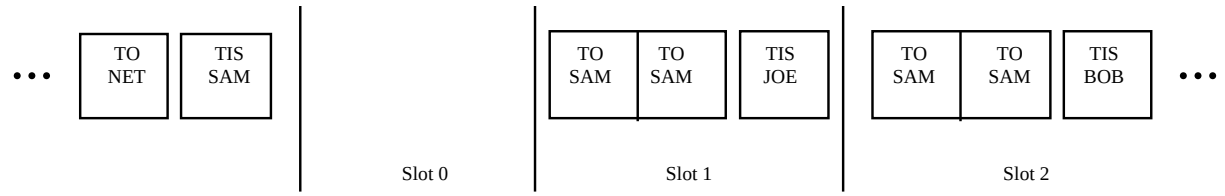


FIGURE A-32. Slotted responses.

A.5.5.4.1.2 Slot widths.
Unless otherwise specified, all slots shall be 14 T_w in duration, which allows response frames with single-word addresses to propagate to and from the other side of the globe and use commonly available HF transceivers and tuners. When any slot is extended, all following slots shall be delayed commensurately.

- When the calling station address is longer than one word, every slot shall be extended by two T_{rw} (six T_w) per additional address word.
- When a called station address is longer than one word, its slot shall be extended by one T_{rw} (three T_w) per additional address word.
- Slots shall be extended by one T_{rw} (three T_w) for each ALE word to be sent in the message section of responses (including LQA CMD).
- The address length of the calling station shall be used to determine the width of slot 0 (T_{slot0}).

A.5.5.4.1.3 Slot wait time formula.
The general formula for determining the correct timing for slotted responses in non-minimum or non-uniform cases is as follows for a selected slot number denoted SN:

$$T_{swt}(SN) = SN \cdot \left[5T_w + 2T_a(\text{caller}) + (\text{optional message})T_m\right] + T_a(\text{caller}) + \sum_{m=1}^{m=SN-1} T_a(m)\ (\text{called})$$

Where T_a (caller) is the address length (an integer multiple of T_{rw}) of the calling station, (optional message)T_m is an optional message section (same size for all slots), present if and only if requested in the call. T_a(m) (called) is the address length of the station that will respond in slot m. (Note that the length of slot 0 is determined by using the address length of the calling station.) The formula for the calling station wait for net reply timeout (T_{wrn}) is

$$T_{wrn} = T_{swt}(NS + 1)$$

where NS is the total number of slots; one is added to include slot zero.

The formula for the called station acknowledgment timer is

$$T_{wan} = T_{wrn} + T_{drw}$$

A.5.5.4.1.4 Slotted response example.
The slotted response example is shown in figure A-33.

FIGURE A-33. 2G ALE slotted responses.

Calculation of the slot timing for the stations SAM, JOE, and BOB shown on Figure A-33 proceeds as follows:

T_a(caller: SAM) = T_a(called: JOE, BOB) = $1T_{rw} = 3T_w$,

$T_m = 0T_{rw} = 0T_w$

$T_{swt}(0) = 0$ (begins at time = 0),

$$T_{swt}(1) = 1 \cdot [5T_w + 2 \cdot 3T_w + 0T_w] + 3T_w + \sum_{m=1}^{0} T_a(m)$$

$$= 1\,[5T_w + 6T_w] + 3T_w + 0 = 14T_w,$$

$T_{slot0} = T_{swt}(1) - T_{swt}(0) = 14T_w$.

$$T_{swt}(2) = 2 \cdot [5T_w + 2 \cdot 3T_w + 0T_w] + 3T_w + \sum_{m=1}^{1} T_a(m)$$

$$= 2\,[5T_w + 6T_w] + 3T_w + 3T_w = 28T_w$$

$T_{slot1} = T_{swt}(2) - T_{swt}(1) = 14T_w$.

The calling station wait for reply timeout is $T_{wrn} = T_{swt}(NS+1) = T_{swt}(3) = 42T_w$.

The called station wait for ack timeout is $T_{wrn} = T_{wrn} + T_{drw} = 42T_w + 6T_w = 48T_w$.

A.5.5.4.2 Star net calling protocol.
A net address is assigned to a set of net member stations, as described in A.5.2.4.4. The slot number and address to be used by each net member are preassigned and known to all net members.

A.5.5.4.2.1 Star net call.
A star net call is identical to a one-to-one call, except that the called station address is a net address, as shown in figure A-34. The calling station address shall be an individual station address (not a net or other collective address).

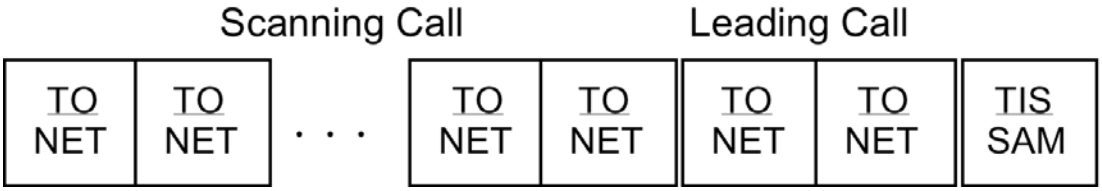


FIGURE A-34. Net call.

A.5.5.4.2.2 Star net response.
When an ALE controller receives a call that is addressed to a net address that appears in its self address memory (see A.4.3.2), it shall process the call using the same checks and timeouts as an individual call (see A.5.5.3.2). If the call is acceptable, it shall respond in accordance with A.5.5.4.1 using its assigned net member address and slot number for the net address that was called.

A.5.5.4.2.3 Star net acknowledgment.
A star net acknowledgment is identical to a one-to-one acknowledgment, except that the called station address is a net address.

An ALE controller that has responded to a net call shall process the acknowledgment from the calling station in accordance with A.5.5.3.4, except that the wait-for-response timeout value shall be the T_{wan} timeout from A.5.5.4.1.3. A TWAS acknowledgment from the calling station shall return the called ALE controller to its pre-linking state. If a TIS acknowledgment is received from the calling station, the called ALE controller shall enter the linked state with the calling station (SAM in this example), alert the operator (and network controller if present), unmute the speaker, and set a wait-for-activity timeout T_{wa}.

A.5.5.4.3 Star group calling protocol.
The group calling protocol extends the power of one-to-many calling to ad hoc collections of stations that have not been preprogrammed as a net. Nothing need be known about the stations except their individual addresses and scanned frequencies. Because a group is not set up in advance, stations must be able to derive group membership and slot parameters on the fly. Group membership is limited as follows:

- The total length of group member station addresses cannot exceed 12 ALE words.
- The set of unique first address words among group members cannot exceed five words.

A.5.5.4.3.1 Star group scanning call.
A group address is produced by combining individual addresses of the stations that are to form the group. During a scanning call, only the first word(s) of addresses shall be sent, just as for individual or net calls. The set of unique first address words for the group members shall be sent repeatedly in rotation until the end of T_{sc}. These address words shall alternate between THRU and REP preambles (see figure A-35 for a sample group consisting of BOB, EDGAR, and SAM).

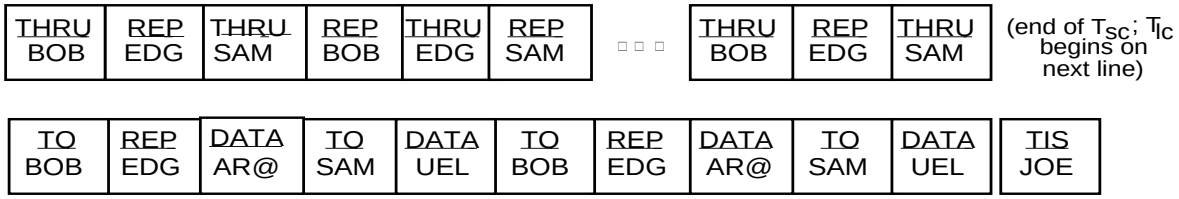


FIGURE A-35. Group call.

When group member addresses share a common first word, that word shall be sent only once during T_{sc}. A limit of five unique first words may be sent in rotation during T_{sc}.

A.5.5.4.3.2 Star group leading call.
During T_{lc}, the complete addresses of the prospective group members shall be sent, using TO preambles as usual. Up to 12 address words total are allowed for the full addresses of group members, so T_{lc} in a group call may last up to 24 T_{rw}. Note in figure A-34 that when a TO word would follow another TO word, a REP preamble must be used, but when a TO follows any other word it shall remain a TO.

A.5.5.4.3.3 Star group call conclusion.
The optional message section and the conclusion of a star group call shall be in accordance with A.5.2.5.

A.5.5.4.3.4 Receiving a star group call.
Slots shall be derived for group call responses by noting the order in which individual addresses appear in the call.

a. When an ALE controller pauses on a channel carrying a group scanning call, it will read either a THRU or a REP preamble. If the address word in this first received word matches the first word of one of its individual addresses, the ALE controller shall stay to read the leading call. Otherwise, it shall continue to read first address words until it finds:

- a match with the first word of a self address, or
- a repetition of a word it has already seen, or
- five unique words.

(In the latter two cases, the station is not being called and the ALE controller shall return to the available or linked state as appropriate.)

b. When T_{lc} starts, an ALE controller potentially addressed in the scanning call shall watch for its complete address. If found, a slot counter shall be set to 1 and incremented for each address that follows it. If that address is found again (as it should be, because the address list is repeated in T_{lc}), the counter shall be then reset to 1, and incremented for each following address as before. The number of words in each following address shall also be noted for use in computing T_{swt}.

c. The message section (if any) and the frame conclusion shall processed in accordance with A.5.5.3.2.

In the event that an addressed ALE controller arrives on channel too late to identify the size of the called group, it will be unable to compute the correct T_{wan}. In this situation, it shall use a default value for T_{wan}, which is equal to the longest possible group call of twelve one-word addresses. It will, however, have computed its correct slot number because to have received its own address it must also have received the addresses that followed that self address in the leading call.

A.5.5.4.3.5 Star group slotted responses.
Slotted responses shall be sent and checked in accordance with A.5.5.4.1, using the derived slot numbers and the self address contained in the leading call.

A.5.5.4.3.6 Star group acknowledgment.
The acknowledgment in a group call handshake shall be addressed to any subset of the members originally called, and is usually limited to those whose responses were heard by the calling station. The leading call of the acknowledgment shall include the full addresses of the stations addressed, sent twice, using the same syntax as in the call (A.5.5.4.3.2).

An ALE controller that responded to a group call shall await acknowledgment and process an incoming acknowledgment in accordance with A.5.5.3.4, with the following exceptions:

- The wait-for-response timeout value shall be the T_{wan} timeout from A.5.5.4.1.3, not $T_{wr.}$
- Self address detection shall search through the entire leading call group address.

An ALE controller that responded but was not named in the acknowledgment shall return to its pre-linking state. An ALE controller that is addressed in the acknowledgment shall proceed as follows:

- A TWAS acknowledgment from the calling station shall return the called ALE controller to its pre-linking state.
- If a TIS acknowledgment is received from the calling station, the called ALE controller shall enter the linked state with the calling station (SAM in this example), alert the operator (and network controller if present), unmute the speaker, and set a wait-for-activity timeout T_{wa}.

A.5.5.4.3.7 Star group call example.
In the example group call in figure A-35, SAMUEL will respond in slot 1, with $T_{swt} = 14\ T_w$ (the one-word address JOE causes slot 0 to be $14\ T_w$). EDGAR will respond in slot 2, with $T_{swt} = 14 + 17\ T_w = 31\ T_w$ (slot 1 is $17\ T_w$ because of SAMUEL's two-word address). BOB will respond in slot 3, with $T_{swt} = 48\ T_w$. JOE will send an acknowledgment after $62\ T_w$.

A.5.5.4.3.8 Multiple self addresses in group call.
If a station is addressed multiple times in a group call, even by different addresses, it shall properly respond to at least one address.

NOTE: The fact that the called station has multiple addresses may not be known to the caller. In some cases, it would be confusing or inappropriate to respond to one but not another address. Redundant calling address conflicts can be resolved after successful linking, if there is a problem.

A.5.5.4.4 Allcall protocol.
An AllCall requests all stations hearing it to stop and listen, but not respond. The AllCall special address structure(s) (see A.5.2.4.7) shall be the exclusive member(s) of the scanning call and the leading call, and shall not be used in any other address field or any other part of the handshake. The global AllCall address shall appear only in TO words. Selective AllCalls with more than one selective AllCall address, however, shall be sent using group addressing, using THRU (alternating with REP) during the scanning call and TO (alternating with REP) during the leading call.

An AllCall pertains to an ALE controller when it is a global AllCall, or when a selective AllCall specifies a character that matches the last character of any self address assigned to that station. Upon receipt of a pertinent AllCall, an ALE controller shall temporarily stop scanning and listen for a preset limited time, $T_{cc\ max}$.

- If a message section or frame conclusion does not arrive within $T_{cc\ max}$, the controller shall automatically resume scanning.
- If a quick-ID (an address beginning with a FROM word immediately after the calling cycle) arrives, the pause for the message section shall be extended for no more than five words (5 T_{rw}), and if a CMD does not arrive, the controller shall resume scanning.
- If a message arrives (indicated by receipt of a CMD), the controller shall pause for a preset limited time, $T_{m\ max}$ to read the message. If the frame conclusion does not arrive within $T_{m\ max}$, the controller shall automatically resume scanning. If a conclusion arrives (indicated by receipt of a TIS or TWAS), the controller shall pause (for a preset limited time, $T_{x\ max}$) to read the caller's address. If the end of the signal does not arrive within $T_{x\ max}$, the controller shall automatically resume scanning.

If a pertinent AllCall frame is successfully received and is concluded with a TIS, the controller shall enter the linked state, alert the operator, unmute its speaker and start a wait-for-activity timeout. If an AllCall is successfully received with a TWAS conclusion, the called controller shall automatically resume scanning and not respond (unless otherwise directed by the operator or controller).

If a station receiving an AllCall desires to attempt to link with the calling station, the operator may initiate a handshake within the pause after a TIS conclusion. Note that in all handshakes (the initial AllCall does not constitute a handshake), the AllCall address shall not be used. To minimize possible adverse effects resulting from overuse or abuse of AllCalls, controllers shall have the capability to ignore AllCalls. Normally AllCall processing should be enabled.

A.5.5.4.5 AnyCall protocol.
An AnyCall is similar to an AllCall, but it instead requests responses. Use of the AnyCall special address structures is identical to that for the AllCall special address structures. Upon receipt of a pertinent AnyCall, an ALE controller shall temporarily stop scanning and examine the call identically to the procedure for AllCalls, including the $T_{cc\ max}$, $T_{m\ max}$, and $T_{x\ max}$ limits.

If the AnyCall is successfully received, and is concluded with TIS, the controller shall enter the linking state and automatically generate a slotted response in accordance with A.5.5.4.1 and the following special procedure:

- Because neither preprogrammed nor derived slot data are available, the controller shall randomly select a slot number, 1 through 16.
- Each slot shall be 20 T_w (2613.33...ms) wide, unless the calling station requests LQA responses, in which case the slots shall expand by 3 T_w to 23 T_w to accommodate the CMD LQA message section.
- The controller shall compute values for T_{swt} and T_{wan} using this slot width and its random slot number.
- Slot 0 shall be used for tuning, as usual for slotted response protocols.
- Upon expiration of its T_{swt} timeout, the controller shall send a standard star net response consisting of TO (with the address of the caller) and TIS (with the address of the responder), with the LQA CMD included if requested. Responders shall use a self address no longer than five words minus twice the caller address length. (For example, if the caller address is two words, the responder shall use a one-word address.) The AnyCall special address shall not be sent.

In this protocol, collisions are expected and tolerated. The station sending the AnyCall shall attempt to read the best response in each slot.

Upon receipt of the slotted responses, the calling station shall transmit an ACK to any subset of stations whose responses were read, using an individual or group address. The AnyCall special address shall not be used in the acknowledgment. The caller selects the conclusion of its ACK to either maintain the link for additional interoperation and traffic with the responders (TIS), or return everyone to scan (TWAS), as appropriate to the caller's original purpose.

An ALE controller that responded to an AnyCall shall await and process the acknowledgment in accordance with A.5.5.4.3.6.

To minimize possible adverse effects resulting from overuse or abuse of AnyCalls, controllers shall have the capability to ignore AnyCalls. Normally AnyCall processing should be enabled.

A.5.5.4.6 Wildcard calling protocol.
Wildcard addresses shall be the exclusive members of a calling cycle in a call, and shall not be used in any other address sequence in the ALE frame or handshake. The span (number of cases possible) of the wildcard(s) used should be minimized to only the essential needs of the user(s).

Calls to wildcard addresses that conclude with TWAS shall be processed identically to the All-Call protocol.

Responses to wildcard calls that conclude with TIS shall be sent in pseudorandomly-selected slots in accordance with the AnyCall protocol.

As in both the AllCall and AnyCall, the controller shall be programmable to ignore wildcard calls, but wildcard call processing should normally be enabled.

A.5.6. ALE control functions (CMDs other than AMD, DTM, and DBM).
In addition to automatically establishing links, stations shall have the capability to transfer information within the orderwire, or message, section of the frame. This section describes these messages, including data, control, error checking, networking, and special purpose functions. Table A-XVI provides a summary of the CMD functions. CMD functions not flagged in the table as mandatory are optional.

NOTE: For critical orderwire messages that require increased protection from interference and noise, several ALE techniques are available. Any message may be specially encoded off-line and then transmitted using the full 128 ASCII CMD data DTM mode (which also accepts random data bits). Larger blocks of information may be Golay FEC coded and deeply interleaved using the CMD DBM mode. Both modes have an automatic repeat request (ARQ) error-control capability. Integrity of the data may be ensured using the CMD cyclic redundancy check (CRC) mode (see A.5.6.1). In addition, once a link has been established, totally separate equipment, such as heavily coded and robust modems, may be switched onto the rf link in the normal circuit (traffic-bearing) mode.

TABLE A-XVI. Summary of CMD functions.

	First Character		Second Character		Function	Reference
Mandatory	Any of the extended-64 character set				AMD	A.5.7.2
	“	1100000			Advanced LQA	A.5.6.3.7
Mandatory	a	1100001			LQA	A.5.4.1
	b	1100010			Data block message	A.5.7.4
	c	1100011			Channels	A.5.6.3.1
	d	1100100			DTM	A.5.7.3
	f	1100110			Frequency	A.5.6.3.2
	l	1101100			Location	A.5.6.8
	m	1101101		**Mode selection commands**		A.5.6.5
			a	1100001	Analog port Selection	
			c	1100011	Crypto negotiation	
			d	1100100	Data port selection	
			n	1101110	Modem negotiation	
			q	1110001	Digital squelch	
	n	1101110			Noise report	A.5.4.4
	p	1110000			Power control	A.5.6.2
	r	1110010			LQA report	A.5.6.3.5
	t	1110100		**Scheduling commands**		A.5.6.4
			a	1100001	Adjust slot width	
			b	1100010	Station busy	
			c	1100011	Channel busy	
			d	1100100	Set dwell time	
			h	1101000	Halt and wait	
			l	1101100	Contact later	
			m	1101101	Meet me	
			n	1101110	Poll operator, default NAK	
			o	1101111	Request operator ACK	
			p	1110000	Schedule periodic function	
			q	1110001	Quiet contact	
			r	1110010	Respond and wait	
			s	1110011	Set sounding interval	
			t	1110100	Tune and wait	
			w	1110111	Set slot width	
			x	1111000	Do not respond	
			y	1111001	Year and date	
			z	1111010	Zulu time	
Mandatory	v	1110110	c	1100011	Capabilities	A.5.6.6.2
Mandatory			s	1110011	Version	A.5.6.6.1
*	x	1111000			CRC*	A.5.6.1
	y	1111001			CRC*	
	z	1111010			CRC*	
	{	1111011			CRC*	
	|	1111100			User-unique functions	A.5.6.9
**	~	1111110			Time exchange	A.5.6.4.3

* 16-bit CRC overflows into the two least-significant bits of the first two character. CRC is mandatory only if DTM or DBM is provided.
** Mandatory if linking protection at AL-2 or higher is provided (see Appendix B – Linking Protection)

A.5.6.1 CRC.
This special error-checking function is available to provide data integrity assurance for any form of message in an ALE call.

NOTE: The CRC function is optional, but mandatory when used with the DTM or DBM modes.

The 16-bit frame check sequence (FCS) generator polynomial is

$$X^{16} + X^{12} + X^5 + 1$$

and the sixteen FCS bits are designated

(MSB) X^{15}, X^{14}, X^{13}, X^{12}...X^1, X^0 (LSB)

The shift register used to compute the FCS shall be initialized to all 1's. Bits of the ALE words to be checked (see below) shall be processed starting with the most-significant bit of each ALE word. After processing the final ALE word, the FCS shall be the 2's complement of the contents of the shift register.

For example, the AMD message "THIS IS AMD " (note the final space character) would produce a CRC word as follows:

```
Input ALE words:
  24 bit word 0xD52449 CMD  "THI"
  24 bit word 0x14D049 DATA "S I"
  24 bit word 0xF4D041 REP  "S A"
  24 bit word 0x136220 DATA "MD "

Result:
  16 bit FCS is 0x7D25
24 bit CRC command is 0xDE7D25
```

The ALE CRC is employed two ways: within the DTM data words, and following the DBM data field, described in paragraphs A.5.7.3 and A.5.7.4, respectively. The first, and the standard, usages are described in this section.

The CMD CRC word shall be constructed as shown in table A-XVII. The preamble shall be CMD (110) in bits P3 through P1 (W1 through W3). The first character shall be "x" (1111000), "y" (1111001), "z" (1111010), or "{" (1111011) in bits C1-7 through C1-1 (W4 through W10). Note that four identifying characters result from FCS bits X^{15} and X^{14} which occupy C1-2 and

C1-1 (W9 and W10) in the first character field respectively. The conversion of FCS bits to and from ALE CRC format bits shall be as described in table A-XVII where X^{15} through X^{0} correspond to W9 through W24.

The CMD CRC message should normally appear at the end of the message section of a transmission, but it may be inserted within the message section (but not within the message being checked) any number of times for any number of separately checked messages, and at any point except the first word (except as noted below). The CRC analysis shall be performed on all ALE words in the message section that precede the CMD CRC word bearing the FCS information, and which are bounded by the end of the calling cycle, or the previous CMD CRC word, whichever is closest. The selected ALE words shall be analyzed in their non-redundant and unencoded (or FEC decoded) basic ALE word (24-bit) form in the bit sequence (MSB) W1, W2, W3, W4...W24 (LSB), followed by the unencoded bits W1 through W24 from the next word sent (or received), followed by the bits of the next word, until the first CMD CRC is inserted (or found). Therefore, each CMD CRC inserted and sent in the message section ensures the data integrity of all the bits in the previous checked ALE words, including their preambles. If it is necessary to check the ALE words in the calling cycle (TO) preceding the message section, an optional calling cycle CMD CRC shall be used as the calling cycle terminator (first FROM or CMD), shall therefore appear first in the message section, and shall analyze the calling cycle words in their simplest (T_c), nonredundant and nonrotated form. If it is necessary to check the words in a conclusion (TIS or TWAS), an optional conclusion CRC shall directly precede the conclusion portion of the call, shall be at the end of the message section, and shall itself be directly preceded by a separate CMD CRC (which may be used to check the message section or calling cycle, as described herein). Stations shall perform CRC analysis on all received ALE transmissions and shall be prepared to compare analytical FCS values with any CMD CRC words which may be received. If a CRC FCS comparison fails, an ARC (or operator initiated) or other appropriate procedure may be used to correct the message.

TABLE A-XVII. Cyclic redundancy check structure.

		CRC bits		Word bits	
CMD preamble		MSB	P3-1	MSB	W1
			P2-1		W2
		LSB	P1-0		W3
	(c)	MSB	CL-7-1		W4
			CL-6-1		W5
First characters			CL-5-1		W6
"x,y,z, {"			CL-4-1		W7
			CL-3-0		W8
	(x)	MSB	CL-2-x^{15}		W9
	(c)	LSB	CL-1-x^{14}		W10
			X^{13}		W11
			X^{12}		W12
			X^{11}		W13
			X^{10}		W14
			X^{9}		W15
			X^{8}		W16
			X^{7}		W17
			X^{6}		W18
			X^{5}		W19
			X^{4}		W20
			X^{3}		W21
			X^{2}		W22
			X^{1}		W23
	(x)	LSB	X^{0}	LSB	W24

NOTES:

1. CMD CRC first character is one of four, "x" (1111000), "y" (1111001), "z" (11111010), or "{" (1111011), depending on CRC bits x^{15} and x^{14}, which are also C1-2 and C1-1, respectively.
2. "x^{n}" indicates FCS bits.

A.5.6.2 Power control (optional).
The power control orderwire function is used to advise parties to a link that they should raise or lower their rf power for optimum system performance. The power control CMD word format shall be as shown in figure A-36. The KP control bits shall be used as shown in table XVIII.

3	7	3	6	5
CMD	1110000 ('p': power control)	KP1-3	Power	(reserved)

FIGURE A-36. Power control CMD format.

TABLE A-XVIII. Power control CMD bits (KP_{1-3}).

Bit	Value	Meaning
KP_3 (MSB)	1	Request to adjust power
	0	Report of current power level
KP_2	1	Relative Power (in dB)
	0	Absolute Power (in dBW)
KP_1 (LSB)	1	Relative Power (dB) is positive
	0	Relative Power (dB) is negative

The procedure shall be:

a. When KP_3 is set to 1, the power control command is a request to adjust the power from the transmitter. If KP_2 is 1, the adjustment is relative to the current operating power, i.e., to raise ($KP_1 = 1$) or lower ($KP_1 = 0$) power by the number of dB indicated in the relative power field. If KP_2 is 0, the requested power is specified as an absolute power in dBW.

b. When KP_3 is set to 0, the power control command reports the current power output of the transmitter, in dB relative to nominal power if KP_2 is 1, or in absolute dBW if KP_2 is 0.

c. KP_1 shall be set to 0 whenever KP_2 is 0.

d. Normally, a station receiving a power control request ($KP_3 = 1$) should approximate the requested effect as closely as possible, and respond with a power report ($KP_3 = 0$) indicating the result of its power adjustment.

A.5.6.3 Channel related functions (optional).
The channel related functions are defined in the following subparagraphs.

A.5.6.3.1 Channel designation.
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 five-digit string (20 bits), in which the first digit is the 10 megahertz (MHz) digit, followed by 1 MHz, 100 kilohertz (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 shall also contain a bit to select either a positive or a negative frequency offset.

A.5.6.3.2 Frequency designation.
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 A.4.3.1. As in the case of frequency designators, channels may be specified either absolutely or relatively. In either case, a 7-bit binary integer shall be used that is interpreted as an unsigned integer in the range 0 through 127. Bits in the associated command shall indicate whether the channel designator represents an absolute channel number, a positive offset, or a negative offset.

a. The frequency select CMD word shall be formatted as shown in figure A-37. A frequency designator (in accordance with A.5.6.3.1) is sent in a DATA word immediately following the frequency select CMD; bit W4 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

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

FIGURE A-37. 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 make whatever response is required by an active protocol on the indicated frequency.

A.5.6.3.3 Full-duplex independent link establishment (optional).
Full duplex independent link establishment is an optional feature; however, if this option is selected the transmit and receive frequencies for use on a link shall be negotiated independently as follows:

a. The caller shall select 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).

b. If the responder hears the call, it shall 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).

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

A.5.6.3.4 LQA polling (optional).
not yet standardized.

A.5.6.3.5 LQA reporting (optional).
not yet standardized.

A.5.6.3.6 LQA scan with linking (optional).
not yet standardized.

A.5.6.3.7 Advanced LQA (optional).
not yet standardized.

A.5.6.4 Time-related functions.

A.5.6.4.1 Tune and wait (optional).
The CMD tune and wait special control function directs the receiving station(s) to perform the initial parts of the handshake, up through tune-up, and wait on channel for further instructions during the specified time limit. The time limit timer is essentially the WRTT as used in net slotted responses where its value T_{wrn} is set by the timing information in the special control instruction, and it starts from the detected end of the call. The CMD tune and wait instruction shall suppress any normal or preset responses. Except for the tune-up itself, the receiving station(s) shall make no additional emissions, and they shall quit the channel and resume scan if no further instructions are received.

NOTE: This special control function enables very slow tuning stations, or stations that must wait for manual operator interaction, to effectively interface with automated networks.

The CMD tune and wait shall be constructed as follows and as shown in table A-XIX. The preamble shall be CMD (110) in bits P3 through P1 (W1 through W3). The first character (C1) shall be "t" (1110100) in bits C1-7 through C1-1 (W4 through W10) and "t" (1110100) in bits C2-7 through C2-1 (W11 through W17), for "time, tune-up." The "T" time bits TB7 through TB1 (W18 through W24) shall be values selected from table A-XX, and limited as shown in table A-XXI. The lowest value (00000) shall cause the tuning to be performed immediately, with zero waiting time, resulting in immediate return to normal scan after tuning.

A.5.6.4.2 Scheduling commands (optional).
These special control functions permit the manipulation of timing in the ALE system. They are based on the standard "T" time values, presented in table A-XX, which have the following ranges based on exact multiples of T_w (130.66...ms) or T_{rw} (392 ms).

- 0 to 4 seconds in 1/8 second (T_w) increments
- 0 to 36 seconds in 1 second (3 T_{rw}) increments
- 0 to 31 minutes in 1 minute (153 T_{rw}) increments
- 0 to 29 hours in 1 hour (9184 T_{rw}) increments

There are several specific functions that utilize these special timing controls. All shall use the CMD (110) preamble in bits P3 through P1 (W1 through W3). The first character is "t" (1110100) for "time." The second character indicates the function as shown in table A-XXI. The basic structure is the same as in table A-XIX.

TABLE A-XIX. Tune and wait structure.

	Tune and Wait Bits		Word Bits	
CMD Preamble	MSB	P3 = 1	MSB	W1
		P2 = 1		W2
	LSB	P1 = 0		W3
First Character "t"	MSB	C1-7 = 1		W4
		C1-6 = 1		W5
		C1-5 = 1		W6
		C1-4 = 0		W7
		C1-3 = 1		W8
		C1-2 = 0		W9
	LSB	C1-1 = 0		W10
Second Character "t"	MSB	C2-7 = 1		W11
		C2-6 = 1		W12
		C2-5 = 1		W13
		C2-4 = 0		W14
		C2-3 = 1		W15
		C2-2 = 0		W16
	LSB	C2-1 = 0		W17
Time Bits "T"	MSB	TB7		W18
		TB6		W19
		TB5		W20
		TB4		W21
		TB3		W22
		TB2		W23
	LSB	TB1	LSB	W24

NOTES:

1. CMD tune and wait first two characters are "t" (1110100) and "t" (1110100) for "time tune-up."
2. Time bits TB7 through TB1 from table A-XX.

TABLE A-XX. Time values.

MULTIPLIER: MSBs									
MSB TB7 (W18)	TB6 (W19)	Exact increment				Approximate increment		Approximate range of "T" values	
0	0	T_w 130.66 . . ms				1/8 second		0 - 4 seconds	
0	1	3 T_{rw} 1176 ms				1 second		0 - 36 seconds	
1	0	153 T_{rw} 59.976 sec				1 minute		0 - 31 minutes	
1	1	9184 T_{rw} 60.002min				1 hour		0 - 29 hours	
		INDEX: Least significant Bits (LSBs)							
TB5 (W20)	TB4 (W21)	TB3 (W22)	TB2 (W23)	LBS TB1 (W24)	INDEX VALUE	"T" VALUE FOR MSB=00	"T" VALUE FOR MSB=01	"T" VALUE FOR MSB=10	"T" VALUE FOR MSB=11
0	0	0	0	0	0	0(1)	0	0	0
0	0	0	0	1	1	130.66 ms	1.176 s	1.00 min	1.00 hr
0	0	0	1	0	2	261.33 ms	2.352 s	2.00 min	2.00 hr
0	0	0	1	1	3	392.0 ms	3.528 s	3.00 min	3.00 hr
0	0	1	0	0	4	523.66 ms	4.204 s	4.00 min	4.00 hr
0	0	1	0	1	5	653.33 ms	5.880 s	5.00 min	5.00 hr
•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•
1	1	1	0	1	29	3789.3 ms	34.10 s	29.0 min	29.0 hr
1	1	1	1	0	30	3920.0 ms	35.28 s	30.0 min	(3)
1	1	1	1	1	31	4050.7 ms	36.46 s	31.0 min	(2)

NOTES:

1. The minimum value "0" (TB = 0000000) is interpreted as "do immediately" if a delay, or "zero size" if a time width, as specified in usage.
2. The maximum value "127" (TB = 1111111) is interpreted as "do it at time or date following," as specified in next CMD.
3. The next maximum value "126" (TB = 1111110) is interpreted as "indefinite time," unlimited except by other CMD or timeout protocol.

TABLE A-XXI. Time-related CMD functions.

Identification	First Character	Second Character	Function
Adjust Slot Width	"t"	"a" (1100001)	Add T to width of all slots for this response. TB=0, normal. TB7=0 as 36 second limit.
Halt and Wait	"t"	"h" (1101000)	Stop scan on channel, do not tune or respond, wait T for instruction; quit and resume scan if nothing. TB=0, quit after call. TB7=0 as 36 second limit.
Operator NAK	"t"	"n" (1101110)	Same as "t,o" operator ACK, except that at T, if no input, automatic tune-up and respond NAK (TIS), in slots if any. TB=0, NAK now.
Operator ACK	"t"	"o" (1101111)	Stop scan, alert operator to manually input ACK (or NAK), which causes tune-up (if needed) and ACK response TWAS, or TIS; if no input by operator by T, simply quit. TB=0, ACK now. TB7=0 as 36 second time limit. TB=1111111, do at date/time following.
Respond and Wait	"t"	"r" (1110010)	Stop scan, tune-up and respond as normal, wait T for instructions, quit and resume scan if nothing. TB=0, quit after response. TB7=0 as 36 second limit. TB=1111111, do at date/time following.
Tune and Wait	"t"	"t" (1110100)	Stop scan, tune-up, do not respond, wait T for Instructions, quit and resume scan if nothing. TB=0, quit after tune-up. TB7=0 as 36 second limit.
Width of Slots	"t"	"w" (1110111)	Set all slots to T wide for this response. TB=0, no responses. TB7=0 as 36 second limit.

NOTES:
1. Preamble is CMD (110).
2. First character is "t" (1110100) for all.
3. Third-character field is binary bits TB7 through TB1 (W18 through W24), designating a time interval "T" as a standard value in table A-XX.
4. When the optional UUF is implemented, the STAY command function is required.
5. This second ASCII character will vary, depending on the resulting binary value.

A.5.6.4.3 Time exchange word formats.
The mandatory time protocols employ the following three types of ALE words: (1) command words, (2) coarse time words, and, (3) authentication words, in the formats listed below.

A.5.6.4.3.1 Command words.
Time exchange command words Time Is and Time Request that are used to request and to provide time of day (TOD) data, shall be formatted as shown in figure A-38. The three most-significant bits (W1-3) shall contain the standard CMD preamble (110). The next seven bits (W4-10) 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 in accordance with A.5.6.4.6.

A.5.6.4.3.2 Time Is command.
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 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, in accordance with table A-XXII and A.5.6.4.6. When a protocol requires transmission of the 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 1s.

A.5.6.4.3.3 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 1s, and the ticks field set to 30 (11110).

A.5.6.4.3.4 Other encodings.
All encodings of the seconds and ticks fields not specified here are reserved, and shall not be used until standardized.

A.5.6.4.4 Coarse time word.
Coarse time words shall be formatted as shown in figure A-39, and shall contain the coarse time current as of the beginning of that word.

Time Service Example Date=8 May Time=15:57:34:12 Time Quality=4				
3	7	3	6	5
CMD	Time Exchange	Time Quality	Seconds	40 ms ticks
110	1111110	100	100010	00011
“TIME IS” Command				

FIGURE A-38. Time exchange CMD word.

A.5.6.4.5 Authentication word.
Authentication words, formatted as shown in figure A-39, 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 exchange message preceding the authentication word (starting with the Time Is or Time Request command word which begins the message) shall be exclusive-or’d.

b. If the message to be authenticated is in response to a previous time exchange message, the authenticator from that message shall be exclusive-or’d with the result of (1).

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

A.5.6.4.6 Time quality.
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 A-XXII shall be employed for this purpose. The time uncertainty windows on the table are upper bounds on total uncertainty (with respect to coordinated universal time).

TABLE A-XXII. 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
NOTE: Time quality "0" shall be used only by UTC time standard stations.	

Time Service Example

Date = 8 May
Time = 15:57:34:12
Time Quality = 4

3	1	4	5	11
DATA	**0**	**Month**	**Day**	**Minute**
000	**0**	**0101**	**01000**	**011101111101**

Coarse Time Word

3	21
REP	**Authenticator**
111	**11010111001111111110**

Authenticator Word (over CMD and Coarse Time Words)

FIGURE A-39. Coarse time and authentication words.

For example, an uncertainty of ±6 seconds is 12 seconds total and requires a transmitted time quality value of 6. Stations shall power up from a cold start with a time quality of 7. Time

uncertainty is initialized when time is entered (see B.5.2.2.1) and shall be maintained thereafter as follows:

a. 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).

b. 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.

A station accepting time from another station shall add its own uncertainty due to processing and propagation delays to determine its new 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, say ±100 ms, and a propagation delay bound of ±35 ms, to obtain a new time uncertainty of ±185 ms, or 370 ms total, for a time quality of 3. 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. 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. Therefore, such a radio, which has been powered-off for much over three days, shall not be presumed to retain even coarse sync, despite its backup clock, and may require manual entry of time.

A.5.6.5 Mode control functions (optional).
If any of these features are selected, however, they shall be implemented in accordance with this standard. 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 CMD is used to select many of these operating modes, as described in the following paragraphs. The CMD word shall be formatted as shown in figure A-40. The first character shall be ‘m’ to identify the mode control command; the second character identifies the type of mode selection being made; the remaining bits specify the new setting for that mode.

3	7	7	7
CMD	1101101 (‘m’: mode control)	Mode ID	Mode Selection

FIGURE A-40. Mode control CMD format.

A.5.6.5.1 Modem negotiation and handoff.
An ALE data link can be used to negotiate a modem to be used for data traffic by exchanging modem negotiation messages. A modem negotiation message shall contain one modem selection command.

NOTE: This function may best be implemented in a high frequency node controller (HFNC) to avoid retrofit to existing ALE controllers, and for the greater flexibility inherent in network management information bases.

A.5.6.5.1.1 Modem selection CMD.
The modem selection CMD word shall be formatted as shown in figure A-41, and may be followed by one or more DATA words, as described below. The defined modem codes are listed in table A-XXIII. Codes not defined are reserved, and shall not be used until standardized.

3	7	7	7
CMD	1101101 (‘m’: mode control)	1101110 (‘n’: modem select)	Modem Code

FIGURE A-41. Modem selection CMD format.

A.5.6.5.1.2 Modem negotiating.

Modem negotiating shall employ modem negotiation messages in the following protocol:

a. The station initiating the negotiation will send a modem selection CMD word containing the code of the modem it wants to use.

b. The responding station(s) may either accept this modem selection or suggest alternatives. A station accepting a suggested modem shall send a modem selection CMD word containing the code of that modem.

c. A station may negotiate by sending a modem selection CMD word containing all 1s in the modem code field, followed by one or more DATA words containing the codes of one or more suggested modems. Modem codes shall be listed in order of preference in the DATA word(s). Unused positions in the DATA word(s) shall be filled with the all 1s code.

d. The negotiation is concluded when the most recent modem negotiation message from all participating stations contains an identical modem selection CMD word with the same modem code (not all 1s). When this occurs, the station that initiated the negotiation will normally begin sending traffic using the selected modem.

TABLE A-XXIII. Modem codes.

Code		Modem Type
0000000		(Reserved)
0000001		ALE modem
0000010		Serial-tone HF data modem (MIL-STD-188-110)
0000011		16-tone DPSK HF data modem (MIL-STD-188-110)
0000100		39-Tone HF data modem (MIL-STD-188-110)
0000101		ANDVT
0000110		FSK 170 Hz shift (MIL-STD-188-110)
0000111		FSK 850 Hz shift (MIL-STD-188-110)
Short intlv	(010xxxx) long intlv	STANAG 4285
0100000	0101000	75 b/s
0100001	0101001	150 b/s
0100010	0101010	300 b/s
0100011	0101011	600 b/s
0100100	0101100	1200 b/s
0100101	0101101	2400 b/s
0100110	0101110	4800 b/s
(011xxxx)		STANAG 4529:
0110000	0111000	75 b/s
0110001	0111001	150 b/s
0110010	0111010	300 b/s
0110011	0111011	600 b/s
0110100	0111100	1200 b/s
0110101	0111101	2400 b/s
0110110	0111110	4800 b/s
1111111		Reserved to indicate no modem code. (All others reserved until defined)

A.5.6.5.2 Crypto negotiation and handoff.
When crypto negotiation and handoff are required, the following applies:

a. An ALE data link can also be used to negotiate an encryption device to be used for voice or data traffic by exchanging crypto negotiation messages. The crypto selection CMD word is formatted as shown in figure A-42. The defined crypto codes are listed in table A-XXIV. Codes not defined are reserved, and shall not be used until standardized.

NOTE: This function may best be implemented in an HFNC to avoid retrofit to existing ALE controllers, and for the greater flexibility inherent in network management information bases.

3	7	7	7
CMD	1101101 (‘m’: mode control)	1100011 (‘c’: crypto select)	Crypto Code

FIGURE A-42. Crypto selection CMD format.

TABLE A-XXIV. Crypto codes.

Code	Crypto Type
0000000	No encryption
1111111	Reserved to indicate no crypto code
	(All others reserved until defined)

b. Crypto negotiation shall employ crypto negotiation messages in the protocol described above for modem negotiation.

A.5.6.6 Capabilities reporting functions.

A.5.6.6.1 Version CMD (mandatory).
The version CMD function is used to request ALE controller version identification. The first character is 'v' to indicate the version family of ALE CMD word functions. The second character shall be set to 's' to select a summary report.

NOTE: The capabilities function in A.5.6.6.2 is a variant of this function that provides more detailed information.

a. The response to a version CMD is a printable ASCII message in manufacturer-specific format that indicates a manufacturers' identification, the version(s) of hardware, operating firmware and software, and/or management firmware and software of the responding ALE controller, as requested by control bits KVC_{1-3} of the version CMD format (see figure A-43 and table A- XXV).

3	7	7	3	4
CMD	1110110 ('v': version CMD)	1110011 ('s': summary)	Comps (KVC)	Formats (KVF)

FIGURE A-43. Version CMD format.

TABLE A-XXV. Component selection.

Bit	Component whose version is requested when bit set to 1
KVC3 (MSB)	ALE controller hardware
KVC2	ALE controller operating firmware
KVC1 (LSB)	ALE controller network management firmware (i.e., HNMP)

b. The requesting station specifies acceptable formats for the response in control bits KVF_{1-4} in accordance with table A-XXVI. A controller responding to a version function shall attempt to maximize the utility of its response and:

(1) Shall report the version(s) of all of the components requested by the KVC control bits that are present in the controller.

(2) Shall use the ALE message format that represents the highest level of mutual capability of itself and the requesting station by comparing the message types that it can generate with those desired by the requesting station, and selecting the message type in the intersection of these two sets that correspond to the highest-numbered KFV bit.

TABLE A-XXVI. Format selection.

Bit	Reporting format desired when bit set to 1
KVF4 (MSB)	Reserved (always set to 0)
KVF3	DBM
KVF2	DTM
KVF1 (LSB)	AMD Message

A.5.6.6.2 Capabilities function. (mandatory).
The capabilities function is used to obtain a compact representation of the features available in a remote ALE controller. This function uses a variant of the version CMD word, as shown in figures A-44 and A-45.

A.5.6.6.2.1 Capabilities query.
The capabilities query, shown in figure A-44, consists of a single ALE CMD word. The second character position shall be set to ‘c’ to select a full capabilities report (rather than a summary as in the version CMD). The third character position shall be set to ‘q’ in a capabilities query to request a capabilities report.

3	7	7	7
CMD	1110110 (‘v’: version CMD)	1100011 (‘c’: capability)	1110001 (‘q’: query)

FIGURE A-44. Capabilities query CMD format.

A.5.6.6.2.2 Capabilities report CMD.
The capabilities report shall consist of a CMD word followed by five DATA words, as shown in figure A-45. The second character position of the capabilities report CMD word shall be set to ‘c’ and the third character position shall be set to ‘r’. (The DATA preamble in the second and fourth DATA words shall be replaced by REP for transmission, as required by the ALE protocol).

3	7	7	7
CMD	1110110 (‘v’: version CMD)	1100011 (‘c’: capability)	1110010 (‘r’: report)

3	5	8	8
DATA	Scan Rate (SR_{1-5})	Channels Scanned (CS_{1-8})	Max Tune Time (TT_{1-8})

3	4	4	3	5	5
DATA	Turnaround (TTA_{1-4})	Timeout (TWA_{1-4})	Listen (TWT_{1-3})	Polling (PP_{1-5})	LP Levels (LPL_{1-5})

3	6	7	8
DATA	LP Time (LPT_{1-6})	ALE Protocols (VAP_{1-7})	ALQA ($ALQA_{1-8}$)

3	8	8	5
DATA	Orderwire (OW_{1-8})	Reserved	Reserved

3	21
DATA	Scheduling (SCH_{1-21})

FIGURE A-45. Capabilities report CMD and DATA format.

A.5.6.6.2.3 Data format.

The format of the DATA words in a capabilities report is constant, regardless of the capabilities reported, to simplify the software that implements the capabilities command. The data fields of the capabilities report shall be encoded in accordance with tables A-XXVII, A-XXVIII, and A-XXIX. The values encoded shall represent the current operational capabilities of the responding ALE controller, i.e., the timing or functions currently programmed. All timing fields shall be encoded as unsigned integers.

TABLE A-XXVII. Capabilities report data fields (ALE timing).

Group	Field	Value	Units	Parameter from table A-XV "Timing"
ALE Timing	SR_{1-5}	Scan rate	Channels/s	$1/T_d$
	CS_{1-8}	Chan. scanned		C
	TT_{1-8}	Max tune time	100 ms	T_t
	TTA_{1-4}	Turnaround time	100 ms	T_{ta}
	TWA_{1-4}	Activity timeout	$\log_2$ s	T_{wa}*
	TWT_{1-3}	Listen time	1 s	T_{wt}
* $T_{wa}=\log_2 n$ where n is the number of seconds of no detected activity before timeout.				

TABLE A-XXVIII. Capabilities report data fields (mode settings).

Group	Bit	Set to 1 if and only if (iff)	Cross Ref: MIL-STD
ALE Protocols	VAP_7 (MSB)	Accepting ALL calls	188-141 (Allcalls)
	VAP_6	Accepting ANY calls	188-141 (AnyCalls)
	VAP_5	Accepting AMD 2msgs	188-141 (AMD mode)
	VAP_4	Accepting DTM msgs	188-141 (DTM mode)
	VAP_3	Accepting DBM msgs	188-141 (DBM mode)
	VAP_2	DTM capabilities	188-141 (DTM mode)
	VAP_1 (LSB)	DBM capabilities	188-141 (DBM mode)
LP Levels	LPL_5 (MSB)	Capable of other LP	
	LPL_4	Capable of AL-4 LP	188-141 Appendix B
	LPL_3	Capable of AL-3 LP	188-141 Appendix B
	LPL_2	Capable of AL-2 LP	188-141 Appendix B
	LPL_1 (LSB)	Capable of AL-1 LP	188-141 Appendix B
Time Ex-change	LPT_6 (MSB)	Acting as time server	188-141 (Time service response, Time service response (non-protected))
	LPT_5	Active time acq. enable	188-141 (Active time acquisition (protected), Active time acquisition (non-protected))
	LPT_4	Passive time acq. enable	188-141 (Passive time acquisition)
	LPT_3	Will send time broadcasts	188-141 (Time broadcast)
	LPT_2	Time iteration capable	(not yet standardized)
	LPT_1 (LSB)	Precision time capable	(not yet standardized)

TABLE A-XXIX. Capabilities report data field (feature capabilities).

Group	Bit	Set to 1 iff Feature Implemented	Cross Ref: MIL-STD (paragraph)
Polling	PP_5 (MSB)	Full Net Poll	(not yet standardized)
	PP_4	Full Group Poll	(not yet standardized)
	PP_3	Channel Scan CMD	(not yet standardized)
	PP_2	LQA Report	(not yet standardized)
	PP_1 (LSB)	Local Noise Report	188-141 (Local Noise Report)
ALQA	$ALQA_8$ (MSB)	Reserved (always set to 0)	(not yet standardized)
	$ALQA_7$	ALQA SINAD	(not yet standardized)
	$ALQA_6$	ALQA PBER	(not yet standardized)
	$ALQA_5$	ALQA AI	(not yet standardized)
	$ALQA_4$	ALQA SD	(not yet standardized)
	$ALQA_3$	ALQA EFI	(not yet standardized)
	$ALQA_2$	ALQA AVQ	(not yet standardized)
	$ALQA_1$ (LSB)	ALQA ADC	(not yet standardized)
Orderwire	OW_8 (MSB)	Frequency Select CMD	(not yet standardized)
	OW_7	Channel Select CMD	(not yet standardized)
	OW_6	Modem Negotiation	188-141 (Modem Negotiation and Handoff)
	OW_5	Crypto Negotiation	188-141 (Crypto Negotiation and handoff)
	OW_4	Analog Port Selection	(not yet standardized)
	OW_3	Data Port selection	(not yet standardized)
	OW_2	Digital Squelch	(not yet standardized)
	OW_1 (LSB)	Power Control	(not yet standardized)
Scheduling	SCH_{21} (MSB)	Reserved (always set to 0)	
	SCH_{20}	Adjust Slot Width	(not yet standardized)
	SCH_{19}	Station Busy	(not yet standardized)
	SCH_{18}	Channel Busy	(not yet standardized)
	SCH_{17}	Set Dwell Time	(not yet standardized)
	SCH_{16}	Halt and Wait	(not yet standardized)
	SCH_{15}	Contact Later	(not yet standardized)
	SCH_{14}	Meet Me	(not yet standardized)
	SCH_{13}	Poll Operator (default NAK)	(not yet standardized)
	SCH_{12}	Request Operator ACK	(not yet standardized)
	SCH_{11}	Schedule Periodic Function	(not yet standardized)
	SCH_{10}	Quiet Contact	(not yet standardized)
	SCH_9	Respond and Wait	(not yet standardized)
	SCH_8	Set Sounding Interval	(not yet standardized)
	SCH_7	Tune and wait	(not yet standardized)
	SCH_6	Set Slot Width	(not yet standardized)
	SCH_5	Year and Date	(not yet standardized)
	SCH_4	Zulu Time	(not yet standardized)
	SCH_3	Do Not Respond	188-141 (Do Not Respond)
	SCH_2	Reserved (always set to 0)	
	SCH_1 (LSB)	Reserved (always set to 0)	

A.5.6.7 Do not respond CMD.
When an ALE controller receives this CMD in a transmission, it shall not respond unless a response is specifically required by some other CMD in the transmission (e.g., an LQA request or a DTM or DBM with ARQ requested). In a Do Not Responds CMD, no three-way ALE handshake needs to be completed.

A.5.6.8 Location report (optional).
not yet standardized.

A.5.6.9 User unique functions (UUFs).
UUFs are for special uses, as coordinated with specific users or manufacturers, which use the ALE system in conjunction with unique, nonstandard, or non-ALE, purposes. There are 16384 specific types of CMD UUF codes available, as indicated by a 14-bit (or two-character) unique index (UI). Each unique type of special function that employees a UUF shall have a specific UI assigned to it to ensure interoperability, compatibility, and identification. The UI shall be assigned for use before any transmission of the UUF or the associated unique activity, and the ALE UUF shall always include the appropriate UI when sent.

The UUF shall be used only among stations that are specifically addressed and included within the protocol, and shall be used only with stations specifically capable of participating in the UUF activity, and all other (non-participating) stations should be terminated. There are two exceptions for stations that are not capable of participating in the UUF and are required to be retained in the protocol until concluded. They shall be handled using either of the two following procedures. First, the calling station shall direct all the addressed and included stations to stay linked for the duration of the UUF, to read and use anything that they are capable of during that time, and to resume acquisition and tracking of the ALE frame and protocol after the UUF ends. To accomplish this, and immediately before the CMD UUF, the sending station shall send the CMD STAY, which shall indicate the time period (T) for which the receiving stations shall wait for resumption of the frame and protocol. Second, the sending station shall use any standard CMD function to direct the non-participating stations to wait or return later, or do anything else appropriate and controllable through the standard orderwire functions.

If a CMD UUF is included within an ALE frame, it shall only be within the message section. The UUF activity itself should be conducted completely outside of the frame and should not interfere with the protocols. If the UUF activity itself must be conducted within the message section, will occupy time on the channel, and is incompatible with the ALE system, that activity shall be conducted immediately after the CMD UUF and it shall be for a limited amount of time (T). A CMD STAY shall precede the UUF instruction, as described herein, to indicate that time (T). The sending station shall resume the same previous redundant word phase when the frame and protocol resumes, to ensure synchronization. The STAY function preserves maintenance of the frame and link. It instructs the stations to wait, because the amount of time occupied by the UUF activity or its signaling may conflict with functions such as the wait-for-activity timer (T_{wa}). This may interfere with the protocols or maintenance of the link. In any case, the users of

the UUF shall be responsible for noninterference with other stations and users, and also for controlling their own stations and link management functions to avoid these conflicts.

The UUF shall be constructed as follows and as shown in table A-XXX. The UUF word shall use the CMD (110) preamble in bits P3 through P1 (W1 through W3). The character in the first position shall be the pipe "¦" or vertical bar "|" (1111100) in bits C1-7 through C1-1 (W4 through W10), which shall identify the "unique" function. The user or manufacturer-specific UI shall be a 14-bit (or two-character, 7-bit ASCII) code using bits UI-14 through UI-1 (W11 through W24). All unassigned UI codes shall be reserved and shall not be used until assigned for a specific use.

TABLE A-XXX. User unique functions structure.

	User Unique Function Bits		**Word Bits**	
CMD Preamble	MSB	P3=1	MSB	W1
		P2=1		W2
	LSB	P1=0		W3
First Character |	MSB	C1 (bit-7) =1		W4
		C1 (bit-6)=1		W5
		C1 (bit-5) =1		W6
		C1 (bit-4) =1		W7
		C1 (bit-3) =1		W8
		C1 (bit-2) =0		W9
	LSB	C1 (bit-1) =0		W10
First UI Character	MSB	UI-1-7		W11
		UI-1-6		W12
		UI-1-5		W13
		UI-1-4		W14
		UI-1-3		W15
		UI-1-2		W16
	LSB	UI-1-1		W17
Second UI Character	MSB	UI-2-7		W18
		UI-2-6		W19
		UI-2-5		W20
		UI-2-4		W21
		UI-2-3		W22
		UI-2-2		W23
	LSB	UI-2-1	LSB	W24

NOTES:
1. CMD user unique functions first character is "¦" (1111100) for "unique."
2. Unique index (UI) characters UI-1 and UI-2 from central registry and assignment.

A.5.7 ALE message protocols.

A.5.7.1 Overview.
Three message protocols are available for carrying user data using the ALE waveform and signal structure. The characteristics of these three protocols are summarized in the table A-XXXI. All ALE controllers complying with this appendix shall implement the AMD protocol.

TABLE A-XXXI. ALE message protocols.

Protocol	Mandatory	Character Set	Peak Through-put	ARQ
AMD	Y	Expanded 64	55 b/s	N
DTM	N	unrestricted	61 b/s	Opt
DBM	N	unrestricted	187 b/s	Opt

A.5.7.2 AMD mode (mandatory).
The operators and controllers shall be able to send and receive simple ASCII text messages using only the existing station equipment.

A.5.7.2.1 Expanded 64-channel subset.
The expanded 64 ASCII subset shall include all capital alphabetics (A-Z), all digits (0-9), the utility symbols "@" and "?," plus 26 other commonly used symbols. See figure A-46. The expanded 64 subset shall be used for all basic orderwire message functions, plus special functions as may be standardized. For orderwire message use, the subset members shall be enclosed within a sequence of DATA (and REP) words and shall be preceded by an associated CMD (such as DTM). The CMD designates the usage of the information that follows, and shall also be preceded by a valid and appropriate calling cycle using the Basic 38 ASCII subset addressing. Digital discrimination of the expanded 64 ASCII subset may be accomplished by examination of the two MSBs (b_7 and b_6), as all of the members within the "01" and "10" MSBs are acceptable. No parity bits are transmitted because the integrity of the information is protected by the basic ALE FEC and redundancy and may be ensured by optional use of the CMD CRC as described in A.5.6.1. The station shall have the capability to both send and receive AMD messages from and to both the operator and the controller. The station shall also have the capability to display any received AMD messages directly to the operator and controller upon arrival, and to alert them. The operator and controller shall have the capability to disable the display and the alarm when their functions would be operationally inappropriate.

BITS b_7 b_6 b_5				0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
b_4	b_3	b_2	b_1	COLUMN / ROW	0	1	2	3	4	5	6	7
0	0	0	0	0	**NUL**	**DLE**	**SP**	0	@	P	**`**	**p**
0	0	0	1	1	**SOH**	**DC1**	**!**	1	A	Q	**a**	**q**
0	0	1	0	2	**STX**	**DC2**	**"**	2	B	R	**b**	**r**
0	0	1	1	3	**ETX**	**DC3**	**#**	3	C	S	**c**	**s**
0	1	0	0	4	**EOT**	**DC4**	**$**	4	D	T	**d**	**t**
0	1	0	1	5	**ENQ**	**NAK**	**%**	5	E	U	**e**	**u**
0	1	1	0	6	**ACK**	**SYN**	**&**	6	F	V	**f**	**v**
0	1	1	1	7	**BEL**	**ETB**	**'**	7	G	W	**g**	**w**
1	0	0	0	8	**BS**	**CAN**	**(**	8	H	X	**h**	**x**
1	0	0	1	9	**HT**	**EM**	**)**	9	I	Y	**i**	**y**
1	0	1	0	10	**LF**	**SUB**	*****	**:**	J	Z	**j**	**z**
1	0	1	1	11	**VT**	**ESC**	**+**	**;**	K	**[**	**k**	**{**
1	1	0	0	12	**FF**	**FS**	**,**	<	L	\	**l**	**|**
1	1	0	1	13	**CR**	**GS**	**-**	=	M	**]**	**m**	**}**
1	1	1	0	14	**SO**	**RS**	**.**	>	N	^	**n**	**~**
1	1	1	1	15	**SI**	**US**	**/**	?	O	**?**	**o**	**DEL**

FIGURE A-46. Expanded 64 ASCII subset (shown unshaded).

A.5.7.2.2 AMD protocol.

When an ASCII short orderwire AMD type function is required, the following CMD AMD protocol shall be used, unless another protocol in this standard is substituted. An AMD message shall be constructed in the standard word format, as described herein, and the AMD message shall be inserted in the message section of the frame. The receiving station shall be capable of receiving an AMD message contained in any ALE frame, including calls, responses, and acknowledgments. Within the AMD structure, the first word shall be a CMD AMD word, which shall contain the first three characters of the message. It shall be followed by a sequence of alternating DATA and REP words that shall contain the remainder of the message. The CMD, DATA, and REP words shall all contain only characters from the expanded ASCII 64 subset, which shall identify them as an AMD transmission. Each separate AMD message shall be kept intact and shall only be sent in a single frame, and in the exact sequence of the message itself. If one or two additional characters are required to fill the triplet in the last word sent, the position(s) shall be "stuffed" with the "space" character (0100000) automatically by the controller, without operator action. The end of the AMD message shall be indicated by the start of the frame conclusion, or by the receipt of another CMD. Multiple AMD messages may be sent within a frame, but they each shall start with their own CMD AMD with the first three characters.

A.5.7.2.3 Maximum AMD message size.
Receipt of the CMD AMD word shall warn the receiving station that an AMD message is arriving and shall instruct it to alert the operator and controller and display the message, unless they disable these outputs. The station shall have the capability to distinguish among, and separately display, multiple separate AMD messages that were in one or several transmissions.
The AMD word format shall consist of a CMD (110) in bits P3 through P1 (W1 through W3), followed by the three standard character fields C1, C2, and C3. In each character field, each character shall have its most significant bits (MSBs) bit 7 and bit 6 (C1-7 and C1-6, C2-7 and C2-6, and C3-7 and C3-6) set to the values of "01" or "10" (that is, all three characters are members of the expanded ASCII 64 subset). The rest of the AMD message shall be constructed identically, except for the alternating use of the DATA and REP preambles.

Any quantity of AMD words may be sent within the message section of the frame within the $T_{m\ max}$ limitation of 30 words (90 characters). $T_{m\ max}$ shall be expanded from 30 words, to a maximum of 59 words, with the inclusion of CMD words within the message section. The maximum AMD message shall remain 30 words, exclusive of additional CMD words included within the message section of the frame. The maximum number of CMD words within the message section shall be 30. The message characters within the AMD structure shall be displayed verbatim as received. If a detectable information loss or error occurs, the station shall warn of this by the substitution of a unique and distinct error indication, such as all display elements activated (like a "block"). The display shall have a capacity of at least 20 characters (DO: at least 40). The AMD message storage capacity, for recall of the most recently received message(s), shall be at least 90 characters plus sending station address. (DO: at least 400). By operator or controller direction, the display shall be capable of reviewing all messages in the AMD memory and shall also be capable of identifying the originating station's address. If words are received that have the proper AMD format but are within a portion of the message section under the control of another message protocol (such as DTM), the other protocol shall take precedence and the words shall be ignored by the station's AMD function.

NOTE: If higher data integrity or reliability is required, the CMD DTM and DBM protocols should be used.

A.5.7.3 DTM mode (optional).
The DTM ALE (orderwire) message protocol function enables stations to communicate (full ASCII or unformatted binary bits) messages to and from any selected station(s) for direct output to and input from associated data terminals or other date terminal equipment (DTE) devices through their standard data circuit-terminating equipment (DCE) ports. The DTM data transfer function is a standard speed mode (like AMD) with improved robustness, especially against weak signals and short noise bursts. When used over medium frequency (MF)/HF by the ALE system, DTM orderwire messages may be unilateral or bilateral, and broadcast or acknowledged. As the DTM data blocks are of moderate sizes, this special orderwire message function enables utilization of the inherent redundancy and FEC techniques to detect weak HF signals and tolerate short noise bursts.

The DTM data blocks shall be fully buffered at each station and should appear transparent to the using DTEs or data terminals. As a DO, and under the direction of the operator or controller, the stations should have the capability of using the DTM data traffic mode (ASCII or binary bits) to control switching of the DTM data traffic to the appropriate DCE port or associated DTE equipment, such as to printers and terminals (if ASCII mode), or computers and cryptographic devices (if binary bits mode). As an operator or controller selected option, the received DTM message may also be presented on the operator display similar to the method for AMD in A.5.7.2.

There are four CMD DTM modes: BASIC, EXTENDED, NULL, and ARQ. The DTM BASIC block ranges over a moderate size and contains a variable quantity of data, from zero to full as required, which is exactly measured to ensure integrity of the data during transfer. The DTM EXTENDED blocks are variable over a larger range of sizes, in integral multiples of the ALE basic word, and are filled with integral multiples of message data. The DTM NULL and ARQ modes are used for both link management, and error and flow control. The characteristics of the CMD DTM orderwire message functions are listed in table A-XXXII and are summarized below:

CMD DTM Mode	BASIC	EXTENDED	ARQ NULL
Maximum Size, Bits	651	7371	0
Cyclic Redundancy Check	16 Bits	16 Bits	0
Data Capacity, ASCII	0-93	3-1053, by 3	0
Data Capacity, Bits	1-651	21-7371, by 21	0
ALE Word Redundancy	3 Fixed	3 Fixed	0
Data Transmission	392 ms - 12.152 sec	392 ms - 2.29 min	0

TABLE A-XXXII. DTM characteristics.

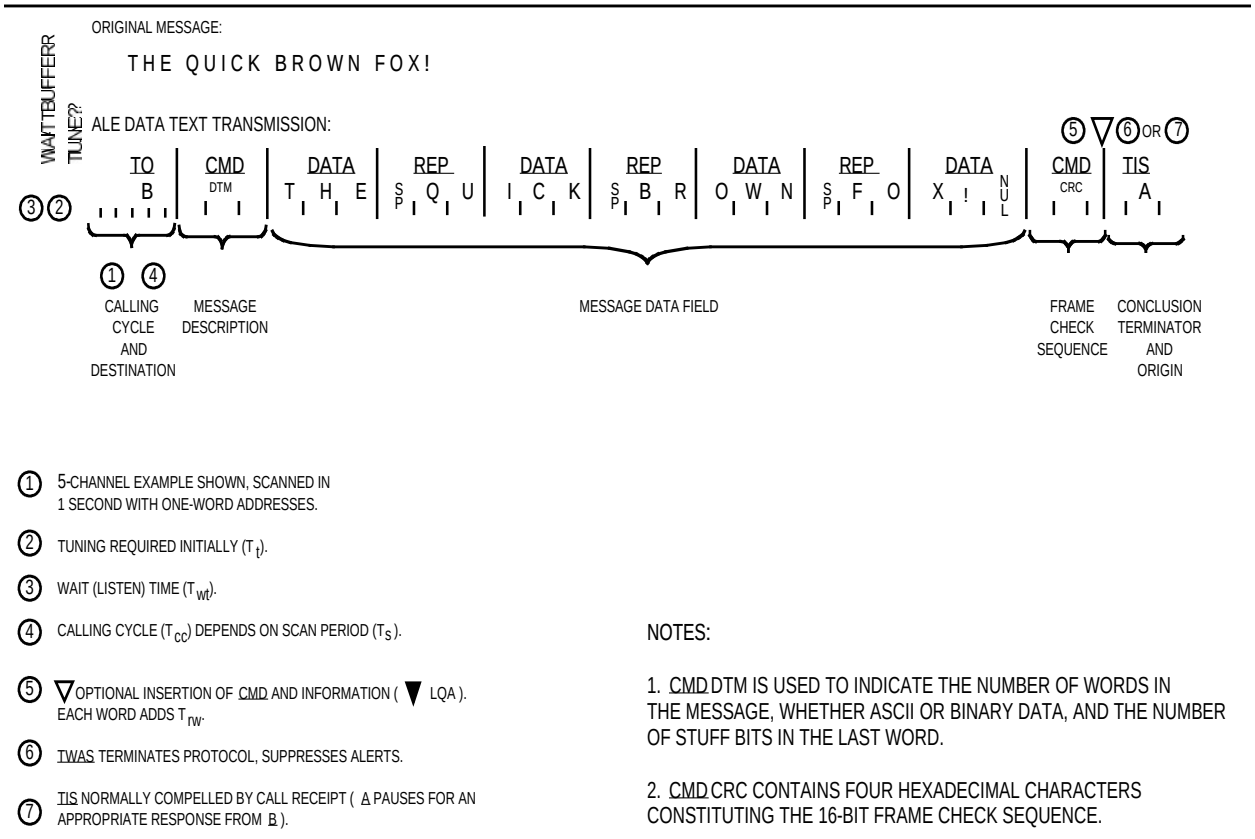
	WORD BITS		DTM CODE (DC) DECIMAL (n)	DATA WORDS (w)	BINARY BITS DATA	ASCII CHAR DATA	DATA TIME	TOTAL DTM (T_{rw})
	W 15----W 19	W 20----W 24						
	DTM CODE BITS							
	DC 10----DC 6	DC 5----DC 1						
DTM NULL*	0 0 0 0 0	0 0 0 0 0	0	0*	0	0	0	1*
DTM EXTENDED (FULL)	0 0 0 0 0	0 0 0 0 1	1	1	21	3	392 ms	3
	0 0 0 0 0	0 0 0 1 0	2	2	42	6	784 ms	4
	↓ ↓ ↓ ↓ ↓	↓ ↓ ↓ ↓ ↓		n	21n	3n	nx392 ms	n+2
	0 1 0 1 0	1 1 1 1 0	350	350	7350	1050	2.28 min	352
	0 1 0 1 0	1 1 1 1 1	351	351	7371	1053	2.29 min	353
DTM ARQ*	0 1 0 1 1	0 0 0 0 0	352	0*	0	0	0	1*
(RESERVED)*	(12≤m≤31	0 0 0 0 0	32m	---	---	---	---	---
DTM BASIC (EXACT)	0 1 0 1 1	(01≤p≤31)	352+p	p	(21p+m-31)	3(p-1 to p)	px392 ms	p + 2
	0 1 1 0 0		384+p	↓	↓	↓	↓	↓
	↓ ↓ ↓ ↓ ↓		32m+p					
	1 1 1 1 0		960+p					
	1 1 1 1 1	(01≤p≤31)	992+p	p	(21p+m-31)	3(p-1 to p)	px392 ms	p + 2
	(11≤m≤31)	0 0 0 0 1	32m+1	1	1-21	0-3	392 ms	w + 2
		0 0 0 1 0	32m+2	2	22-42	3-6	784 ms	↓
		↓ ↓ ↓ ↓ ↓	32m+p	p	(21p+m-31)	3(p-1 to p)	px392 ms	
		1 1 1 1 0	32m+30	30	610-630	87-90	11.760 s	
	(11≤m≤31)	1 1 1 1 1	32m+31	31	631-651	90-93	12.152 s	w + 2

NOTE:
1. * - NO CMD CRC USED.
2. m - BINARY BITS IN LAST WORD + 10.
3. p = DTM DATA WORDS.

This Page Intentionally Blank

When an ASCII, or binary bit, digital data message function is required, the following CMD DTM orderwire structures and protocols shall be used as specified herein, unless another standardized protocol is substituted. The DTM structure shall be inserted within the message section of the standard ALE frame. A CMD DTM word shall be constructed in the standard 24-bit format, using the CMD preamble (see table A-XXXIII). The message data to be transferred shall also be inserted in words, using the DATA and REP preambles. The words shall then be Golay FEC encoded and interleaved, and then shall be transmitted immediately following the CMD DTM word. A CMD CRC shall immediately follow the data block words, and it shall carry the error control CRC FCS.

When the DTM structure transmission time exceeds the maximum limit for the message section ($T_{m\ max}$), the DTM protocol shall take precedence and shall extend the T_m limit to accommodate the DTM. The DTM mode preserves the required consistency of redundant word phase during the transmission. The message expansion due to the DTM is always a multiple of one T_{rw}, as the basic ALE word structure is used. The transmission time of the DTM data block (DTM words x 392 ms) does not include the T_{rw} for the preceding CMD DTM word or the following CMD CRC. Figure A-47 shows an example of a DTM message structure.



1. 5-CHANNEL EXAMPLE SHOWN, SCANNED IN 1 SECOND WITH ONE-WORD ADDRESSES.
2. TUNING REQUIRED INITIALLY (T_t).
3. WAIT (LISTEN) TIME (T_{wt}).
4. CALLING CYCLE (T_{cc}) DEPENDS ON SCAN PERIOD (T_S).
5. ▽ OPTIONAL INSERTION OF CMD AND INFORMATION (▼ LQA). EACH WORD ADDS T_{rw}.
6. TWAS TERMINATES PROTOCOL, SUPPRESSES ALERTS.
7. TIS NORMALLY COMPELLED BY CALL RECEIPT (A PAUSES FOR AN APPROPRIATE RESPONSE FROM B).

NOTES:

1. CMD DTM IS USED TO INDICATE THE NUMBER OF WORDS IN THE MESSAGE, WHETHER ASCII OR BINARY DATA, AND THE NUMBER OF STUFF BITS IN THE LAST WORD.

2. CMD CRC CONTAINS FOUR HEXADECIMAL CHARACTERS CONSTITUTING THE 16-BIT FRAME CHECK SEQUENCE.

FIGURE A-47. DTM structure example.

The DTM protocol shall be as described herein. The CMD DTM BASIC and EXTENDED formats (herein referred to as DTM data blocks) shall be used to transfer messages and information among stations. The CMD DTM ARQ format shall be used to acknowledge other CMD DTM formats and for error and flow control, except for non-ARQ and one-way broadcasts. The CMD DTM NULL format shall be used to (a) interrupt ("break") the DTM and message flow, (b) to interrogate station to confirm DTM capability before initiation of the DTM message transfer protocols, and (c) to terminate the DTM protocols while remaining linked. When used in ALE handshakes and subsequent exchanges, the protocol frame terminations for all involved stations shall be TIS until all the DTM messages are successfully transferred, and all are acknowledged if ARQ error control is required. The only exceptions shall be when the protocol is a one-way broadcast or the station is forced to abandon the exchange by the operator or controller, in which cases the termination should be TWAS.

Once a CMD DTM word of any type has been received by a called (addressed) or linked station, the station shall remain on channel for the entire specified DTM data block time (if any), unless forced to abandon the protocol by the operator or controller. The start of the DTM data block itself shall be exactly indicated by the end of the CMD DTM BASIC or EXTENDED word itself. The station shall attempt to read the entire DTM data block information in the DATA and REP words, and the following CMD CRC, plus the expected frame continuation, which shall contain a conclusion (possibly preceded by additional functions in the message section, as indicated by additional CMD words).

With or without ARQ, identification of each DTM data block and its associated orderwire message (if segmented into sequential DTM data blocks) shall be achieved by use of the sequence and message control bits, KD1 and KD2, (as shown in table A-XXXIII), which shall alternate with each DTM transmission and message, respectively. The type of data contained within the data block (ASCII or binary bits) shall be indicated by KD3 as a data identification bit. Activation of the ARQ error control protocol shall use the ARQ control bit KD4. If no ARQ is required, such as in one-way broadcasts, multiple DTM data blocks may be sent in the same frame, but they shall be in proper sequential order if they are transferring a segmented message.

When ARQ error or flow control is required, the CMD DTM ARQ shall identify the acknowledged DTM data block by the use of the sequence and message control bits KD1 and KD2, which shall be set to the same values as the immediately preceding and referenced DTM data block transmission. Control bit KD3 shall be used as the DTM flow control to pause or continue (or resume) the flow of the DTM data blocks. The ACK and request-for-repeat (NAK) functions shall use the ARQ control bit KD4. If no ARQ has been required by the sending station, but the receiving station needs to control the flow of the DTM data blocks, it shall use the DTM ARQ to request a pause in, and resumption of, the flow.

TABLE A-XXXIII. DTM structure.

	DTM Bits		Word Bits	
CMD preamble	MSB	P3=1	MSB	W1
		P2=1		W2
	LSB	P1=0		W3
First character "d"	MSB	C1 (bit-7) = 1		W4
		C1 (bit-6) = 1		W5
		C1 (bit-5) = 0		W6
		C1 (bit-4) = 0		W7
		C1 (bit-3) = 1		W8
		C1 (bit-2) = 0		W9
	LSB	C1 (bit-1) = 0		W10
Control bits	MSB	KD4		W11
		KD3		W12
		KD2		W13
	LSB	KD1		W14
DTM data code bits	MSB	DC10		W15
		DC9		W16
		DC8		W17
		DC7		W18
		DC6		W19
		DC5		W20
		DC4		W21
		DC3		W22
		DC2		W23
	LSB	DC1	LSB	W24

NOTES:

1. CMD DTM and DTM ARQ first character is "d" for "data".
2. With DTM transmission, control bit KD4 (W11) is set to "0" for no ACK request, and "1" for ACK request.
3. If a DTM ARQ transmission, control bit KD4 (W11) is set to "0" for binary bits, and "1" for 7-bit ASCII characters.
4. With DTM transmission, control bit KD3 (W12) is set to "0" for binary bits and "1" for 7-bit ASCII characters.
5. If a DTM ARQ transmission, control bit KD3 (W12) is set to "0" for flow continue, and "1" for flow pause.
6. With DTM transmissions, control bit KD2 (W13) is set (a) the same ("0" or "1") as the sequentially adjacent DTM(s) if the transmitted data field is to be reintegrated as part of a larger DTM, and (b) alternately different if independent from the prior adjacent DTM data field(s).
7. If a DTM ARQ transmission, control bit KD2 (W13) is set the same as the referenced DTM transmission.
8. With DTM transmission, control bit KD1 (W14) is set alternately to "0" and "1" in any sequence of DTMs, as a sequence control.
9. If a DTM ARQ transmission, control bit KD1 (W14) is set the same as the referenced DTM transmission.
10. Data Code (DC) bits are from table A-XXXII.

When data transfer ARQ error and flow control is required, the DTM data blocks shall be sent individually, in sequence, and each DTM data block shall be acknowledged before the next DTM data block is sent. Therefore, with ARQ there shall be only one DTM data block transmission in each ALE frame. If the transmitted DTM data block causes a NAK in the returned DTM ARQ, as described below, or if ACK or DTM ARQ is detected in the returned frame, or if no ALE frame is detected at all, the sending station shall resend an exact duplicate of the unacknowledged DTM data block. It shall send and continue to resend duplicates (which should be up to at least seven) one at a time and with appropriate pauses for responses, until the involved DTM data block is specifically acknowledged by a correct DTM ARQ. Only then shall the next DTM data block in the sequence be sent. If the sending station is frequently or totally unable to detect ALE frame or DTM ARQ responses, it should abort the DTM transfer protocol, terminate the link, and relink and reinitiate the DTM protocol on a better channel, under operator or controller direction.

Before initiation of the DTM data transfer protocols, the sending stations should confirm the existence of the DTM capability in the intended receiving stations, if not already known. When a DTM interrogation function is required, the following protocol shall be used. Within any standard protocol frame (using TIS), the sending station shall transmit a CMD DTM NULL, with ARQ required, to the intended station(s). These receiving stations shall respond with the appropriate standard frame and protocol, with the following variations. They shall include a CMD DTM ARQ if they are DTM capable, and they shall omit it if they are not DTM capable. The sending station shall examine the ALE and DTM ARQ responses for existence, correctness, and the status of the DTM KD control bits, as described herein. The transmitted CMD DTM NULL shall have its control bits set as follows: KD1 and KD2 set opposite of any subsequent and sequential CMD DTM BASIC or EXTENDED data blocks, which will be transmitted next; KD3 set to indicate the intended type of traffic, and KD4 set to require ARQ. The returned CMD DTM ARQ shall have its control bits set as follows: KD1 and KD2 set to match the interrogating DTM NULL; KD3 set to indicate if the station is ready for DTM data exchanges, or if a pause is requested; and KD4 set to ACK if the station is ready to accept DTM data transmissions with the specified traffic type, and NAK if it cannot or will not participate, or it failed to read the DTM NULL.

The sending (interrogating) station shall handle any and all stations that return a NAK, or do not return a DTM ARQ at all, or do not respond at all, in any combination of the following three ways, and for any combination of these stations. The specific actions and stations shall be selected by the operator or controller. The sending station shall: (a) terminate the link with them, using an appropriate and specific call and the TWAS terminator; or (b) direct them to remain and stay linked during the transmissions, using the CMD STAY protocol in each frame immediately before each CMD DTM word and data block sent; or (c) redirect them to do anything else that is controllable using the CMD functions described within this standard.

Each received DTM data block shall be examined using the CRC data integrity test included within the mandatory associated CMD CRC that immediately follows the DTM data block struc-

ture. If the data block passes the CRC test, the data shall be passed through to the appropriate DCE port (or normal output as directed by the operator or controller). If the data block is part of a larger message segmented before DTM transfer, it shall be recombined before output. If any DTM data blocks are received and do not pass the CRC data integrity test, any detectable but uncorrectable errors or areas likely to contain errors and should be tagged for further analysis, error control, or inspection by the operator or controller.

If ARQ is required, the received but unacceptable data block shall be temporarily stored, and a DTM ARQ NAK shall be returned to sender, who shall retransmit an exact duplicate DTM data block. Upon receipt of the duplicate, the receiving station shall again test the CRC. If the CRC is successful, the data block shall be passed through as described before, the previously unacceptable data block should be deleted, and a DTM ARQ ACK shall be returned. If the CRC fails again, both the duplicate and the previously stored data blocks shall be used to correct, as possible, errors and to create an "improved" data block. See figure A-48 for an example of data block reconstruction. The "improved" data block shall then be CRC tested. If the CRC is successful, the "improved" data block is passed through, the previously unacceptable data blocks should be deleted, and a DTM ARQ ACK shall be returned. If the CRC test fails, the "improved" data block shall be stored and a DTM ARQ NAK shall be returned. This process shall be repeated until: (a) a received duplicate, or an "improved" data block passes the CRC test (the data block is passed through, and a DTM ARQ ACK is returned); (b) the maximum number of duplicates (such as seven or more) have been sent without success (with actions by the sender as described above); or (c) the operators or controllers terminate or redirect the DTM protocol.

During reception of ALE frames and DTM data blocks, it is expected that fades, interferences, and collisions will occur. The receiving station shall have the capability to maintain synchronization with the frame and the DTM data block transmission, once initiated. It shall also have the capability to read and process any colliding and significantly stronger (that is, readable) ALE signals without confusing them with the DTM signal (basic ALE reception in parallel, and always listening). Therefore, useful information that may be derived from readable collisions of ALE signals should not be arbitrarily rejected or wasted. The DTM structures, especially the DTM EXTENDED, can tolerate weak signals, short fades, and short noise bursts. For these cases and for collisions, the DTM protocol can detect DTM words that have been damaged and "tag" them for error correction or repeats. The DTM constructions are described herein. Within the DTM data block structure, the CMD DTM word shall be placed ahead of the DTM data block itself. The DTM word shall alert the receiving station that a DTM data block is arriving, how long it is, what type of traffic it contains, what its message and block sequence is, and if ARQ is required. It shall also indicate the exact start of the data block (the end of the CMD DTM word), and shall initiate the reception, tracking, decoding, reading, and checking of the message data contained within the data block, which itself is within the DATA and REP words. The message data itself shall be either one of two types, binary bits or ASCII.

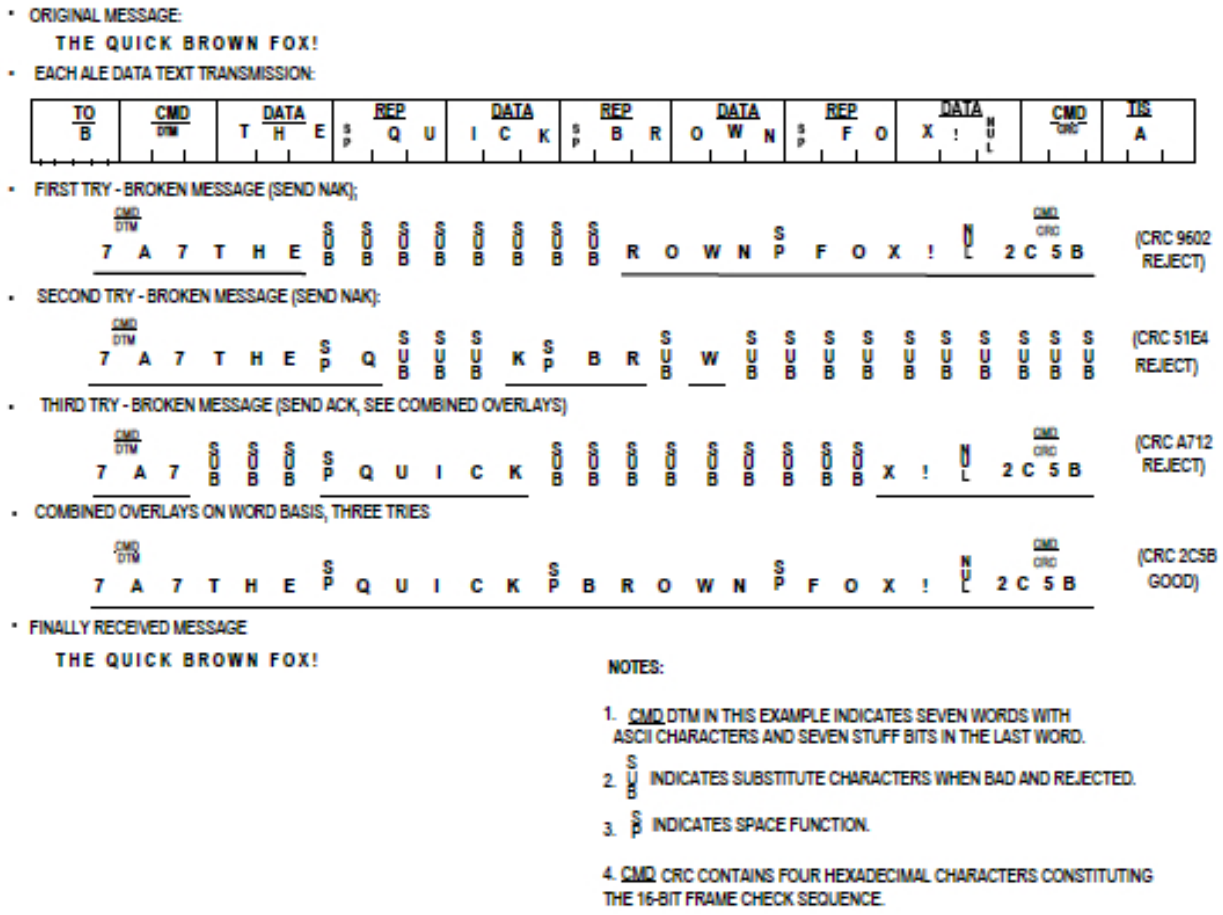


FIGURE A-48. Data text message reconstruction (overlay).

The ASCII characters (typically used for text) shall be the standard 7-bit length, and the start, stop, and parity bits shall be removed at the sending (and restored at the receiving) station. The binary bits (typically used for other character formats, computer files, and cryptographic devices) may have any (or no) pattern or format, and they shall be transferred transparently (that is, exactly as they were input to the sending station) with the same length and without modification.

The size of the DTM BASIC or EXTENDED data block shall be the smallest multiple of DATA and REP words that will accommodate the quantity of the ASCII or binary bits message data to be transferred in the DTM data block. If the message data to be transferred does not exactly fit the unencoded data field of the DTM block size selected, the available empty positions shall be "stuffed" with ASCII "DEL" (1111111) characters or all "1" bits. The combined message and "stuff" data in the uncoded DTM data field shall then be checked by the CRC for error control in the DTM protocol. The resulting 16-bit CRC word shall always be inserted into the CMD CRC word that immediately follows the DTM data block words themselves. All the bits in the data field shall then be inserted into standard DATA and REP words on a 21-bit or three-character basis and Golay FEC encoded, interleaved, and tripled for redundancy. Immediately after the CMD DTM word, the DTM DATA and REP words shall follow standard word format, and the CMD CRC shall be at the end.

The DTM BASIC data block has a relatively compact range of sizes from 0 to 31 words and shall be used to transfer any quantity of message data between zero and the maximum limits for the DTM BASIC structure, which is up to 651 bits or 93 ASCII characters. It is capable of counting the exact quantity of message data it contains, on a bit-by-bit basis. It should be used as a single DTM for any message data within this range. It shall also be used to transfer any message data in this size range that is an "overflow" from the larger size (and increments) DTM EXTENDED data blocks, which shall immediately precede the DTM BASIC in the DTM sequence of sending.

The DTM EXTENDED data blocks are also variable in size in increments of single ALE words up to 351. They should be used as a single, large DTM to maximize the advantages of DTM throughput. The size of the data block should be selected to provide the largest data field size that can be totally filled by the message data to be transferred. Any "overflow" shall be in a message data segment sent within an immediately following and appropriately sized DTM EXTENDED or BASIC data block. Under operator or controller direction, multiple DTM EXTENDED data blocks, with smaller than the maximum appropriate ID sizes, should be selected if they will optimize DTM data transfer throughput and reliability. However, these multiple data blocks will require that the message data be divided into multiple segments at the sending station, that they be sent only in the exact order of the segments in the message, and that the receiving stations recombine the segments into a complete received message. When binary bits are being transferred, the EXTENDED data field shall be filled exactly to the last bit. When ASCII characters are being transferred, there are no stuff bits as the 7-bit characters fit the ALE word 21-bit data field exactly.

If stations are exchanging DTM data blocks and DTM ARQs, they may combine both functions in the same frames, and they shall discriminate based on the direction of transmission and the sending and destination addressing. If ARQ is required in a given direction, only one DTM data block shall be allowed within any frame in that direction, and only one DTM ARQ shall be allowed in each frame in the return direction. If no ARQ is required in a given direction, multiple DTM data blocks may be included in frames in that direction, and multiple DTM ARQ's may be included in the return direction.

As always throughout the DTM protocol, any sequence of DTM data blocks to be transferred shall have the KD1 sequence control bits alternating with the preceding and following DTM data blocks (except duplicates for ARQ, which shall be exactly the same as the originally transmitted DTM data block).

Also, all multiple DTM data blocks transferring multiple segments of a larger data message shall all have their KD2 message control bits set to the same value, and opposite of the preceding and following messages. If a sequence of multiple but unrelated DTM data blocks are sent (such as several independent and short messages within several DTM BASIC data blocks), they may be sent in any sequence. However, the KD1 or KD2 sequence and message control bits shall alternate with those in the adjacent DTM data blocks.

The CMD DTM words shall be constructed as shown in table A-XXXIII. The preamble shall be CMD (110) in bits P3 through P1 (W1 through W3). The first character shall be "d" (1100100) in bits C1-7 through C1-1) (W4 through W10), which shall identify the DTM "data" function.

For DTM BASIC, EXTENDED, and NULL, when the "ARQ" control bit KD4 (W11) is set to "0," no correct data receipt acknowledgment is required; and when set to "1," it is required. For DTM ARQ, "ARQ" control bit KD4 is set to "0" to indicate acknowledgment or correct data block receipt (ACK); and when set to "1," it indicates a failure to receive the data and is therefore a request-for-repeat (NAK). For DTM ARQ responding to a DTM NULL interrogation, KD4 "0" indicates non-participation in the DTM protocol or traffic type, and KD4 "1" indicates affirmative participation in both the DTM protocol and traffic type.

For DTM BASIC, EXTENDED, and NULL, when the "data type" control bit KD3 (W12) is set to "0," the message data contained within the DTM data block shall be binary bits with no required format or pattern; and when KD3 is set to "1" the message data is 7-bit ASCII characters. For DTM ARQ, "flow" control bit KD3 is set to indicate that the DTM transfer flow should continue, or resume; and when KD3 is set to "1" it indicates that the sending station should pause (until another and identical DTM ARQ is returned, except that KD3 shall be "0").

For DTM BASIC, EXTENDED, and NULL, when the “message” control bit KD2 (W13) is set to the same value as the KD2 in any sequentially adjacent DTM data block, the message data contained within those adjacent blocks (after individual error control) shall be recombined with the message data within the present DTM data block segment-by-segment to reconstitute the original whole message, and when KD2 is set opposite to any sequentially adjacent DTM data blocks, those data blocks contain separate message data and shall not be combined. For DTM ARQ, “message” control bit KD2 shall be set to match the referenced DTM data block KD2 value to provide message confirmation.

For DTM BASIC, EXTENDED, and NULL, the “sequence” control bit KD1 (W14) shall be set opposite to the KD1 value in the sequentially adjacent DTM BASIC, EXTENDED, or NULLs to be sent (the KD1 values therefore alternate, regardless of their message dependencies). When KD1 is set to the same value as any sequentially adjacent DTM sent, it indicates that it is a duplicate (which shall be exactly the same). For DTM ARQ, “sequence” control bit KD1 shall be set to match the referenced DTM data block or NULL KD1 value to provide sequence confirmation.

When used for the DTM protocols, the ten DTM data code (DC) bits DC10 through DC1 (W15 through W24) shall indicate the DTM mode (BASIC, EXTENDED, ARQ, or NULL). They shall also indicate the size of the message data and the length of the data block. The DTM NULL DC value shall be “0” (0000000000), and it shall designate the single CMD DTM NULL word. The DTM EXTENDED DC values shall range from “1” (0000000001) to “351” (0101011111), and they designate the CMD DTM EXTENDED word and the data block multiple of DATA and REP words that define the variable data block sizes. The EXTENDED sizes shall range from 1 to 351 words, with a range of 21 to 7371 binary bits, in increments of 21; or three to 1053 ASCII characters, in increments of three. The DTM BASIC DC values shall range from “353” (0101100001) to “1023” (1111111111), and they shall designate the CMD DTM BASIC word and the exact size of the message data in compact and variable size data blocks, with up to 651 binary bits or 93 ASCII characters. The DTM ARQ DC value shall be “352” (0101100000), and it shall designate the single CMD DTM ARQ word. The DC values “384” (0110000000) and all higher multiples of “32m” (m x 100000) shall be reserved until standardized. See table A-XXXII for DC values and DTM block sizes and other characteristics.

A.5.7.4 DBM mode (optional).
The DBM ALE (orderwire) message protocol function enables ALE stations to communicate either full ASCII, or unformatted binary bit messages to and from any selected ALE station(s) for direct output to and input from associated data terminal or other DTE devices through their standard DCE ports. This DBM data transfer function is a high-speed mode (relative to DTM and AMD) with improved robustness, especially against long fades and noise bursts. When used over MF/HF by the ALE system, DBM orderwire messages may be unilateral or bilateral, and broadcast or acknowledged. As the DBM data blocks can be very large, this special orderwire message function enables exploitation of deep interleaving and FEC techniques to penetrate HF-channel long fades and large noise bursts.

The DBM data blocks shall be fully buffered at each station and should appear transparent to the using DTEs or data terminals. As a design objective and under the direction of the operator or controller, the stations should have the capability of using the DBM data traffic mode (ASCII or binary bits) to control switching of the DBM data traffic to the appropriate DCE port or associated DTE equipment, such as to printers and terminals (if ASCII mode) or computers and cryptographic devices (if binary bits mode). As an operator or controller-selected option, the received DBM message may also be presented on the operator display, similar to the method for AMD in table A.5.7.2.

There are four CMD DBM modes: BASIC, EXTENDED, NULL, and ARQ. The DBM BASIC block is a fixed size and contains a variable quantity of data, from zero to full as required, which is exactly measured to ensure integrity of the data during transfer. The DBM EXTENDED blocks are variable in size in integral multiples of the BASIC block, and are filled with integral multiples of message data. The DBM NULL and ARQ modes are used for both link management, and error and flow control. The characteristics of the CMD DBM orderwire message functions are listed in table A-XXXIV, and they are summarized below:

CMD DBM Mode	BASIC	EXTENDED	ARQ NULL
Maximum Size, Bits	588	262836	0
CRC	16 Bits	16 Bits	0
Data Capacity, ASCII	0-81	81-37377, by 84	0
Data Capacity, Bits	0-572	572-261644, by 588	0
ALE Word Redundancy	49 Fixed	49-21805, by 49	0
Data Transmission	3.136 Sec	3.136 sec - 23.26 min, by 3.136 sec increments	0

TABLE A-XXXIV. DBM characteristics.

WORD BITS W 15----------W 24 DBM CODE BITS BC 10----------BC 1		DBM CODE (DC) DECIMAL (n)	INTER-LEAVE DEPTH (ID)	BINARY BITS DATA	ASCII CHAR DATA	BLOCK TIME	TOTAL DBM (T_{rw})
DBM NULL*	0000000000	0	0	0	0	0*	1*
DBM EXTENDED (FULL)	0000000001	1	49	572	81	3.136s	9
	0000000010	2	98	1160	165	6.272s	17
	↓	n	49n	12ID-16	BITS+7	IDx64ms	8n+1
	0110111100	444	21756	261056	37293	23.21min	3553
(RESERVED)	0110111101	445	21805	261644	37377	23.26min	3561
	0110111110	446	---	---	---	---	---
	0110111111	447	---	---	---	---	---
DBM BASIC (EXACT)	0111000000	448	49	0	0	3.136s	9
	0111000001	449	↓	1	0	↓	↓
	0111000011	450		2	0		
	↓	↓		n-448	BITS+7		
	1111111011	1019		571	81		
	1111111100	1020	49	572	81	3.136s	9
DBM ARQ*	1111111101	1021	0	0	0	0*	1*
(RESERVED)*	1111111110	1022	---	---	---	---	---
(RESERVED)*	1111111111	1023	---	---	---	---	---

NOTE:
*NO INTERNAL CRC USED.

When an ASCII, or binary bit, digital data message function is required, the following CMD DBM orderwire structures and protocols shall be used as specified herein, unless another standardized protocol is substituted. The DBM structure shall be inserted within the message section of the standard frame. A CMD DBM word shall be constructed in the standard format. The data to be transferred shall be Golay FEC encoded, interleaved (for error spreading during decoding), and transmitted immediately following the CMD DBM word.

When the DBM structure transmission time exceeds the maximum for the message section ($T_{m\ max}$), the DBM protocol shall take precedence and shall extend the T_m limit to accommodate the DBM. The DBM mode preserves the required consistency of redundant word phase during the transmission. The message expansion due to the DBM is always a multiple of 8 T_{rw}, as the interleaver depth is always a multiple of 49. The transmission time of the DBM data block (T_{dbm}) itself is equal to (interleaver depth x 64ms), not including the T_{rw} for the preceding CMD DBM word. Figure A-49 shows an example of an exchange using the DBM orderwire to transfer and acknowledge messages. Figure A-50 shows an example of a DBM data interleaver, and figure A-51 shows the transmitted DBM bit-stream sequence.

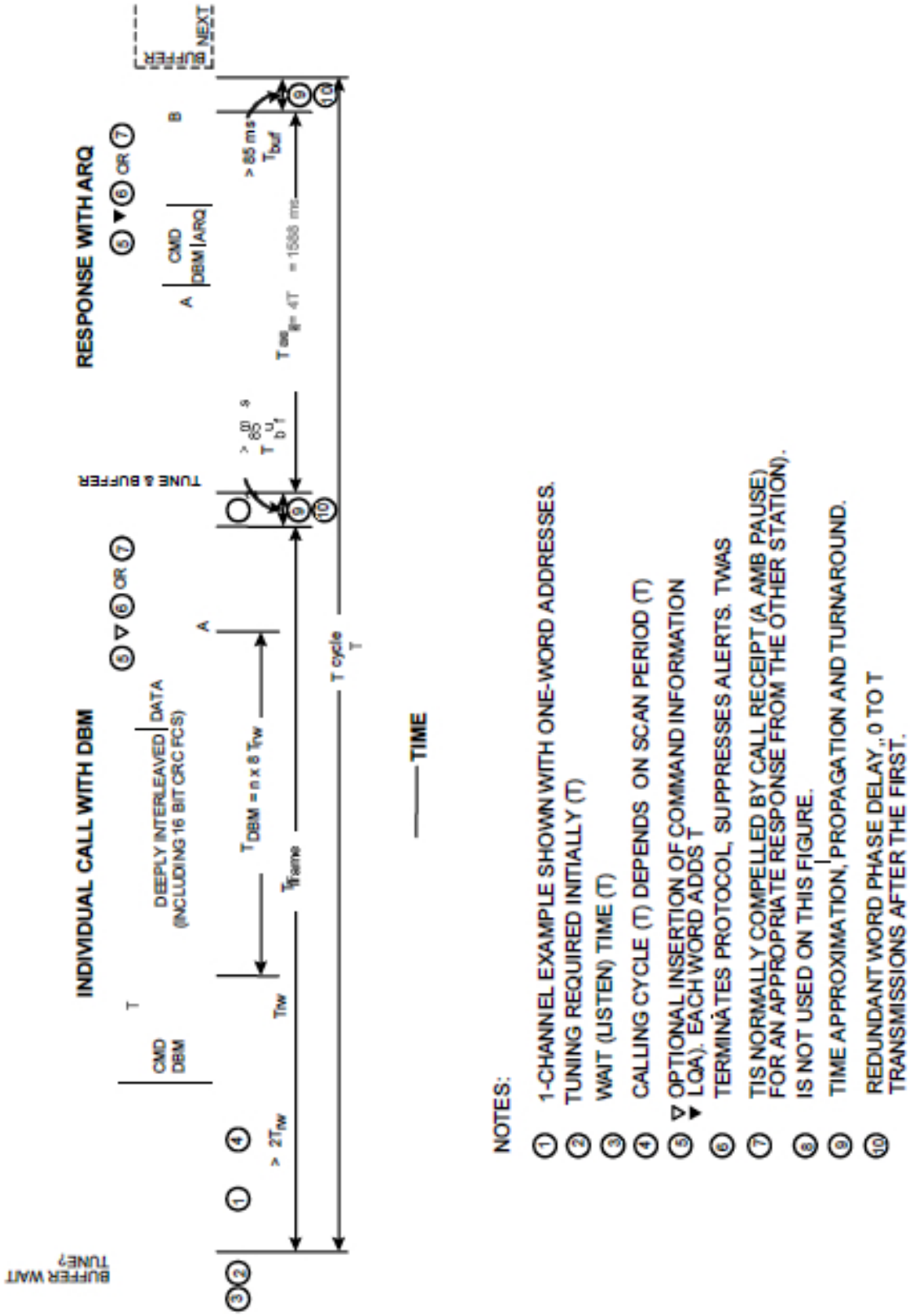
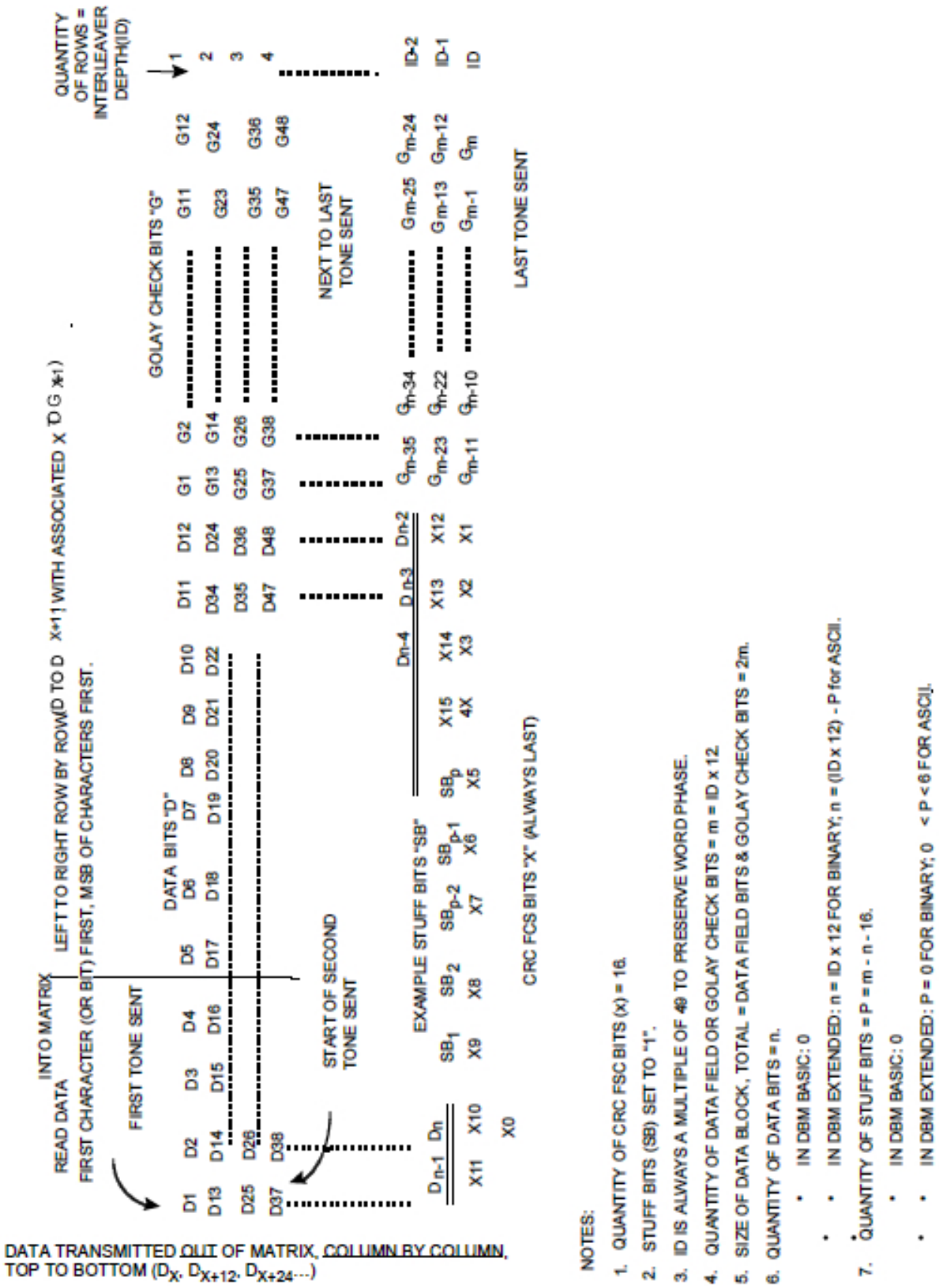


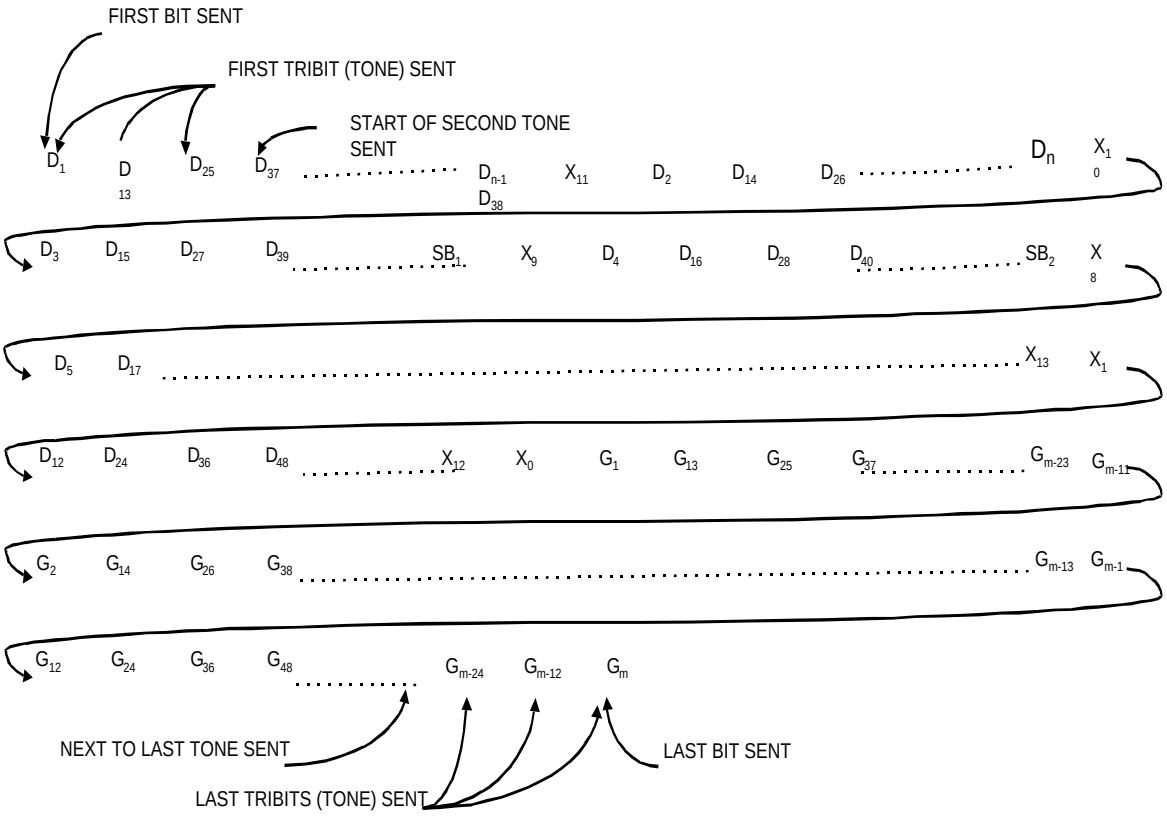
FIGURE A-49. Data block message structure and ARQ example.



NOTES:

1. QUANTITY OF CRC FSC BITS (x) = 16.
2. STUFF BITS (SB) SET TO "1".
3. ID IS ALWAYS A MULTIPLE OF 48 TO PRESERVE WORD PHASE.
4. QUANTITY OF DATA FIELD OR GOLAY CHECK BITS = m = ID x 12.
5. SIZE OF DATA BLOCK, TOTAL = DATA FIELD BITS & GOLAY CHECK BITS = 2m.
6. QUANTITY OF DATA BITS = n.
   - IN DBM BASIC: 0
   - IN DBM EXTENDED: n = ID x 12 FOR BINARY; n = (ID x 12) - P for ASCII.
7. QUANTITY OF STUFF BITS = P = m - n - 16.
   - IN DBM BASIC: 0
   - IN DBM EXTENDED: P = 0 FOR BINARY; 0 < P < 6 FOR ASCII.

FIGURE A-50. DBM interleaver and deinterleaver.



Notes:
1. Quantity of tones sent = 2M/3 = (2 X 12 X ID)/3 = ID X 8.
2. Time of block sent = ID x 8 x 8 ms = ID x 64 ms.

FIGURE A-51. DBM example.

The DBM protocol shall be as described herein. The CMD DBM BASIC and EXTENDED formats (herein referred to as DBM data blocks) shall be used to transfer messages in information among ALE stations. The CMD DBM ARQ format shall be used to acknowledge other CMD DBM formats and for error and flow control, except for non-ARQ and one-way broadcasts. The CMD DBM NULL format shall be used to: (a) interrupt ("break") the DBM and message flow; (b) to interrogate stations to confirm DBM capability before initiation of the DBM message transfer protocols; and (c) to terminate the DBM protocols while remaining linked. When used in handshakes and subsequent exchanges, the protocol frame terminations for all involved stations shall be TIS until all the DBM messages are successfully transferred, and all are acknowledged if ARQ error control is required. The only exceptions shall be when the protocol is a one-way broadcast or the station is forced to abandon the exchange by the operator or controller, in which cases the termination should be TWAS.

Once a CMD DBM word of any type has been received by a called (addressed) or linked station, the station shall remain on channel for the entire specified DBM data block time (if any), unless

forced to abandon the protocol by the operator or controller. The start of the DBM data block itself shall be exactly indicated by the end of the CMD DBM BASIC or EXTENDED word itself. The station shall attempt to read the entire DBM data block information, plus the expected frame continuation, which shall contain a conclusion (possibly preceded by additional functions in the message section, as indicated by additional CMD words).

With or without ARQ, identification of each DBM data block and its associated orderwire message (if segmented into sequential DBM data blocks) shall be achieved by use of the sequence and message control bits, KB1 and KB2, (see table A-XXXV) which shall alternate with each DBM transmission and message, respectively. The type of data contained within the data block (ASCII or binary bits) shall be indicated by KB3 as a data identification bit. Activation of the ARQ error-control protocol shall use the ARQ control bit KB4. If no ARQ is required, such as in one-way broadcasts, multiple DBM data blocks may be sent in the same frame, but they shall be in proper sequence if they are transferring a segmented message.

TABLE A-XXXV. DBM structures.

	DBM Bits		Word Bits	
CMD preamble	MSB	P3 = 1	MSB	W3
		P2 = 1		W1
	LSB	P1 = 0		W2
First character "b"	MSB	C1 (bit-7) = 1		W4
		C1 (bit-6) = 1		W5
		C1 (bit-5) = 0		W6
		C1 (bit-4) = 0		W7
		C1 (bit-3) = 0		W8
		C1 (bit-2) = 1		W9
	LSB	C1 (bit-1) = 0		W10
Control bits	MSB	KB4		W11
		KB3		W12
		KB2		W13
	LSB	KB1		W14
DTM data code bits	MSB	BC10		W15
		BC9		W16
		BC8		W17
		BC7		W18
		BC6		W19
		BC5		W20
		BC4		W21
		BC3		W22
		BC2		W23
	LSB	BC1	LSB	W24

NOTES:

1. CMD DBM and DBM ARQ first character is "b" for "block."
2. With DBM transmission, control bit KB4 (W11) is set to "0" for no ACK request, and "1" for ACK request.
3. If a DBM ARQ transmission, control bit KB4 (W11) is set to "0" for ACK, and "1" for NAK.
4. With DBM transmissions, control bit KB3 (W12) is set to "0" for binary bits and "1" for 7-bit ASCII characters.
5. If a DBM ARQ transmission, control bit KB3 (W12) is set to "0" for flow continue, and "1" for flow pause.
6. With DBM transmissions, control bit KB2 (W13) is set: (a) the same ("0" or "1") as the sequentially adjacent DBM(s) if the transmitted data field is to be reintegrated as part of a larger DBM, and (b) alternately different if independent from the prior adjacent DBM data field(s).
7. If a DBM ARQ transmission, control bit KB2 (W13) is set the same as the referenced DBM transmission.
8. With DBM transmissions, control bit KB1 (W14) is set alternately to "0" and "1" in any sequence of DBMs as a sequence control.
9. If a DBM ARQ transmission, control bit KB1 (W14) is set the same as the referenced DBM transmission.
10. Block code (BC) bits are from table A-XXXIV.

When ARQ error or flow control is required, the CMD DBM ARQ shall identify the acknowledged DBM data block by the use of the sequence and message control bits KB1 and KB2, which shall be set to the same values as the immediately preceding and referenced DBM data block transmission. Control bit KB3 shall be used as the DBM flow control to pause or continue (or resume) the flow of the DBM data blocks. The ACK and NAK functions shall use the ARQ control bit KB4. If no ARQ has been required by the sending station, but the receiving station needs to control the flow of the DBM data blocks, it shall use the DBM ARQ to request a pause in, and resumption of, the flow.

When data transfer ARQ error and flow control is required, the DBM data blocks shall be sent individually and in sequence. Each DBM data block shall be individually acknowledged before the next DBM data block is sent. Therefore, with ARQ there shall be only one DBM data block transmission in each frame. If the transmitted DBM data block causes a NAK in the returned DBM ARQ, as described below, or if no ACK or DBM ARQ is detected in the returned frame, or if no frame is detected at all, the sending station shall resend an exact duplicate of the unacknowledged DBM data block. It shall continue to resend duplicates (which should be at least seven), one at a time and with appropriate pauses for responses, until the involved DBM data block is specifically acknowledged by a correct DBM ARQ. Only then shall the next DBM data block in the sequence be sent. If the sending station is frequently or totally unable to detect frame or DBM ARQ responses, it should abort the DBM transfer protocol, terminate the link and relink and reinitiate the DBM protocol on a better channel (under operator or controller direction).

Before initiation of the DBM data transfer protocols, the sending stations should confirm the existence of the DBM capability in the intended receiving stations, if not already known. When a DBM interrogation function is required, the following protocol shall be used. Within any standard protocol frame (using TIS), the sending station shall transmit a CMD DBM NULL, with ARQ required, to the intended station(s). These receiving stations shall respond with the appropriate standard frame and protocol, with the following variations. They shall include a CMD DBM ARQ if they are DBM capable, and they shall omit it if they are not DBM capable. The sending station shall examine the ALE and DBM ARQ responses for existence, correctness, and the status of the DBM KB control bits, as described herein. The transmitted CMD DBM NULL shall have its control bits set as follows: KB1 and KB2 set opposite of any subsequent and sequential CMD DBM BASIC or EXTENDED data blocks which will be transmitted next; KB3 set to indicate the intended type of traffic; and KB4 set to require ARQ. The returned CMD DBM ARQ shall have its control bits set as follows: KB1 and KB2 set to match the interrogating DBM NULL; KB3 set to indicate if the station is ready for DBM data exchanges, or if a pause is requested; and KB4 set to ACK if the station is ready to accept DBM data transmissions with the specified traffic type, and NAK if it cannot or will not participate, or if it failed to read the DBM NULL.

The sending (interrogating) station shall handle any stations which return a NAK, or do not return a DBM ARQ, or do not respond, in any combination of the following, and for any combination of these stations. The specific actions and stations shall be selected by the operator or controller. The sending station shall: (a) terminate the link with these stations, using an appropriate and specific call and the TWAS terminator; (b) direct the stations to remain and stay linked during the transmissions, using the CMD STAY protocol in each frame immediately before each CMD DBM word and data block sent; or (c) redirect them to do anything else which is controllable using the CMD functions described within this standard.

Each received DBM data block shall be examined using the CRC data integrity test which is embedded within the DBM structure and protocol. If the data block passes the CRC test, the data shall be passed through to the appropriate DCE port (or normal output as directed by the operator or controller). If the data block is part of a larger message which was segmented before DBM transfer, it shall be recombined before output. If any DBM data blocks are received and do not pass the CRC data integrity test, any detectable but uncorrectable errors; or areas likely to contain errors, should be tagged for further analysis, error control, or inspection by the operator or controller.

If ARQ is required, the received but unacceptable data block shall be temporarily stored, and a DBM ARQ NAK shall be returned to the sender, who shall retransmit an exact duplicate DBM data block. Upon receipt of the duplicate, the receiving station shall again test the CRC. If the CRC is successful, the data block shall be passed through as described before, the previously unacceptable data block should be deleted, and a DBM ARQ ACK shall be returned. If the CRC fails again, both the duplicate and the previously stored data blocks shall be used to correct, as possible, errors and to create an “improved” data block. See figure A-48 for an example of data block reconstruction. The “improved” data block shall then be CRC tested. If the CRC is successful, the “improved” data block is passed through, the previously unacceptable data blocks should be deleted, and a DBM ARQ ACK shall be returned. If the CRC test fails, the “improved” data block shall also be stored and a DBM ARQ NAK shall be returned. This process shall be repeated until: (a) a received duplicate, or an “improved” data block passes the CRC test (and the data block is passed through, and a DBM ARQ ACK is returned); (b) the maximum number of duplicates (such as seven or more) have been sent without success (with actions by the sender as described above); or (c) the operators or controllers terminate or redirect the DBM protocol.

During reception of frames and DBM data blocks, it is expected that fades, interferences, and collisions will occur. The receiving station shall have the capability to maintain synchronization with the frame and the DBM data block transmission, once initiated. It shall also have the capability to read and process any colliding and significantly stronger (that is, readable) ALE signals without confusing them with the DBM signal (basic ALE reception in parallel, and always listening). The DBM structures, especially the DBM EXTENDED, can tolerate significant fades, noise bursts, and collisions. Therefore, useful information which may be derived from readable collisions of ALE signals should not be arbitrarily rejected or wasted.

The DBM constructions shall be as described herein. Within the DBM data block structure, a CMD DBM word shall be placed ahead of the encoded and interleaved data block itself. The DBM word shall alert the receiving station that a DBM data block is arriving, how long it is, what type of traffic it contains, what its interleaver depth is, what its message and block sequence is, and if ARQ is required. It shall also indicate the exact start of the data block itself (the end of the CMD DBM word itself) and shall initiate the reception, tracking, deinterleaving, decoding, and checking of the data contained within the block. The message data itself shall be either one of two types, binary bits or ASCII. The ASCII characters (typically used for text) shall be the standard 7-bit length, and the start, stop, and parity bits shall be removed at the sending (and restored at the receiving) station. The binary bits (typically used for other character formats, computer files, and cryptographic devices) may have any (or no) pattern or format, and they shall be transferred transparently, that is, exactly as they were input to the sending station, with the same length and without modification. The value of the interleaver depth shall be the smallest (multiple of 49) which will accommodate the quantity of ASCII or binary bits message data to be transferred in the DBM data block. If the message data to be transferred does not exactly fit the uncoded data field of the DBM block size selected (except for the last 16 bits, which are reserved for the CRC), the available empty positions shall be “stuffed” with ASCII “DEL” characters or all “1” bits. The combined message and “stuff” data in the uncoded DBM data field shall then be checked by the CRC for error control in the DBM protocol. The resulting 16-bit CRC word shall always occupy the last 16 bits in the data field. All the bits in the field shall then be Golay FEC encoded, on a 12-bit basis, to produce rows of 24-bit code words, arranged from top to bottom in the interleaver matrix (or equivalent), as shown in figure A-50. The bits in the matrix are then read out by columns (of length equal to the interleaver depth) for transmission. Immediately after the CMD DBM word, the encoded and interleaved data blocks bits shall follow in bit format, three bits per symbol (tone).

The DBM BASIC data block has a fixed size (interleaver depth 49) and shall be used to transfer any quantity of message data between zero and the maximum limits for the DBM BASIC structure, which is up to 572 bits or 81 ASCII characters. It is capable of counting the exact quantity of message data which it contains, on a bit-by-bit basis. It should be used as a single DBM for any message data within this range. It shall also be used to transfer any message data in this size range which is an “overflow” from the larger size (and increments) DBM EXTENDED data blocks (which shall immediately precede the DBM BASIC in the DBM sequence of sending).

The DBM EXTENDED data blocks are variable in size, in increments of 49 times the interleaver depth. They should be used as a single, large DBM to maximize the advantages of DBM deep interleaving, FEC techniques, and higher speed (than DTM or AMD) transfer of data. The interleaver depth of the EXTENDED data block should be selected to provide the largest data field size which can be totally filled by the message data to be transferred. Any “overflow” shall be in a message data segment sent within an immediately following DBM EXTENDED or BASIC data block. Under operator or controller direction, multiple DBM EXTENDED data blocks, with smaller than the maximum appropriate interleaver depth sizes, should be selected if they will optimize DBM data transfer throughput and reliability. However, these multiple data blocks will

require that the message data be divided into multiple segments at the sending station and sent only in the exact order of the segments in the message. The receiving stations must recombine the segments into a complete received message. When binary bits are being transferred, the EXTENDED data field shall be filled exactly to the last bit. When ASCII characters are being transferred, the EXTENDED data field may have 0 to 6 “stuff” bits inserted. Individual ASCII characters shall not be split between DBM data blocks and the receiving station shall read the decoded data field on a 7-bit basis, and it shall discard any remaining “stuff” bits (modulo-7 remainder).

If stations are exchanging DBM data blocks and DBM ARQs, they may combine both functions in the same frames. They shall discriminate based on the direction of transmission and the sending and destination addressing. If ARQ is required in a given direction, only one DBM data block shall be allowed within any frame in that direction, and only one DBM ARQ shall be allowed in each frame in the return direction. If no ARQ is required in a given direction, multiple DBM data blocks may be included in frames in that direction, and multiple DBM ARQs may be included in the return direction.

As always throughout the DBM protocol, any sequence of DBM data blocks to be transferred shall have their KB1 sequence control bits alternating with the preceding and following DBM data blocks (except duplicates for ARQ, which shall be exactly the same as their originally transmitted DBM data block). Also, all multiple DBM data blocks transferring multiple segments of a large data message shall all have their KB2 message control bits set to the same value, and opposite of the preceding and following messages. If a sequence of multiple but unrelated DBM data blocks are sent (such as several independent and short messages within several DBM BASIC data blocks), they may be sent in any sequence. However, when sent, the associated KB1 and KB2 sequence and message control bits shall alternate with those in the adjacent DBM data blocks.

The CMD DBM words shall be constructed as shown in table A-XXXV. The preamble shall be CMD (110) in bits P3 through P1 (W1 through W3). The first character shall be “b” (1100010) in bits C1-7 through C1-1 (W4 through W10), which shall identify the DBM “block” function.

For DBM BASIC, EXTENDED, and NULL, when the ARQ control bit KB4 (W11) is set to “0,” no correct data receipt acknowledgment is required; and when set to “1,” it is required. For DBM ARQ, ARQ control bit KB4 is set to “0” to indicate acknowledgment or correct data block receipt (ACK); and when set to “1,” it indicates a failure to receive the data and is therefore a request-for-repeat (NAK). For DBM ARQ responding to a DBM NULL interrogation, KB4 “0” indicates non-participation in the DBM protocol or traffic type, and KB4 “1” indicates affirmative participation in both the DBM protocol and traffic type.

For DBM BASIC, EXTENDED, and NULL, when the data type control bit KB3 (W12) is set to “0,” the message data contained within the DBM data block shall be binary bits with no required

format or pattern; and when KB3 is set to “1” the message data is 7-bit ASCII characters. For DBM ARQ, flow control bit KB3 is set to “0” to indicate that the DBM transfer flow should continue or resume; and when KB3 is set to “1” it indicates that the sending station should pause (until another and identical DBM ARQ is returned, except that KB3 shall be “0”).

For DBM BASIC, EXTENDED, and NULL, when the “message” control bit KB2 (W13) is set to the same value as the KB2 in any sequentially adjacent DBM data block, the message data contained within those adjacent blocks (after individual error control) shall be recombined with the message data within the present DBM data block to reconstitute (segment-by-segment) the original whole message; and when KB2 is set opposite to any sequentially adjacent DBM data blocks, those data blocks contain separate message data and shall not be combined. For DBM ARQ, “message” control bit KB2 shall be set to match the referenced DBM data block KB2 value to provide message confirmation.

For DBM BASIC, EXTENDED, and NULL, the sequence control bit KB1 (W14) shall be set opposite to the KB1 value in the sequentially adjacent DBM BASIC, EXTENDED, or NULLs be sent (the KB1 values therefore alternate, regardless of their message dependencies). When KB1 is set the same as any sequentially adjacent DBM sent, it indicates a duplicate. For DBM ARQ, sequence control bit KB1 shall be set to match the referenced DBM data block or NULL KB1 value to provide sequence confirmation.

When used for the DBM protocols, the ten DBM data code (BC) bits BC10 through BC1 (W15 through W24) shall indicate the DBM mode (BASIC, EXTENDED, ARQ, or NULL). They shall also indicate the size of the message data and the length of the data block. The DBM NULL BC value shall be “0” (0000000000), and it shall designate the single CMD DBM NULL word. The DBM EXTENDED BC values shall range from “1” (0000000001) to “445” (0110111101), and they shall designate the CMD DBM EXTENDED word and the data block multiple (of 49 INTERLEAVER DEPTH) which defines the variable data block sizes, in increments of 588 binary bits or 84 ASCII characters. The DBM BASIC BC values shall range from “448” (0111000000) to “1020” (1111111100), and they shall designate the CMD DBM BASIC word and the exact size of the message data in a fixed size (INTERLEAVER DEPTH = 49) data block, with up to 572 binary bits or 81 ASCII characters. The DBM ARQ BC value shall be “1021” (1111111101), and it shall designate the single CMD DBM ARQ word.

NOTES:
1. The values “446” (0110111110) and “447” (0110111111) are reserved.
2. The values “1022” (1111111110) and “1023” (1111111111) are reserved until standardized (see table A-XXXIV).

A.5.8 AQC (optional) .
AQC-ALE is designed to use shorter linking transmissions than those of baseline second generation ALE (2G ALE) described previously in this appendix. AQC-ALE uses an extended version of the 2G ALE signaling structure to assure backward compatibility to already fielded radios. Special features of AQC-ALE include the following:

- The signaling structure separates the call attempt from the inlink-state transactions. This allows radios that are scanning to detect and exit a channel that is carrying traffic that is of no interest.
- The address format is a fixed form to allow end of address detection without requiring the last word wait timeout.
- Control features distinguish call setup channels from traffic carrying channels.
- Local Noise Reports are inherent in the sound and call setup frames to minimize the need to sound as frequently.
- Resources that are needed during the linked state can be identified and bid for during the link setup. This provides a mechanism to bid for needed resources during linking.

A.5.8.1 Signaling structure .
The AQC-ALE signaling structure is identical to that described previously in this appendix, except as provided below and in the remaining subsections of this section:

- The AQC-ALE word is encoded differently (see A.5.8.1.1).

A.5.8.1.1 AQC-ALE word structure.
The AQC-ALE word shall consist of a three-bit preamble, an address differentiation flag, a 16-bit packed address field, and a 4-bit Data Exchange field. These fields shall be formatted and used as described in the following paragraphs. Every AQC-ALE word shall have the form shown in figure A-52, AQC-ALE Word. The data values associated with a particular AQC-ALE word are defined by the context of the frame transmission (see A.5.8.2).

A.5.8.1.1.1 Packed address.
AQC-ALE packs the 21 bits representing three address characters in the 38-character ASCII subset into 16 bits. This is performed by assigning an ordinal value between 0 and 39 to each member of the 38-character subset. Base 40 arithmetic is used to pack the mapped data into a 16-bit number. The ASCII characters used for addressing shall be mapped to the values defined in table A-XXXVI, Address Character Ordinal Values, with character 1's value multiplied by 1600, Character 2’s value multiplied by 40, and Character 3’s value multiplied by 1. The sum of the three values shall be used as the 16-bit packed address (see example below).

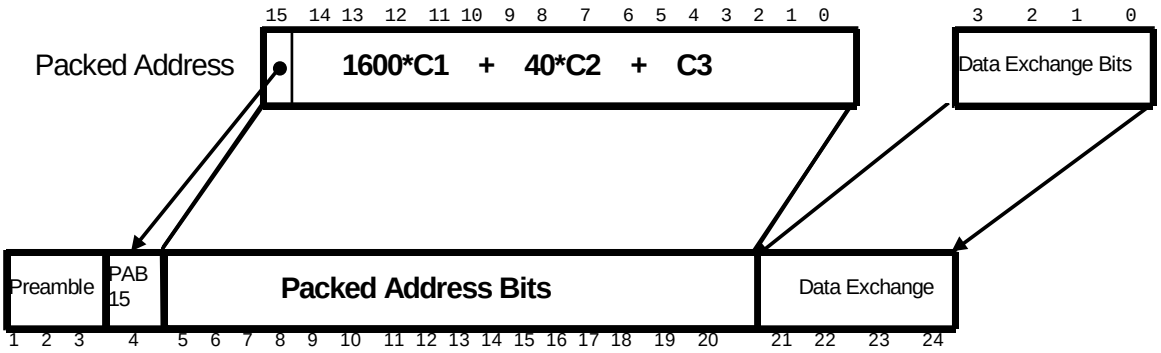


FIGURE A-52. AQC-ALE data exchange word.

TABLE A-XXXVI. AQC address character ordinal value.

Character	Value
*	0
0 to 9	1 to 10
?	11
@	12
A to Z	13 to 38
_ (Underscore)	39

Note: The "*" and "_" characters are not part of the standard ALE ASCII-38 character set. These characters shall not be used in station addresses in any network that is required to interoperate with stations that support only baseline 2G ALE.

Example:

Using table A-XXXVI, the address 'ABC' would be computed as:

(Value('A') * 1600) + (Value('B')* 40) + Value('C')
which is
(13 * 1600) + (14 * 40) + 15 = 21,375

The smallest valued legal address is "000" for a packed value of ➔ 1,641
A legal address such as "ABC" would have a packed value of ➔ 21,375
The largest valued legal address is "ZZZ" for a packed value of ➔ 62,358

A.5.8.1.1.2 Address differentiation flag.
Bit 4 of the AQC-ALE word shall be a copy of the most significant bit of the 16-bit packed address. This combination results in no legal address in AQC-ALE being legal in baseline 2G ALE and vice versa. The packed address shall occupy the next 16 bits of the 21-bit data portion of the address.

A.5.8.1.2 Preambles .
The preambles shall be as shown in table A-XXXVII AQC-ALE word types (and preambles)

TABLE A-XXXVII. AQC-ALE word types (and preambles).

Word Type	Code Bits	Functions	Significance
INLINK	001	direct routing	Transaction for linked members
TO	010	--	See table A-VIII
CMD	110	--	See table A-VIII
PART2	100	direct routing	indicates this is the second part of the full AQC-ALE address
TIS	101	--	See table A-VIII
TWAS	011	--	See table A-VIII
DATA	000	extension of information	Used only in message section to extend information being sent
REP	111	duplication and extension of information	Used only in message section to extend information being sent

A.5.8.1.2.1 TO.
This preamble shall have a binary value of 010 and is functionally identical to the TO preamble in A.5.2.3.2.1. The AQC-ALE TO preamble shall represent the first of two words identifying the address of the station or net.

A.5.8.1.2.2 THIS IS (TIS).
This preamble shall have a binary value of 101. The preamble is functionally identical to the TIS preamble in A.5.2.3.2.2. The AQC-ALE TIS preamble identifies the AQC-ALE word as containing the first three characters of the of the calling or sounding station address.

A.5.8.1.2.3 THIS WAS (TWAS).
This preamble shall have a binary value of 011. This preamble is functionally identical to the TWAS preamble in A.5.2.3.2.3. The AQC-ALE TWAS preamble identifies the AQC-ALE word as containing the first three characters of the of the calling or sounding station address.

A.5.8.1.2.4 PART2.
This preamble shall have a binary value of 100. This preamble is shared with the baseline 2G ALE preamble of FROM. This preamble identifies the second set of three characters in an AQC-ALE address. This preamble shall be used for the second word of every AQC-ALE packed address transmission.

A.5.8.1.2.5 INLINK.
This preamble shall have a binary value of 001. This preamble is shared with the baseline 2G ALE preamble of THRU. This preamble shall be used by AQC-ALE whenever a transmission to stations already in an established link is required. This preamble identifies the AQC-ALE word as containing the first three characters of the transmitting station address. This preamble may also be used in the acknowledgement frame of a three-way handshake as described in A.5.8.2.3.

A.5.8.1.2.6 COMMAND.
No Change to A.5.2.3.3.1

A.5.8.1.2.7 DATA.
See A.5-2.3.4.1. In the AQC-ALE word, this preamble never applies to a station address.

A.5.8.1.2.8 REPEAT.
See A.5-2.3.4.2. In the AQC-ALE word, this preamble never applies to a station address.

A.5.8.1.3 AQC-ALE address characteristics .

A.5.8.1.3.1 Address size.
Addresses shall be from 1 to 6 characters.

A.5.8.1.3.2 Address character set.
The address character set shall be the same ASCII-38 character set as for baseline 2G ALE.

A.5.8.1.3.3 Support of ISDN (option) (NT).
To support an ISDN address requirement, the station shall be capable of mapping any 15 character address to and from a 6 character address for displaying or calling. This optional mapping shall be available for at least one Self Address and all programmed Other Addresses in the radio.

A.5.8.1.3.4 Over-the-air address format.
A two AQC-ALE word sequence shall be broadcast for any AQC-ALE address. The “@” shall be used as the stuff character to complete an address that contains fewer than six characters. The sequence shall be an AQC-ALE word with the preamble TO, TIS, TWAS, or INLINK for the first three characters of the address followed by an AQC-ALE word with the preamble PART2 for the last three address characters.

A.5.8.1.4 Address formats by call type.

A.5.8.1.4.1 Unit addresses.
A unit or other address shall be from one to six characters.

A.5.8.1.4.2 StarNet addresses.
A StarNet address shall be from one to six characters.

A.5.8.1.4.3 Group addresses.
This feature is not applicable to AQC-ALE.

A.5.8.1.4.4 AllCall address.
AQC-ALE AllCall address shall be six characters. The second three characters of the AllCall address shall be the same as the first three characters. Thus, a global AllCall sequence would look like:

TO-**@?@**|PART2-**@?@**.

A.5.8.1.4.5 AnyCall address.
AQC-ALE AnyCall address shall be six characters. The second three characters of the AnyCall address shall be the same as the first three characters. Thus, a global AnyCall sequence would look like:

TO-**@@?**|PART2-**@@?**.

A.5.8.1.5 Data exchange field.
The 4-bit data exchange field shall be encoded as described in Table A-XXXVIII and the following paragraphs. The use of the various encodings DE(1) through (9) shall be as shown in the figures for the Sound, Unit call, Starnet call, All call, and Any call in the respective subsections of A.5.8.2.

NOTE: A station may use the contents of the data exchange field to further validate the correctness of a given frame.

TABLE A-XXXVIII. Data exchange definitions.

	Bit 3	Bit 2	Bit 1	Bit 0	Description
DE(1)	1	1	1	1	No Data Available
DE(2)	x	x	x	x	Number of TOs Left in Calling Cycle Section
DE(3)	x	x	x	x	Inlink Resource List Expected
DE(4)	x	x	x	x	Local Noise Index
DE(5)	0	< BER Range>			BER estimate
DE(6)	x	x	x	x	LQA Measurement Index
DE(7)	x	x	x	x	Number of Tis/Twas left in Sound
DE(8)	Ack This	<# of Command Preambles>			Most Significant Bits of the Inlink Transaction Code
DE(9)	I'm Inlink	< Transaction Code >			Least significant 4 bits of Inlink

A.5.8.1.5.1 DE(1) no data available.
DE(1) shall be sent in the TIS word in the conclusion of a Call frame. All data bits shall be set to 1s.

A.5.8.1.5.2 DE(2) number of TO words left in calling cycle.
DE(2) shall be sent in every AQC-ALE word that contains a TO preamble. In a Call frame, the DE(2) field shall indicate the remaining number of TO preambles that remain in the frame. This is an inclusive number and when set to a value of 1 the next address shall be the caller's address using a TIS or TWAS preamble. When the remaining call duration would require a count greater than 15, a count of 15 shall be used.

A value of 0 shall be used in in the Response frame and Acknowledgement frame when a single address in required. DE(2) shall count down to 1 whenever multiple addresses are transmitted in an address section.

A.5.8.1.5.3 DE(3) Inlink resource list.
DE(3) shall be sent in the PART 2 word that follows each TO word. The DE(3) field shall indicate the type of traffic to be conveyed during the Inlink state, using the encodings in table AXXXIX. Values not specified in the table are reserved, and shall not be used until standardized.

Upon receipt of the INLINK Resource List in the Call, the called station shall determine whether the station can operate with the desired resource. When responding to the call, the called station shall honor the requested resource whenever possible. If the resource requested is unavailable, the called unit shall respond with an alternate resource that is the best possible alternative resource available to the receiver. This information is provided in the Response frame of a handshake.

By definition, when the calling station enters an Inlink state with the called station, the calling station accepted the Inlink resource that the called station can provide.

TABLE A-XXXIX. Inlink resource list.

Value	Meaning	Alternate Resource
0	Clear Voice	15
1	Digital Voice	0
2	High Fidelity Digital (HFD) Voice	1 or 0
3	Reserved	NA
4	Secure Digital Voice	2, 1, 0
5	Secure HFD Voice	4, 2, 1, 0
6	Reserved	NA
7	Reserved	NA
8	ALE Messaging	15
9	PSK Messaging	0 or 15
10	39 Tone Messaging	0 or 15
11	HF Email	9, 8, 0
12	KY-100 Data Security Active	9
13	Reserved	NA
14	Reserved	NA
15	Undeclared Traffic. Usually a mixture.	Always Acceptable

A.5.8.1.5.4 DE(4) local noise report.
DE(4) shall be sent in the PART 2 word that concludes a Call frame and in every PART 2 word in a Sounding frame. The Local Noise Report contains information which describes the type of local noise at the sender's location. The Local Noise Report provides a broadcast alternative to sounding that permits receiving stations to approximately predict the bilateral link quality for the channel carrying the report. An example application of this technique is networks in which most stations are silent but which need to have a high probability of linking on the first attempt with a base station. A station receiving a Local Noise Report can compare the noise level at the transmitter to its own local noise level, and thereby estimate the bilateral link quality from its own LQA measurement of the received noise report transmission. The report includes a mean and maximum noise power measured on the channel in the past 60 minutes with measurement intervals at least once per minute.

The Local Noise Report shall be formatted as shown in figure A.5.8-5. Units for the Max and Mean fields are dB relative to 0.1 µV 3 kHz noise. The Max noise level shall be the amount of distance from the Mean that the local noise was measured against. When averaging is used, standard rounding rules to the integer shall apply. 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 that destination. For a more detailed local noise report, a station may broadcast the ALE Local Noise Report command in the message section. When deriving the average noise floor, signals which can be recognized shall be excluded from the power measurement.

TABLE A-XL. Local noise report.

Value	Delta Max Noise from Mean	Mean Noise Level
0	0 <= Noise < 6 dB	Mean <= 6 dB
1	6 <= Noise < 12 dB	Mean <= 6 dB
2	Noise >= 12 dB	Mean <= 6 dB
3	0 <= Noise < 6 dB	6 < Mean <= 15 dB
4	6 <= Noise < 12 dB	6 < Mean <= 15 dB
5	Noise >= 6 dB	6 < Mean <= 15 dB
6	0 <= Noise < 6 dB	15< Mean <= 40 dB
7	6 <= Noise < 12 dB	15< Mean <= 40 dB
8	Noise >= 12 dB	15< Mean <= 40 dB
9	0 <= Noise < 6 dB	40 < Mean <= 60 dB
10	6 <= Noise < 12 dB	40 < Mean <= 60 dB
11	Noise >= 12db	40 < Mean <= 60 dB
12	No Definition	60 < Mean <= 80 dB
13	No Definition	80 < Mean <= 100 dB
14	No Definition	Mean > 100 dB
15	No Data	No Data

A.5.8.1.5.5 DE(5) LQA variation.
DE(5) shall be sent in the TIS or TWAS word in the conclusion of AQC-ALE Response and Acknowledgement frames. It shall report the signal quality variation measured on the immediately preceding transmission of the handshake.

Whenever an AQC-ALE or ALE word is received, a bit error ratio (BER) estimate shall be computed by counting non-unanimous votes in accordance with paragraph A.5.4.1.1. This measurement can be used to determine the capacity of the channel to handle traffic. The DE(5) LQA Data Exchange word shall report the average number of non-unanimous votes in the preceding transmission; i.e., the DE(5) in the AQC-ALE Response shall report the average number of non-unanimous votes in the AQC-ALE Call, and the DE(5) in the Acknowledgement shall report the average number of non-unanimous votes in the Response.

	Bit 3	Bit 2	Bit 1	Bit 0	Description
DE(5)	0	<BER Range>			one bit spare, 3 bits of BER variation data

The average number of non-unanimous votes shall be encoded in accordance with Table A-XLI for transmission in DE(5).

TABLE A-XLI. DE(5) Encoding of BER Range.

Average Non-Unanimous Votes	Bit index
0	000
1	001
2 - 3	010
4 - 8	011
9 - 13	100
14 - 19	101
20 - 25	110
>25	111

A.5.8.1.5.6 DE(6) LQA measurement.
DE(6) shall be sent in the PART 2 word in the conclusion of AQC-ALE Response and Acknowledgement frames. The Link Quality Measurement contains the predicted quality of the channel to handle traffic. This value may be used as a first approximation to setting data rates for data transmission, determining that propagation conditions could carry voice traffic, or directing the station to continue to search for a better channel. (See A.5.8.1.5.5 for a description of the LQA.) This can also be used to determine which channels are more likely to provide sufficient propagation characteristics for the intended Inlink state traffic. Table A-XLII shall be used to encode the measured mean SNR value. An additional column is provided suggesting possible channel usage for the given SNR value.

TABLE A-XLII. LQA scores.

Value	Measured SNR	Potential Channel Usage
0	SNR <= -6	Choose another channel
1	-6 < SNR <= -3	use 50 to 75 bps data
2	-3 < SNR <= 0	use 50 to 75 bps data
3	0 < SNR <= 3	use 150 bps data
4	3 < SNR <= 6	use 300 bps data
5	6 < SNR <= 9	use 300 bps data
6	9 < SNR <= 12	use 1200 bps data, could carry voice, digital voice, KY-100 data, secure digital voice
7	12 < SNR <= 15	use 1200 bps data, could carry voice
8	15 < SNR <= 18	use 2400 bps data, could carry voice
9	18 < SNR <= 21	use 2400 bps data, could carry good quality voice, HFD Voice, Secure HFD Voice
10	21 < SNR <= 24	use 4800 bps data, could carry high quality voice
11	24 < SNR <= 27	use 4800 bps data, could carry poor quality voice
12	27 < SNR <= 30	Very high data rates can be supported (9600 baud)
13	30 < SNR <= 33	
14	SNR > 33	
15	No Measurement Taken	Value in DE(5) shall be ignored

A.5.8.1.5.7 DE(7) number of Tis/Twas left in sounding cycle.
While transmitting the sounding frame, DE(7) shall be sent in each TIS/TWAS word to identify the remaining number of TIS/TWAS words that will be transmitted in the frame. This is an inclusive number and when set to a value of 1, only one PART2 word remains in the frame.

When the sound duration would require an initial count greater than 15, a count of 15 shall be used until the count can correctly decrement to 14. From this point, DE(7) shall count down to 1.

A.5.8.1.5.8 DE(8) inlink data definition from INLINK.
Inlink Event transaction definitions are defined by 2 data exchange words. DE(8) shall be used when the INLINK preamble is used, while DE(9) shall be used for the second half of the address begun with the INLINK preamble.

	Bit 3	Bit 2	Bit 1	Bit 0	Description
DE(8)	AckThis	<# of Command Preambles>			Most Significant Bits of the Inlink Transaction Code

A.5.8.1.5.8.1 Acknowledge this frame.
Data Bit3, ACK-THIS, when set to 1, shall indicate that the stations which are linked to the transmitting station are to generate an ACK Inlink message in response to this frame. If the address section of an Inlink transaction is present, then only the addressed stations in the link are to respond. The responding station Inlink event shall return a NAK if any CRC in the received message fails, otherwise the Inlink event shall be an ACK. When Data Bit3 is set to 0, the transmitting station is broadcasting the information and no response by the receiving stations is required.

A.5.8.1.5.8.2 Identify command section count.
Data Bits 0-2 represent the number of command sections that are present in the frame. A value of 0 indicates no command sections are present, i.e., the frame is complete when the immediately following PART2 address word is received. A value of 1 indicates that 1 command section is present. Up to seven command sections can be transmitted in one Inlink event transaction.

A.5.8.1.5.9 DE(9) Inlink data definition from PART2.
Inlink Event transaction definitions are defined by 2 data exchange words. DE(9) is used for the second half of the address begun with the INLINK preamble.

	Bit 3	Bit 2	Bit 1	Bit 0	Description
DE(9)	I'm Inlink	<	Transaction Code	>	Least significant 4 bits of Inlink

A.5.8.1.5.9.1 I AM remaining in a link state.
Data Bit3, I'mInlink, when set to 1, shall indicate that the transmitting station will continue to be available for Inlink transactions. When set to 0, the station is departing the linked state with all

associated stations. It shall be the receiver's decision to return to scan or perform other overhead functions when a station departs from a link state. All Inlink event transactions should set this to '1' when the members of the link are to remain in the linked state.

Valid combinations of data bit ACK-THIS and I'mInlink are defined in table A-XLIII.

TABLE A-XLIII. Valid combinations of ACK-This and I'm Inlink.

Ack This Value	I'm Inlink Value	Description
0	0	Station departing linked state
0	1	Station remaining in linked state
1	0	Not valid. A station cannot leave a link and expect a response
1	1	Acknowledge this transmission.

A.5.8.1.5.9.2 Inlink event transaction code.
Data Bits 0-2 represent the type of Inlink event that is being transmitted. Table A-XLIV shall be used to encode the types of Inlink events. The Operator ACK/NAK and AQC-ALE Control Message sections are described in A.5.8.3.

TABLE A-XLIV. DE(9) inlink transaction identifier.

Value	Notes	Meaning	Message Section Count
0		Reserved	0
1		MS_141A Section Definition. Each section shall be terminated with a CRC	1 to 7
2		ACK'ng Last Transaction	0
3		NAK'ng Last Transaction	0
4	(1)	Directed Link Terminate	0
5	(1) (2)	Operator ACK/NAK	1
6	(1) (2)	AQC-ALE Control Message	1 to 7
7		Reserved	0
FIGURE 3.Requires that an address section (To,Part2) was received in the frame. FIGURE 4.Optional Transaction Code.			

A.5.8.2 AQC-ALE frame structure and protocols.

A.5.8.2.1 Calling cycle.
The calling cycle frame is used when the caller is attempting to reach a station that is scanning. Sufficient address words are repeated continuously until the scanning radio has had ample opportunity to stop on the channel. Other receivers, upon hearing an address, may recognize the presence of an ongoing call and skip processing the channel until the handshake is completed.

The calling cycle shall be composed of the target address broadcast for at least the period defined as the call duration for the radio, followed by the target address followed by the caller's (source) address. Data exchange values shall be per the specific type of call being attempted. When the call duration is not evenly divisible by 2 Trw, then an additional full address may be transmitted. When an entire address is not used to complete a fractional portion of the call duration, the caller shall begin the transmission with the second half of the target address using the PART2 preamble. In this case, the LP word number shall be 1.

When the radio is programmed to automatically derive the call duration, the equation shall be:

Number of Channels * 0.196

Table A-XLV specifies minimum and maximum number of words used for the scanning cycle section of a call. The total number of words used for calling is four additional words. The unit call time column presents the maximum time to complete a unit call as measured from the first tone transmitted by the caller to the last tone transmitted by the caller in the Acknowledgement frame. Users will see times greater than these due to call setup time, caller tune time, listen before call, and link notification delay; these may add several seconds to the response time seen by a user.

TABLE A-XLV. Scanning part duration using automated calculation.

Channels	AQC-ALE Minimum Scan Trw	AQC-ALE Maximum Scan Trw	Call Time in Seconds
1	0	0	4.8
2	1	2	5.6
3	2	2	5.6
4	2	2	5.6
5	3	4	6.4
6	3	4	6.4
7	4	4	6.4
8	4	4	6.4
9	5	6	7.2
10	5	6	7.2
11	6	6	7.2
12	6	6	7.2
13	7	8	8.0
14	7	8	8.0
15	8	8	8.0
16	8	8	8.0
17	9	10	8.8
18	9	10	8.8
19	10	10	8.8
20	10	10	8.8

A.5.8.2.2 Unit call structure.

A unit call in AQC-ALE follows the same principles as a standard ALE unit call with the following changes. In the Leading Call section of the Call and Response, the address shall appears once instead of twice. In the Acknowledgement frame, only the conclusion section shall be sent. See figure A-53 for an example of a unit call sequence from SOURCE to TARGET.

- See A.5.8.2.1, Calling Cycle to determine the maximum number of words to send during the scanning call portion of the Call.
- An Inlink Event Transaction shall be used in lieu of the Acknowledgement frame when ALE data traffic is available for the Inlink State in AQC-ALE.

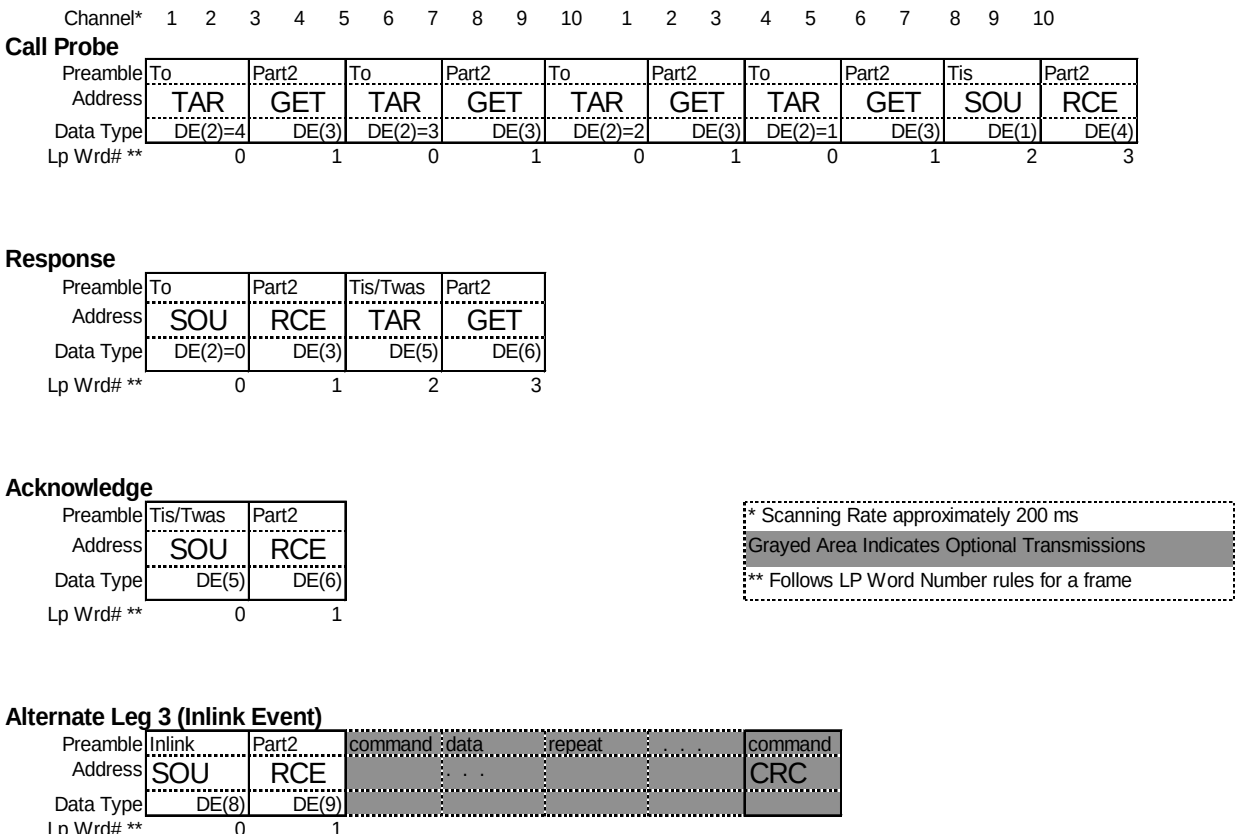


FIGURE A-53. Example of unit call format.

A.5.8.2.3 Star net call structure.

The call probe shall be identical to a Unit call where the star net address replaces the unit address. The Slotted Response portion shall always use a two word address for the TO and TIS addresses. Just as in Baseline 2G ALE, the slotted response shall be 5 Tw wider than the 6 Tw needed to transmit the TIS/TWAS address. Slot 0 shall be 17 Tw to accommodate a non-net member participating in the call. Slot 1 and all remaining slots shall be 11 Tw wide. No LQA information shall be emitted in the Acknowledgement portion of the Start Net Call except as provided through the data exchange bits.

The Data Exchange values shall be per figure A-54.

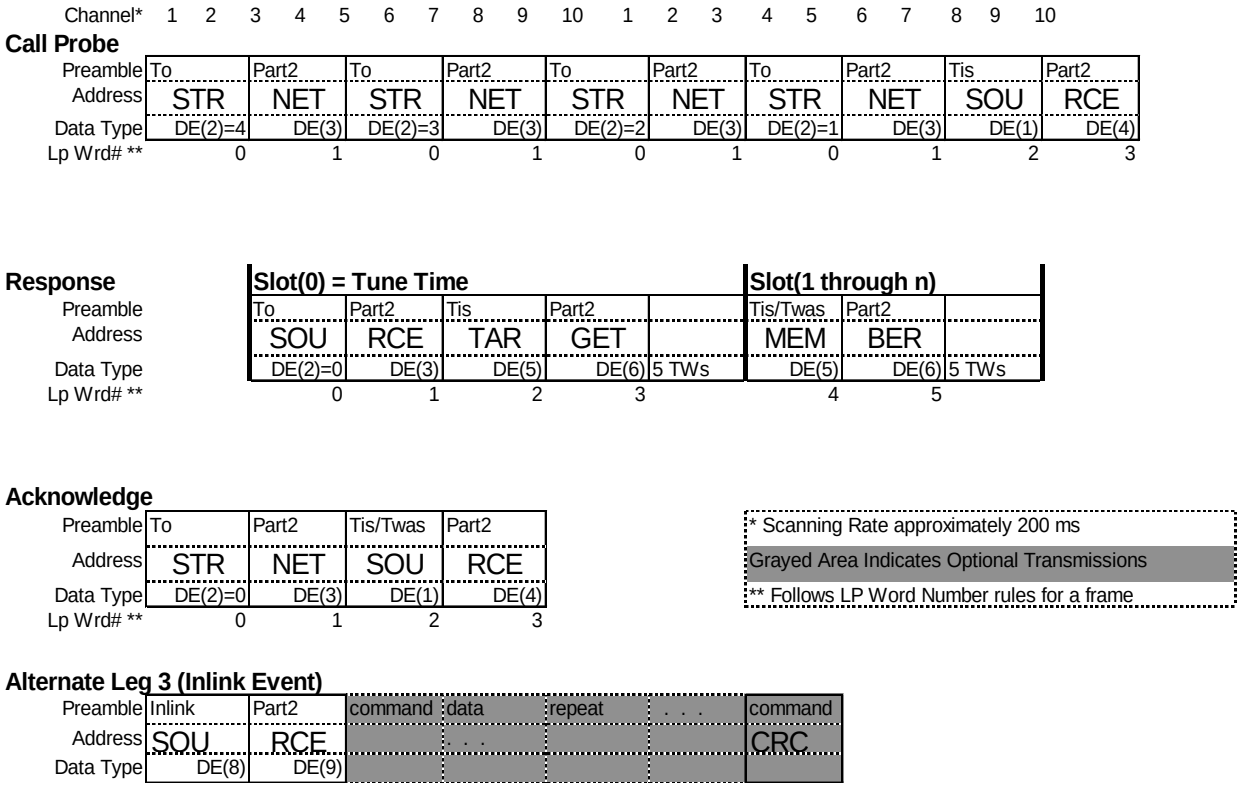


FIGURE A-54. Example of StarNet format.

An Inlink Event frame may be used for the Acknowledgement frame. Slots 1 and beyond may be expanded by fixed number of Trw for certain types of AQC-ALE Inlink Messages.

A.5.8.2.4 AllCall frame formats.

A station placing an AllCall shall issue the call using the calling cycle definition in A.5.8.2.1. The actions taken shall be as described for baseline 2G ALE AllCalls. The Data Exchange values shall be per figure A.-55, AllCall Frame Format. Selective AllCall shall be supported.

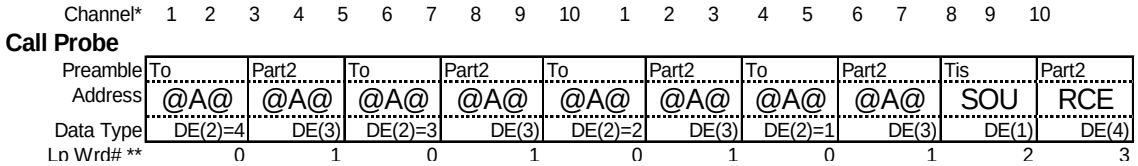


FIGURE A-55. Example AllCall frame format.

A.5.8.2.5 AnyCall frame formats.

A station placing an AnyCall shall issue the call using the calling cycle definition in A.5.8.2.1. The actions taken shall be a described for baseline 2G ALE AnyCalls except that the Slot width shall be fixed at 17 Tw. The leading address section and conclusion shall be used for each slotted response. The Data Exchange values shall be per figure A-56. Selective AnyCall and Double Selective AnyCall shall be supported.

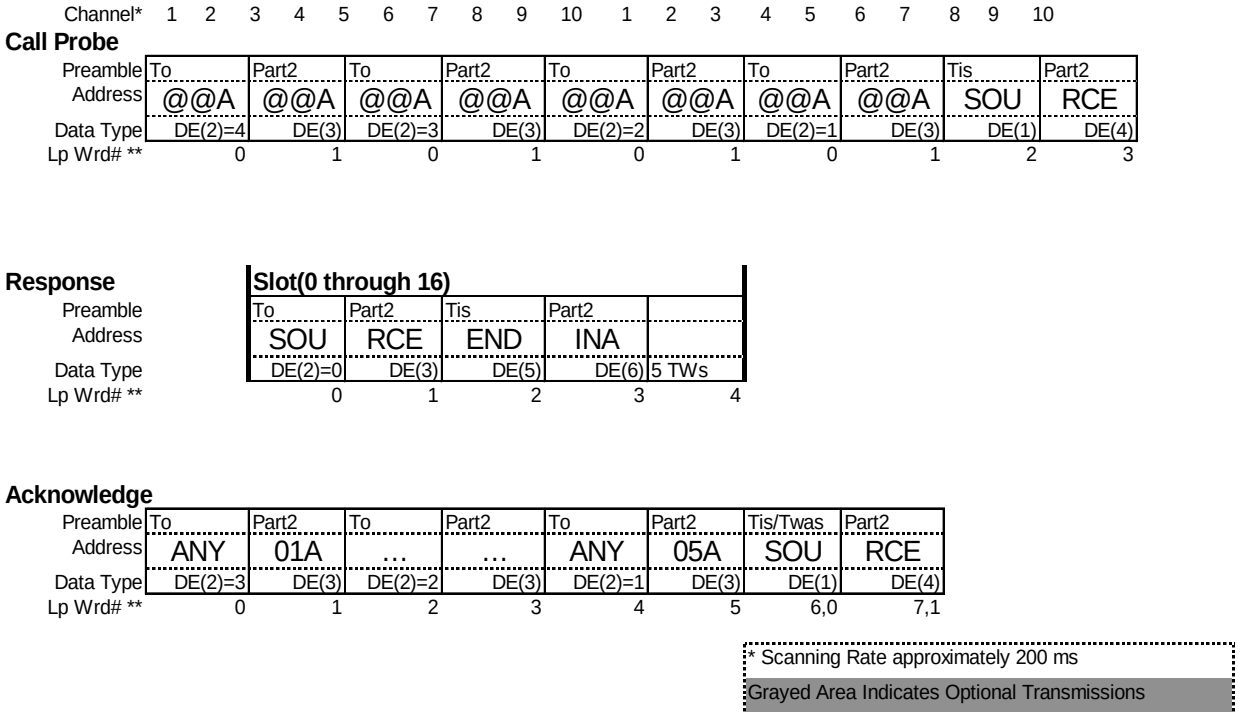


FIGURE A-56. Example AnyCall frame formats.

An Inlink Event frame shall not be used for the Acknowledgement frame.

A.5.8.2.6 Sounding.
The sounding cycle shall be composed of the station's address broadcast for at least the period defined as the sound duration for the radio. Data exchange values shall be as denoted in figure A-57. When the call duration is not evenly divisible by 2 triple-redundant word times, then the additional full address may be transmitted. When an entire address is not used to complete a fractional portion of the sound duration, the caller shall begin the transmission with the second half of the target address using the PART2 preamble. In this case, the LP word number shall be 1. As shown in figure A-57, the LP word number shall toggle between 0 and 1.

When the radio is programmed to automatically derive the sound duration, the equation shall be:

Number of Channels * 0.196 + 0.784

See figure A-58 for the minimum and maximum number of Trw to broadcast automatically.

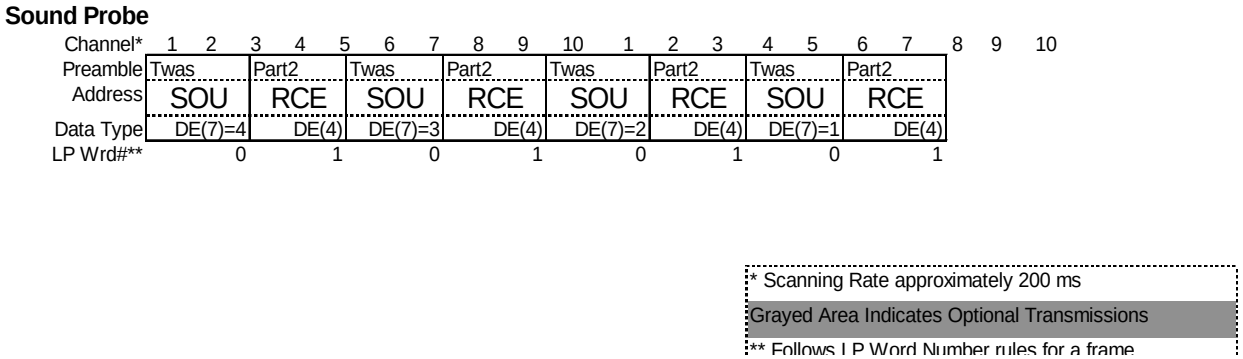
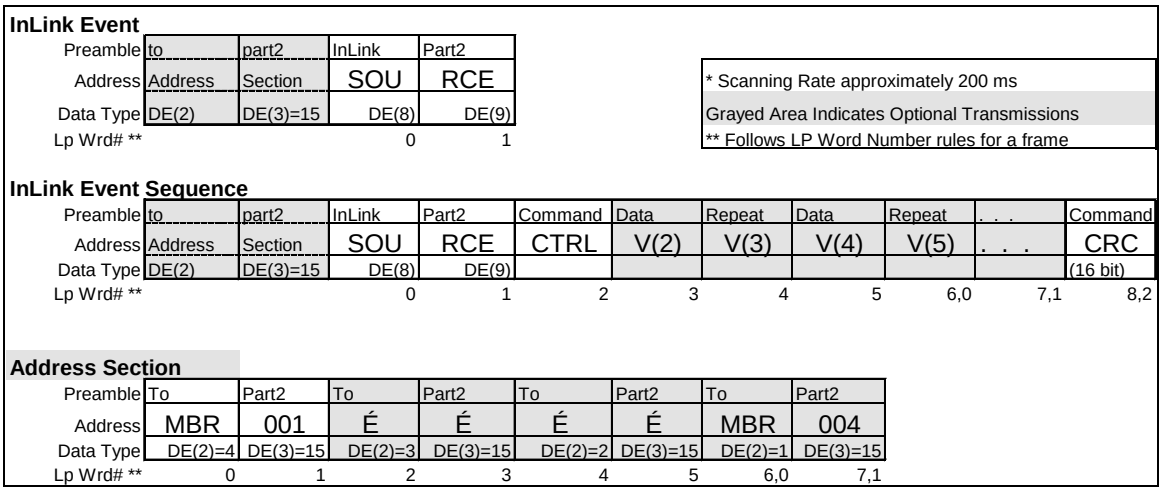


FIGURE A-57. Example sounding frame format.

A.5.8.2.7 Inlink transactions.
AQC-ALE stations shall have the capability to transfer information within the Inlink state of the radio. A special purpose frame is defined for the purpose of separating link establishment transactions from transactions that occur during the Inlink state. Two types of Inlink transactions are defined, Inlink Event and Inlink Event Sequence. Either transaction can have an optional address section appended to the beginning of the frame. This optional address section indicates that the transaction is targeted at the addresses defined in this section of the frame.

The Inlink frame uses Data Exchange DE(8) and DE(9). DE(8) informs the recipient of the type of transaction and whether this frame needs to be acknowledged. See A.5.8.3.8. DE(9) data content indicates to the caller the exact form of the data and identifies if the sender intends to remain in the linked state with all those represented in the address section of the frame. When the address section is omitted, the frame shall be targeted to all stations currently linked with the transmitting station. See A.5.8.3.9.

The data Exchange values shall be per figure A-58. This figure outlines the general format of both types of Inlink transaction events.



InLink Event

Preamble	to	part2	InLink	Part2
Address	Address	Section	SOU	RCE
Data Type	DE(2)	DE(3)=15	DE(8)	DE(9)
Lp Wrd# **			0	1

* Scanning Rate approximately 200 ms
Grayed Area Indicates Optional Transmissions
** Follows LP Word Number rules for a frame

InLink Event Sequence

Preamble	to	part2	InLink	Part2	Command	Data	Repeat	Data	Repeat	. . .	Command
Address	Address	Section	SOU	RCE	CTRL	V(2)	V(3)	V(4)	V(5)	. . .	CRC
Data Type	DE(2)	DE(3)=15	DE(8)	DE(9)							(16 bit)
Lp Wrd# **			0	1	2	3	4	5	6,0	7,1	8,2

Address Section

Preamble	To	Part2	To	Part2	To	Part2	To	Part2
Address	MBR	001	É	É	É	É	MBR	004
Data Type	DE(2)=4	DE(3)=15	DE(2)=3	DE(3)=15	DE(2)=2	DE(3)=15	DE(2)=1	DE(3)=15
Lp Wrd# **	0	1	2	3	4	5	6,0	7,1

FIGURE A-58. Example inlink transaction TRW sequences.

A.5.8.2.7.1 Inlink transaction as an acknowledgement (NT).
The Inlink Event or the Inlink Event Sequence shall be used as the Acknowledgement frame of a handshake whenever the calling radio has a message for the radios entering the Inlink state. If the INLINK preamble is replacing a TIS preamble indicating that the radios were to remain in an Inlink state, then the I'M LINKED bit shall be set to 1. If a TWAS preamble would normally be used for this transmission, the I'M LINKED bit shall be set to 0. Thus, the calling station can minimize over the air time for any transaction by judicious use of Inlink state and associated control bits.

A.5.8.2.7.2 CRC for Inlink event sequences.
As seen in figure A-58, a command section of an Inlink event sequence shall consist of the COMMAND preamble, followed by the data associated with the command using the preambles DATA and REPEAT. The Inlink event sequence frame shall be terminated with a COMMAND preamble containing the CRC of the data contained in all words starting with the first COMMAND preamble. The procedure for computing the CRC of AQC inlink transmissions differs from that in paragraph A.5.6.1. The same polynomial shall be used ($X^{16} + X^{12} + X^5 + 1$) but the shift register shall be initialized to all 0, bits of the ALE words to be checked shall be processed starting with the least-significant bit, and the final shift register contents shall not be inverted, but shall instead be bit reversed. For the AMD example in 5.6.1, this procedure produces 0x4FF6.

The receiver shall maintain a history of failed CRC. The history may be displayed to the operator or used in channel selection algorithms for follow-on traffic.

A.5.8.2.7.3 Use of address section.
The address section of a Inlink transaction, when present, shall indicate that the addressed stations in the link are to react to the information contained in the message section.

A.5.8.2.7.4 Slotted responses in an Inlink state (NT).
When an acknowledgement has been requested, each radio in the address section shall be assigned a response slot in the same manner as a standard ALE group call. The slot width shall be as specified for AQC-ALE StarNet call, A.5.8.2.4. When the address section contains a StarNet address, the slot assignments shall be per the StarNet definition. When no slot assignment can be determined and an acknowledgement is requested, the receiving radio shall respond as quickly as possible.

Slotted responses shall use an Inlink transaction frame beginning with the INLINK preamble. The address section shall not be permitted in the slotted response. When a the transmitting station issues a message that requires a responding message, such as time-request to Time-is, the slot widths for slot 1 and greater shall automatically expand by a fixed number of Trw to satisfy the response.

When a response could be variable in length, the maximum slot width shall be used. The maximum width in Tw for an Inlink transaction shall be 44 Tw. This could represent an AMD message of up to 27 characters.

A.5.8.3 AQC-ALE orderwire functions (optional) (NT).
The Operator ACK/NAK and AQC-ALE Control Message sections are described below. These functions may only appear in frames containing INLINK transactions, and may never be used in baseline 2G ALE frames.

A.5.8.3.1 Operator ACK/NAK transaction command section (optional) (NT).
This optional message section is a means to poll every station to determine if a site is currently manned. The operator must respond to the request for acknowledgement in a timely manner. AMD messages formatted in accordance with table A.5.8-11 Operator ACK/NAK shall be used to define the values and meaning of the message. When a request for ACK is received, the operator shall have 15 seconds to respond. The ACK message shall be sent immediately as an Inlink Event if the operator responds. If no response from the operator occurs the receiving station shall emit an Operator NAK response Inlink Event.

TABLE A-XLVI. Operator ACK/NAK command.

AMD Message Section Content	Action to be Taken
"REQ"	Receiving station should notify operator that a response to this message is required. The response must occur within 15 seconds.
"ACK"	The operator acknowledges receipt of last Inlink event.
"NAK"	The operator failed to respond to the last Inlink event.

A.5.8.3.2 AQC-ALE control message section (optional) (NT).
Table A-XLVII defines the values used to declare a AQC-ALE control message. When sending these commands, all commands in the frame shall be AQC-ALE control messages. Table A-XLVI defines which message types in an AQC-ALE message section are mandatory for all implementations of AQC-ALE and which messages are optional for AQC-ALE implementations.

TABLE A-XLVII. AQC-ALE control message section word sequences.

MsgId Value	# Words	Description	Handle Message Section
0	n	AMD Dictionary Message	Mandatory
1	3	Channel Definition	Mandatory
2	1	Slot Assignment	Mandatory
3	1	List Content of Database	Optional
4	1	List Database Activation Time	Optional
5	2	Set Database Activation Time	Optional
6	n	Define Database Content	Optional
7	n	Database Content Listing	Optional

As seen in figure A-59, each word with a COMMAND preamble contains a 5-bit MsfID field to define the type of control message present. Because ALE orderwire functions are still allowed, MsgID values greater than 7 are not allowed, as these would overlap with existing ALE orderwire commands.

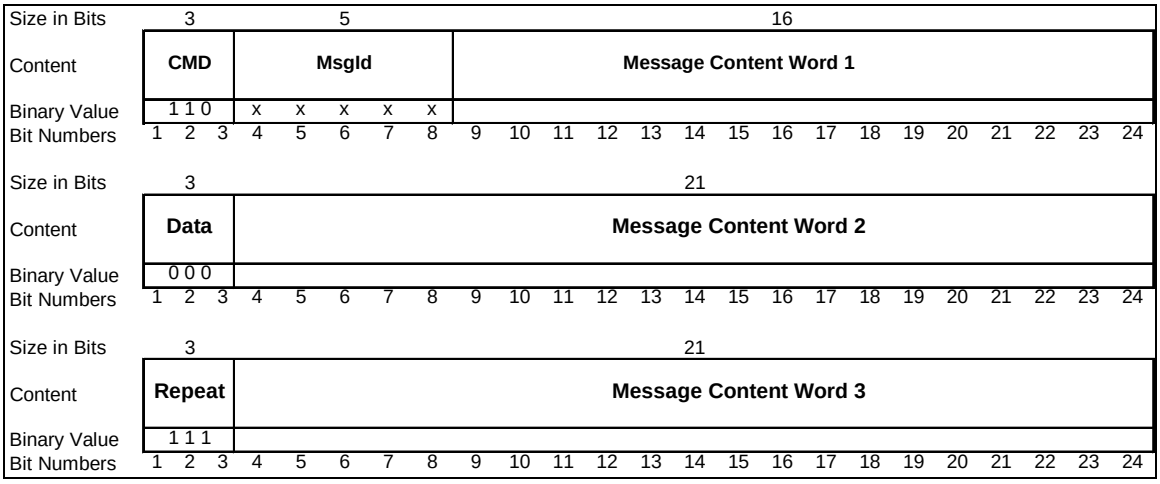


FIGURE A-59. Generalized AQC-ALE control message format.

A.5.8.3.2.1 AMD dictionary message (NT).
When a message section can be translated into a dictionary and all stations linked are using AQC-ALE, an AMD message may use the dictionary word as provided in table A-XLVIII. Each character in the AMD message will represent itself or a word/phrase found in one of three look up tables. Because messages are short, when a transmission word is lost, the complete message could be rendered meaningless if a bit packing approach was used. This method shall consist of a series of 7-bit values. This is the same size as currently used for an AMD message. At a min-

imum, a radio shall provide lookups for values 2 through 95. A mapped entry can be of any length. Every radio communicating with packed AMD formats must use the same programmed values for words or confusion in the message will result. Messages should be displayed in their unpacked form as looked up or optionally with curly braces around the numeric value of the lookup, i.e. {2.5} would indicate word is in Dictionary Set 2 at index position 5. (See figure A-60 for the format of an AQC-ALE Packed AMD message.)

The two dictionaries sets provide a means to identify the most frequently used words communication for a mission. Dictionary Set 1 shall be the initial dictionary used for values 96 through 127. When a character with value 1 is received in a Packed AMD Message, then Dictionary Set 2 shall be the word list for character values 96 through 127 until the end of that message or receipt of a character with value 0 in that message, after which Dictionary Set 1 shall again be used, and so on.

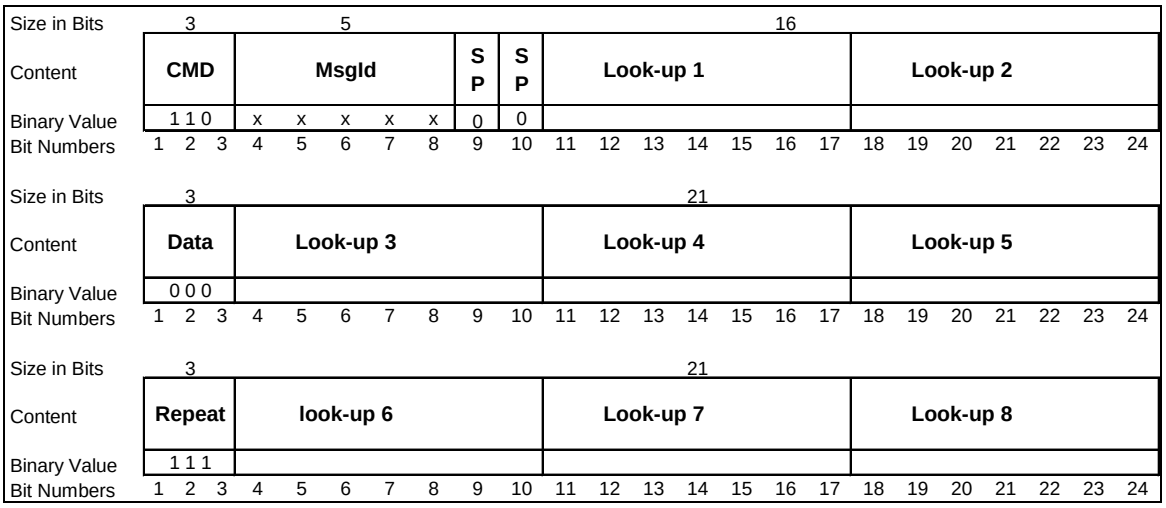


FIGURE A-60. AQC-ALE dictionary lookup message.

A network manager might choose to minimize air time and provide some unique information using Dictionary Set 1 by placing tactical user phrases in the dictionary, such as "**AT WAY POINT**". To identify where the a unit is, the AMD message "**AT WAY POINT 1**" would be entered. What would be transmitted in the Packed AMD message would be a 4 TRW Inlink event transmission consisting of INLINK, PART2, COMMAND, REPEAT preambles. That is the entire message would fit in one COMMAND TRW as:

- Message Type = AQC-ALE Packed AMD Message
- Look-up 1 = Index into Dictionary Set 1 for "**AT WAY POINT**"
- Look-up 2 = The character "**1**"

No spaces are needed because the lookup table transform shall place spaces into the expanded message as defined in table A-XLIX.

TABLE A-XLVIII. Lookup tables for packed AMD messages.

ASCII Ordinal Value	Dictionary Set 0 (0 to 31)	ASCII 64 Character Set (32 to 63)	ASCII 64 Character Set (64 to 95)	Dictionary Set 1 (96 to 127)	Dictionary Set 2 (96 to 127)
0	(Use Set 1)	Space	@	Programmable	Programmable
1	(Use Set 2)	!	A	Programmable	Programmable
2	A	"	B	Programmable	Programmable
3	AN	#	C	Programmable	Programmable
4	AND	$	D	Programmable	Programmable
5	ARE	%	E	Programmable	Programmable
6	AS	&	F	Programmable	Programmable
7	BE	'	G	Programmable	Programmable
8	CAN	(	H	Programmable	Programmable
9	EACH	)	I	Programmable	Programmable
10	EAST	*	J	Programmable	Programmable
11	FOR	+	K	Programmable	Programmable
12	FROM	,	L	Programmable	Programmable
13	IN	-	M	Programmable	Programmable
14	IS	.	N	Programmable	Programmable
15	NORTH	/	O	Programmable	Programmable
16	NOT	0	P	Programmable	Programmable
17	OF	1	Q	Programmable	Programmable
18	ON	2	R	Programmable	Programmable
19	OR	3	S	Programmable	Programmable
20	SIZE	4	T	Programmable	Programmable
21	SOUTH	5	U	Programmable	Programmable
22	SYSTEM	6	V	Programmable	Programmable
23	THAT	7	W	Programmable	Programmable
24	THE	8	X	Programmable	Programmable
25	THIS	9	Y	Programmable	Programmable
26	TO	:	Z	Programmable	Programmable
27	USE	;	[	Programmable	Programmable
28	WEST	<	\	Programmable	Programmable
29	WILL	=	]	Programmable	Programmable
30	WITH	>	^	Programmable	Programmable
31	YOU	?	___	Programmable	Programmable

TABLE A-XLIX. Adding spaces during AMD unpacking.

	Message Value is in a Dictionary	Message Value is in ASCII-64 and not Alphanumeric	Message is Value is Alphanumeric
First Character of Message	No Leading Space	No Leading Space	No Leading Space
Last Expanded Character from Lookup	Add Leading Space	No Leading Space	Add Leading Space
Last Expanded Character is ASCII-64	Add Leading Space	No Leading Space	No Leading Space

A.5.8.3.2.2 Channel definition (NT).
The channel definition provides a system to reprogram the radio with a different frequency or to cause stations in a link to move to a traffic channel. This allows the radios to listen for general propagation characteristics in a common area and then move to a nearby channel to manage the inlink state transactions. By allowing a channel to be reprogrammed, the radio can adapt to a wide variety of conditions that may occur on a mission. If congestion is experienced on the assigned frequency, the stations shall return to the normal scan list and reestablish the call.

The channel index number is specified from a range of 0 to 255. A radio shall have at least 100 channels available for reprogramming. A channel index of 0 shall indicate that the receive and transmit frequencies are to be used for the remainder of this link. Other channel index numbers indicate that the new assignment shall be entered into the channel table.

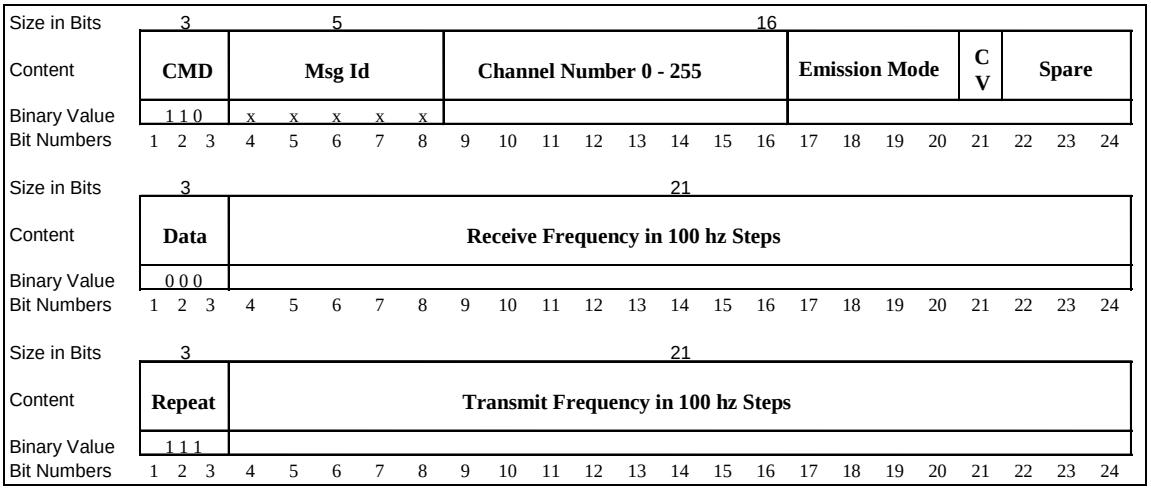


FIGURE A-61. Channel definition and meet-me function.

Frequencies shall be specified as a 21-bit values with each step being 100 Hz. See figure A-61 for an example format of this message. A 2-bit value 0 for emission mode shall indicate upper side band and a value of 1 shall indicate a value of lower side band. Bits 17-18 refer to the receive frequency, bits 19-20 to the transmit frequency. A value of "1" in bit 21 or the Channel Verification bit indicates that the called station will initiate an inlink transmission requesting an acknowledgement from the calling station upon going to the new channel. This bit is only valid in the event that the Channel Number was specified to be "0".

A.5.8.3.2.3 Slot assignment (NT).
The slot assignment feature allows a control station to dynamically assign response slots for stations with which it is linked. In this manner, when a response is required from several stations in an inlink state, orderly responses can be generated. The slot width shall be in Tw. When set to 11 or less, the radio shall respond with the shortest form possible allowing for 5 Tw as timing error. Figure A-62 depicts the format of a slot assignment.

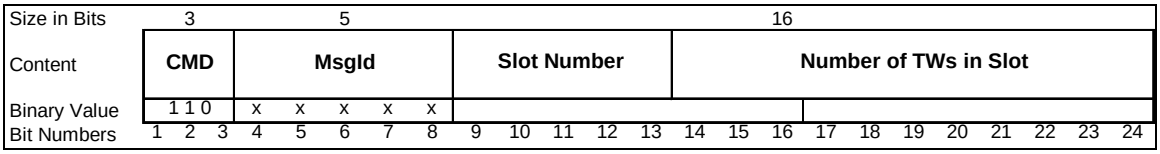


FIGURE A-62. AQC-ALE slot assignment.

Examples of this usage would be setting up a link to several stations and then periodically polling them with an operator ACK/NAK request or a position report request. Each radio would respond at a specified time following that transmission. This form of time division multiplexing is self-synchronizing to minimize the need for time of day clock synchronization. If more traffic is required on a channel, slot widths can be expanded.

A.5.8.3.2.4 List content of database (NT).
The list content of database (FIGURE a-63) shall display the programmable values of a scanning radio such that the receiver can inter-operate with that station in the best possible manner. This command requests the contents to be displayed. The Database identifier shall be the ASCII36 character set plus the characters “*” and “_”.

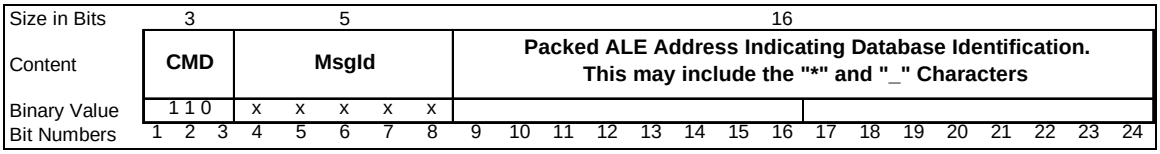


FIGURE A-63. List content of database.

A.5.8.3.2.5 List database activation time (NT).
This function requests the time stamp of a database. Its format is identical to that shown in figure A-64.

A.5.8.3.2.6 Set database activation time (NT).
This function (figure A-64) sets or displays the time stamp of a database. The first word format of the command is identical to the List Content of Database. The second word contains the time of day that the database is to be active. Only one database shall be active at a time. When the SET bit=1, the command represents the time to assert when the database becomes active. When the SET bit=0, this is a report of the current time set value.

A network control station can program or select preprogrammed channel sets and then cause all mission participants to switch to a new set of channels to operate upon. Other uses would include moving from one area of the world to another may cause the user to move into a different set of allocated frequencies.

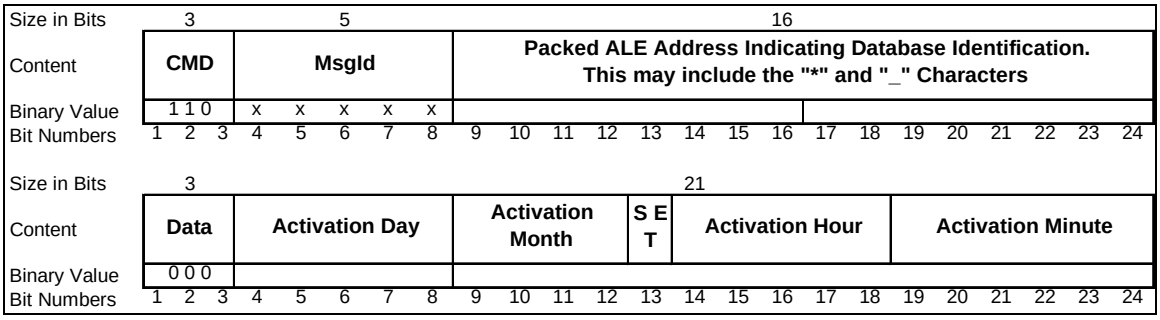


FIGURE A-64. Set database activation time.

A.5.8.3.2.7 Define database content (NT).
This function defines a database over the air. The first TRW format of the command is identical to the List Content of Database. Subsequent words contain association of existing information into a dataset that the radio may operate against. As shown in figure A-65.

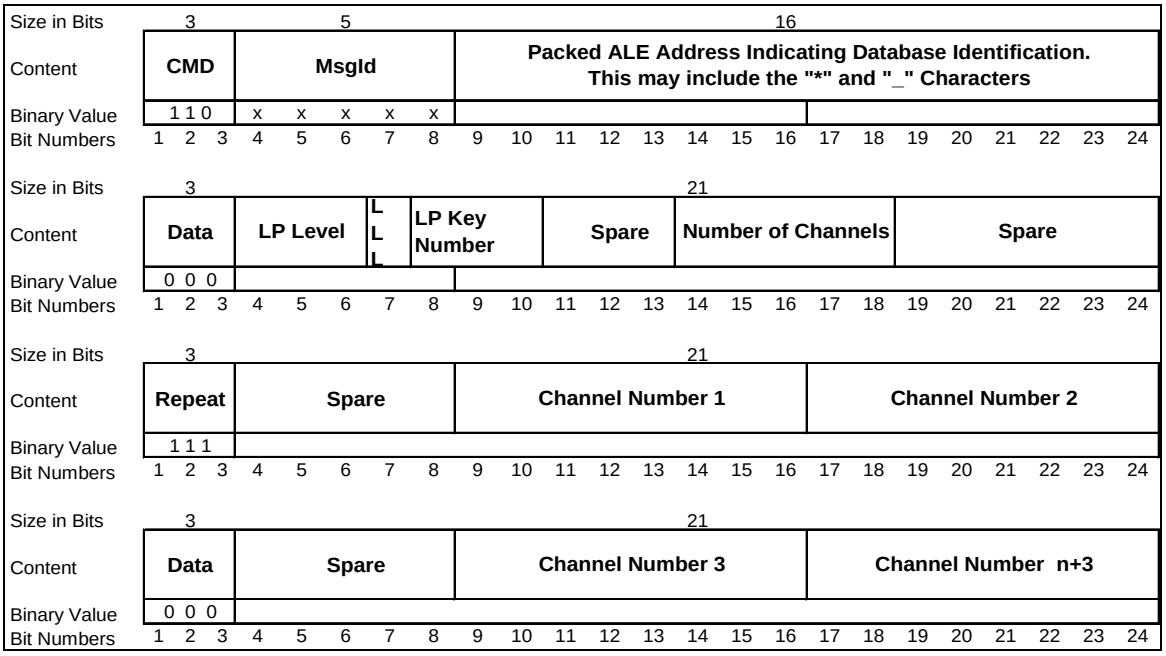


FIGURE A-65. Define database content.

Word 2 of the message shall consists of:

- 3 bits of LP Level number. Values range from 0 through 4.

- 1 bit for Lower Level Linking. When set to 1, the radio shall honor lower level link attempts.
- 3 bits for LP Key number identification. A value of 0 indicates no key assignment. When an LP level greater than 0 exists, this would be an non-operational condition. If more than one type of key is used between LP levels, they must use the same key index. When a radio does not have a key present for a given LP Key, a value of NOKEY shall be used.
- 5 bits for the number of channels. Immediately following this word shall be (number_of_Channels/2) words containing the channel numbers to use. Earlier commands defining channel numbers or a preprogrammed value define the actual frequencies used.
- 6 bits for defining the words from a dictionary into the 64 words. The mapping of a dictionary into a database dictionary allows a specific set of words that yield a higher frequency hit rate to the dictionary. A value of 0 indicates using the orginal programmed dictionary. The mapping of the dictionary is contained in the Trw that follow the channel association.

A.5.8.3.2.8 Database content listing (NT)
This command shall have the same format as the Define Database Content.

A.5.8.4 AQC-ALE linking protection.
When operating in LP with AQC-ALE, every 24-bit AQC-ALE word shall be scrambled in accordance with Appendix B. The same rules for LP in baseline 2G ALE shall be applied to AQC-ALE with the following exceptions:

- The word number for all TO AQC-ALE words during the scanning call shall be 0, and the word number for all PART 2 AQC-ALE words during the scanning call shall be 1. The TIS or TWAS word that concludes a scanning call shall use word number 2 and the following PART 2 word shall use word number 3.
- The AQC-ALE response frame shall use word numbers 0, 1, 2, and 3.
- A 2-word AQC-ALE acknowledgement shall use word numbers 0 and 1. The TOD shall be later than that used at the end of the scanning call.

ANNEX A. DEFINITIONS OF TIMING SYMBOLS

C	Number of channels in sequence
H	Handshake. Completed sequence of call, response, and acknowledgment
n	Integer
NA	Number of addresses
NAm	Number of addresses with “m” words
NAW	Number of original individual address words
NS	Number of slots in response period, total
s	Seconds
SN	Slot number identification
T	Time
T_a	Individual station (or net) whole address time
T_{al}	Individual station (or net) address first word time
$T_{a\ max}$	Maximum individual station (or net) whole address time limit
T_c	Call time, combination of whole address(es), which is usually repeated as a leading call T_{1c}
T_{c1}	Combined different first words of group station address
T_{cc}	Calling cycle time
$T_{c\ max}$	Maximum call time limit
T_d	Basic dwell time on each channel during scan. Sometimes shown with channels per second scanning rate in ( ) e.g. T_d (5).
T_{dbm}	DBM time
T_{dek}	Decode time
T_{drrw}	Detect rotating redundant word time
T_{drw}	Detect redundant word time
T_{ds}	Detect signaling (tones and timing) time
T_{enk}	Encode time
T_{1c}	Leading call time

T_{1d}	Late detect word additional time
Tlrw	on-air leading redundant words
T_{1ww}	Last word wait delay
T_m	Orderwire message section time
$T_{m\ max}$	Maximum orderwire message section time limit
T_p	Propagation time
T_{ps}	Periodic sounding interval
T_{rc}	Redundant call time
T_{rd}	Receiver internal signal delay time
T_{rs}	Redundant sound time
Trsc	scanning redundant call time
T_{rw}	Redundant word time (392 ms)
T_{rwp}	Redundant word phase delay (0 to T_{rw})
T_s	Scan period
T_{sc}	Scan calling time, same as T_{ss}
$T_{s\ max}$	Maximum scan period
$T_{s\ min}$	Minimum scan period
T_{src}	Scanning redundant call time
T_{srs}	Scanning redundant sound time
T_{ss}	Scan sounding time, same as T_{sc}
T_{sw}	Slot width time
T_{swt}	Slot wait time delay after end of call, until slotted response starts
T_t	Tuneup time delay of antenna tuner or coupler
T_{ta}	Turnaround time, receipt of end of signal to start of reply
T_{tc}	Transmitter command (to transmit) time
T_{td}	Transmitter internal signal delay time
T_{tk}	Transmitter acknowledgment (that is transmitting) time
T_{tone}	Tone (8 ms)
T_w	Word time (130.66...ms)

T_{wa}	Wait for activity time
T_{wan}	Wait for net acknowledgment time (for called stations)
$T_{wan\ max}$	Maximum limit group call wait for reply time (for late arrival called stations)
T_{wce}	Wait for calling cycle end (message or terminator stations)
T_{wr}	Wait for reply time
T_{wrn}	Wait for net/group reply time (for calling stations)
T_{wrt}	Wait for reply and tune (scanning) time
T_{wt}	Wait (listen first) time before tune or transmit
T_x	Termination section time
$T_{x\ max}$	Maximum termination section time limit
WRT	Wait for reply timer (load with T_{wr})
WRTT	Wait for response and tune timer (load with T_{wrn} or T_{wrt})

ANNEX B. TIMING

NOTE: Refer to Annex A and Table A-XV.

Basic system timing

- Tone (symbol) rate = 125 symbols per second
- Tone period:

  T_{tone} = 8 ms per symbol
- On-air bit-rate = 375 bits per second
- On-air individual word period (never sent alone):

  T_w = 16.33... symbols x Ttone = 130.66...ms
- On-air (triple) redundant word period:

  T_{rw} = $3T_w$ = 49 tone = 392 ms
- On-air individual (or net) address time for m = 1 to 5 words:

  T_a = m x T_{rw} = 392 ms to 1960 ms
- Propagation time, range divided by speed of wave, for MF/HF signals, local to global:

  T_p = 0 to 70 ms

System timing limits

- Maximum individual station (or net address time limit), based on 15-character (or 5-word) maximum:

  $T_{a\ max} = 5\ T_{rw} = 1{,}960$ ms

- Individual (or net) address first word, used in scan call T_{sc}:

  $T_{al} = T_{rw} = 392$ ms

- Maximum group combined addresses different first words time limit, maximum 5 first words, in scan call T_{sc}:

  $T_{cl} = \Sigma\ T_{al}$ (different)

  $T_{cl\ max} = 5$ Tal $= 5$ Trw $= 1960$ ms

- Maximum call time limit, based on 12-word maximum, chole addresses in T_{lc}:

  $T_{c\ max} = 12$ Trw $= 4{,}704$ ms

- Maximum scan cycle period limit, based on 2 channels per second and 100 channels:

  $T_{s\ max} = 50$ s

- Maximum message (orderwire) section time limit, unless adjusted by CMD:

$T_{m\ max\ basic} = 30$ Trw $= 11.76$ s

$T_{m\ max}$ including $T_{m\ max\ AMD} = 29$ Trw* $+ 30$ Trw $= 23.128$ s

$T_{m\ max}$ including $T_{m\ max\ DTM} = 29$ Trw* $+ 353$ Trw $= 382$ Trw (149.744 s)

$T_{m\ max}$ including $T_{m\ max\ DBM} = 29$ Trw* $+ 3560$ Trw $= 3589$ Trw (1406.888 s)

*NOTE: $T_{m\ max}$ basic equals 29 T_{rw} when combined with AMD, DTM, or DBM. This is due to the requirement to commence the AMD, DTM, or DBM transmission one T_{rw} (392) ms) prior to the close of $T_{m\ max}$ basic which effectively reduces the value of $T_{m\ max}$ basic to 29 T_{rw} in these equations.

- Maximum termination section time limit, same as $T_{a\ max}$:

  $T_{x\ max} = T_{a\ max} = 1{,}960$ms

Individual calling

- Initial and minimum dwell time on each channel by receiving station during normal receive scanning; inverse of scanning rate; not including extended pause to read word:

  $T_d(5)_{min} = 200$ ms at 5 channels per second basic scan rate, or

$T_d(2)_{min}$ = 500 ms at 2 channels per second minimum scan rate

$T_d(10)_{min}$ = 100 ms at 10 channels per second (DO)

- Scan period for receiving station to scan all scanned channels during normal receive scanning, where "C" is the number of scanned channels; not including extended pause to read words:

  $T_{s\ min} = C \times T_{d\ min}$

For example,

$T_{s\ min}$ = 0 for single-channel, nonscan case, or

= 2 seconds for typical C = 10 at 5 chps, or

= 5 seconds for C = 10 2 chps minimum rate

= 1 seconds for C = 10 at chps (DO)

- For scan call T_{sc} computations, use T_s based on probable maximum pause on each channel (T_d, to read words) of $T_{drw} = 2\ T_{rw}$ (T_d may be adjusted by net managers for best system performance):

  $T_s = C \times T_d = C \times T_{drw}$

For example,

T_s = 7,840 ms for C = 10 channels and $T_d = T_{drw}$

- Call time, the called whole address (or combination of called whole addresses, if a group call), which may be repeated in the leading call T_{1c}; maximum limit 12 one-word addresses:

  $T_c = T_c$ (called) for single-station (or net) calls, or

  = T_a (first) + T_a (second) + T_a (last) if group call

- First-word call time, the called address first word (or combination of addresses first words, if a group call), which is repeated in the scanning call T_{sc}; maximum limit 5 different first words:

  $T_{1c} = T_{a1}$ (called) for single-station (or net) calls, or

  = T_{al} (first) + T_{a1} (second different) + T_{a1} (last different) if group call

- Leading call time, composed of two complete repetitions of Tc, which contains the whole address(es):

  $T_{1c} = 2T_c = 2T_a$ (called) for single-station (or net) calls, or

  = 2(T_a (first) + T_a (second) + T_a (last), if group call

- Scanning call time, consisting of repetitions of only the first word(s) T_{a1} of the called address (or combination of addresses, if a group call), for calling station to "capture" scan-

ning receivers during normal scanning calling. Therefore, T_{sc} is a multiple T_{c1} (group of T_{a1}'s if a group call) of words, which is ≥ the receiver's scan period T_s, where n is any integer such that $T_{sc} \geq T_s$:

$$T_{sc} = n \times T_{c1} \geq T_s = C \times T_d$$

For example,

$T_{sc} = 0$ for single-channel individual call case, or

$\geq 20\ T_{rw} = 7840$ ms if $C = 10$ and $T_d = T_{drw}$

- Calling cycle time for calling station to both "capture" scanning receivers and ensure reading the called station address(es), consisting of scan calling time (T_{sc}) plus leading call time (T_{1c}), respectively:

$$T_{cc} = T_{sc} + T_{1c} \geq T_s + T_{1c}$$

For example,

$T_{cc} = T_{1c} = 2T_a$ (called) = 784 ms for single-channel one-word address individual (or net) call case ($T_s = 0$), or

$= T_{sc} + T_{1c} = (20 + 2)\ T_{rw} + 8624$ ms if $C = 10$ and $T_d = T_{drw}$

- Single-channel redundant call time, consisting of individual (or net) leading call T_{1c} (with TO) plus terminator T_a (with TIS or TWAS), not including any message section time:

$T_{rc} = T_{1c} + T_x = 2T_c + T_x = 2T_a$ (called) + T_a (caller)

$= 3\ T_{rw\ min} = 1176$ ms minimum, for individual station (or net) call using one-word addresses.

$= 15\ T_{rw\ min} = 5880$ ms max for 5-word addresses

- Scanning redundant call time, consisting of scanning call time T_{sc}, and redundant call time T_{rc}, respectively:

$$T_{rsc} = T_{sc} + T_{rc}$$

For example, using one-word addresses:

$T_{src} = (20 + 3)\ T_{rw} = 9016$ ms if $C = 10$ and $T_d = T_{drw}$

- Last word wait additional fixed delay at replying or receiving station, after (possibly early) detected end of received call and before start of reply, to avoid on-air overlap, loss of additional termination (caller address) words, and to allow for transmitter turnaround for reception:

$T_{1ww} = T_{rw} = 392$ ms

- Late word detection additional fixed delay at calling station, to increase wait for reply time in case of possibly late detection at called station:

  $T_{1d} = T_w = 130.66...ms$

- Redundant word phase delay. To synchronize a transmission to any recently preceding transmissions, and used on all but first transmission of a handshake or exchange until terminated period:

  $T_{rwp} = 0 \text{ to } 392 \text{ ms} \leq T_{rw}$

- Turnaround time at replying station, measured at rf port(s); from end of received signal to start of transmitted reply, not including delays such as T1ww internal signal delays, T_{rd} and T_{td}; decode and encode times, T_{dek} and T_{enk}; and transmitter command and acknowledgment delays, T_{tc} and T_{tk}:

  $T_{ta} = T_{rd} + T_{dek} + T_{enk} + T_{tc} + T_{tk} + T_{td}$

  For example, approximations:

  $T_{ta} = 0$ for new, fast equipment, or

  $= 2\ T_w = 261.33...ms$ estimated allowance for old slower equipment

- Wait for calling cycle end time at receiving station, is delineated by receipt of start of message, terminator, or quick-ID section:

  $T_{wce} = 2 \times T_s$ (of own station) as default value

- Wait for reply time at calling station, from end of transmitter signal to start of received reply detection periods (T_{ds}, T_{drw}, and T_{drrw}, below); including propagation, T_p; last word wait, T_{1ww}; late word detection, T_{1d}; turnaround, T_{ta}; redundant word phase delay (if not first transmission in handshake or exchange), T_{rwp};, and receiver and transmitter internal signal delays, T_{rd} and T_{td}; in a single-channel case without tune times, or multi-channel scanning case after first tune and transmission:

  $T_{wr} = T_{td} + T_p + T_{1ww} + T_{1ww} + T_{ta} + T_{rwp}$ (if not first) $+ T_{1d} + T_p + T_{rd}$

For example, approximations:

$T_{wr} = 5\ T_w = 653.33...$ ms for fast equipment, or

$= 7\ T_w = 914.66...$ ms for slower equipment, maximum

$= 8\ T_w = 1045.33..$ms for fast equipment if not first

$=10\ T_w = 1306.66..$ms for slower equipment if not first

- Tune time delay, after issuance of tune-up command and before ready to transmit the reply signal:

T_t = maximum tune-up delay for slowest tuner in system (or net/group being called)

For example, typical allowance ranges are:

$T_t \geq T_w$ = 130.66... ms for fast (solid state) tuners or

$\geq 8\ T_w$ = 1,045.33... ms for fast relay tuners, or

≥ 20 seconds for old electromechanical (servo drive) tuners, or as required by available equipment

NOTE: If tune time(s) of called station(s) is unknown, first try default value shall be 8 T_w and second try default value shall be at least 20 seconds.

- Wait for response and tune time, same as wait for reply T_{wr}, plus tune time T_t in scanning cases, and relevant only to first transmission on a channel (which requires tuning time):

  $T_{wrt} = T_{wr} + T_t$

For example, typical allowance ranges are:

$T_{wrt} = 6\ T_w$ = 784 ms for fast tuners, or

$15\ T_w$ = 1,960 ms for slower tuners, or adjusted as required by available equipment

NOTE: If tune time(s) of called station(s) is unknown, first try default value shall be 15 T_w and second try default value shall be at least 20 seconds.

- Detect signaling tones and timing (of call or reply) detection period; after arrival on channel during normal receive scanning, or after end of wait for reply time T_{wr} or T_{wrt} during normal calling, and before automatic return to normal receive scanning; used to identify channel vacancy or occupancy with standard ALE signaling.

  $T_{ds} \leq T_d(5) = 200$ ms

- Detect redundant words detection period, starting same as T_{ds}, and used to continue beyond T_{ds} if tones and timing are detected, before automatic return to normal receive scanning; used for acceptance of basic single-word (and address first work) addressing and to real calls:

  $T_{drw} = T_{rw}$ + spare $T_{rw} = 6\ T_w$ = 784...ms

- Detect rotating redundant words detection period, starting same time as T_{ds}, and used to continue beyond T_{drw} if redundant words are detected, before automatic return to normal receive scanning; used for acceptance of extended (multiword) addressing and/or group calls:

  $T_{drrw} = 2\ T_{rw}$ + spare $T_{rw} = 9\ T_w$ = 1,176 ms

Sounding

- Single-channel redundant sound time, like leading call T_{1c}, but with only the "TIS" or "TWAS" terminator, using twice the whole address:

  $T_{rs} = 2T_a$ (caller)

For example,

$T_{rs} = 2T_{rw}$ = 784 ms minimum, individual single-word address sound on a single channel

- Scanning sound time. Like T_{sc}, but using whole address only (not just first word of address):

  $T_{ss} = n \times T_a$ (caller) $\geq T_s$

- Scanning redundant sound time, like calling cycle time, T_{cc}, consisting of redundant sound time T_{rs}, with addition of scanning sounding time T_{ss} (which is identical to T_{sc}):

  $T_{srs} = T_{ss} + T_{rs} = (2 + n)T_a$(caller) $\geq T_s + T_{rs}$

For example,

$T_{srs} = (20 + 2) T_{rw}$ = 8,624 ms if C = 10, and $T_d = T_{drw}$

Star calling

- Minimum uniform slot width for automatic slotted responses in normal single-word address star net and group calling protocols (but may be modified by CMD):

T_{sw} ($_{min}$) = 14 T_w = 1,829.33... ms for standard replies, or

= 17 T_w = 2221.33...ms for LQA replies, or

= 9 T_w = 1,176 ms for only fixed “tight slot” replies, or

= n x T_w by CMD

NOTE: Replies above are for first transmissions; if not, $T_{sw\ min}$ = 17, 20, and 12 T_w respectively, (due to redundant word-phase delay).

- Slot wait time before start of slotted response and after detection of end of calling signal, where SN is the assigned (or derived) slot number, for group or preset net calling:

$T_{swt}(SN) = T_{sw}$ x SN for uniform slot widths
(by CMD or net manager), or if non-uniform (customized) slot width

$T_{swt}(SN)$ = SN [5 T_w + 2T_a (caller) + (optional LQA) T_{rw} (optional message) T_m]
+ T_a (caller) + (sum of all previous w_a called addresses):

$$\sum_{m=1}^{m=SN-1} T_a(m)\ (called)$$

as the general case.

For example,

$T_{swt}(5)$ = 14 T_w x 5 = 70 T_w = 9,146.66...ms delay for start of normal 5th slot response, first time, no LQA, single word address.

- Wait for net reply buffer time at calling station, after end of star net or group call, until responses should be received and an acknowledgment can be started, where “NS” is the total number of slots (including slot 0):

T_{wrn} (calling) = T_{sw} x (Ns+1) for uniform slots or generally, T_{swt} (NS+1)

- Wait for net acknowledge buffer time at called stations, to receive acknowledgment after end of star net or group call:

T_{wan}(called) =T_{wrn}(calling) + 2T_{rw}

- Turnaround plus tune time totals for slotted responses have the following limits (not including T_{lww}):

T_{ta} + T_t 1500 ms for standard slots, except

2100 ms for slot 1 only, or

360 ms for slot 0 emergency or interrupt

- Maximum star group wait for acknowledgment time at called stations:

$T_{wan\ max}$ = 107 T_w + 27 T_a (caller) + 13 T_{rw} (optional LQA) +

13 T_m(optional message)

- Default maximum star group wait for acknowledgment time for late arrival, called stations, not knowing the size of the group. There are two default maximum waiting values, before automatically returning to normal receive scanning, if no message and caller uses single-word address:

$T_{wan\ max}$ = 188 T_w = 24,563.33...ms if standard or,

277 T_w = 29,661.33...ms if LQA requested

Programmable timing parameters

Unless otherwise programmed by the network manager, the following typical timing values are recommended:

- Dwell time per channel, basic receive scanning:

  $T_d(5)$ = 200 ms for 5 chps basic scan rate

- Dwell time per channel, minimum receive scanning:

  $T_d(2)$ = 500 ms for 2 chps minimum scan rate

- Dwell time for calculations of T_s (and T_{sc}), based on probable maximum typical pause (may be adjusted by net manager for best system performance):

  $T_d = T_{drw} = 2T_{rw}$ = 784 ms

Wait (listen first) time before tune or transmit:

T_{wt} = 2 seconds for voice or general purpose channels or,

= T_{drw} = 784 ms for ALE and data only channels

Tune time allowance for wait for response time is normally set for slowest known tuner in associated network; except if unknown parameter (such as in blind internet calls to “strangers”):

$T_t = 8T_w$ = 1045.33...ms for first call, and

= 20 seconds for next try

- Automatic periodic sounding intervals (when channels are clear):

  T_{ps} = 45 minutes when enabled (T_{ps} must be capable of being disabled).

Wait for activity time after linking or use, before automatic return to normal receive scanning:

T_{wa} = 30 seconds when enabled (T_{wa} must be capable of being disabled).

ANNEX C. SUMMARY OF ALE SIGNAL PARAMETERS

ALE occupied bandwidth	500-2750 Hz
Quantity of tones	8 (one per symbol period)
Tone frequencies	750; 1000; 1250; 1500; 1750; 2000; 2250; 2500 Hz
Tone values	000 001 011 010 110 111 101 100
Symbol changes	Tone transitions are phase continuous
Symbol structure	3 bits of binary coded data
Symbol rate; period	125 symbols per second (sps); 8 ms
Uncoded data rate	375 bits per second (b/s) transmitted
Forward error correction	Golay (24, 12, 3) half-rate coding (4 modes of (FEC) correct/delect; 3/4, 2/5, 1/6, or 0/7)
Auxiliary coding (DTM,	Redundant x 3, with 2/3 majority vote (with 49 AMD, basic ALE) transmitted bits)
Auxiliary coding (DBM)	Interleaving depth (ID) = 49 to 21805 = (n x 49)
Coded data rate (DTM, AMD, basic ALE)	61.22 b/s
Coded data rate (DBM)	187.5 b/s
Coded data bits per basic ALE word (DTM, AMD)	24 (21 (3 characters) plus 3 preamble), per word
Coded data bits per message (DTM)	From 0 to 7371 bits per block
Coded data bits per message	From 0 to 261644 bits per block, plus 16 bits CRC (DBM)
Throughput, maximum data rate (DTM, AMD, basic ALE)	53.57 b/s data bits
Throughput maximum data rate (DBM)	187.5 b/s data bits

Characters per word (AMD or basic ALE)	0 to 3 expanded 64 or full ASCII
Character per message (DTM)	0 to 1053 ASCII characters per block
Character per message (DBM)	0 to 37377 full ASCII characters per block
Character rate (DTM, AMD, basic ALE)	7.653 cps
Character rate (DBM)	26.79 cps
Equivalent throughput maximum word rate (DTM, AMD)	76.53 words per minute (wpm) (5 character plus space per word)
Equivalent throughput maximum word rate (DBM)	267.9 wpm (5 character + space per word)
Unit period (DTM, AMD, or ALE word)	130.66 ... ms per word (T_{rw}) or 392 ms per triple redundant word (T_{rw})
Message period (DTM)	0 to 2.29 minutes per block
Message period (DBM)	0 to 23.26 minutes per block
Minimum sound time	784 ms (2 T_{rw})
Minimum call time	1176 ms (3 T_{rw})
Minimum handshake time	3528 ms (9 T_{rw}) three-way linking
Preamble (word types)	8 (3 bits)
Character sets or random bits	ASCII (Basic 38, expanded 64, full 128),
Link quality analysis (LQA)	ALE (BER, SINAD, and MP)

APPENDIX B

LINKING PROTECTION

TABLE OF CONTENTS

TABLES

FIGURES

LINKING PROTECTION

B.1 GENERAL.

B.1.1 Scope.
This appendix contains the requirements for the prescribed protocols and directions for the implementation and use of high frequency (HF) automatic link establishment (ALE) radio linking protection.

B.1.2 Applicability.
This appendix is a mandatory part of MIL-STD-188-141 whenever linking protection (LP) is a requirement for the HF radio implementation. The functional capability herein described includes linking protection, linking protection application levels, and timing protocols. The capability for manual operation of the radio in order to conduct communications with existing, older generation, non-automated radios shall not be impaired by implementation of these automated procedures.

B.2 APPLICABLE DOCUMENTS.

B.2.1 General.
The documents listed in this section are specified in B. 3, B. 4, and B. 5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in B. 3, B. 4, and B. 5 of this standard, whether or not they are listed.

B.2.2 Government documents.

B.2.2.1 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 cited in the solicitation or contract.

FEDERAL STANDARDS

FED-STD-1037	Telecommunications: Glossary of Telecommunication Terms

(Copies of these documents are available online at http://quicksearch.dla.mil.)

B.3 DEFINITIONS.

B.3.1 Standard abbreviations and acronyms.
The abbreviations and acronyms used in this document are defined below. Those listed in the current edition of FED-STD-1037 have been included for the convenience of the reader.

2G	second generation
3G	third generation
2G ALE	second generation automatic link establishment
3G ALE	third generation automatic link establishment
AL-0	unprotected application level
AL-1	unclassified application level
AL-2	unclassified enhanced application level
AL-3	unclassified but sensitive application level
AL-4	classified application level
ALE	automatic link establishment
AMD	automatic message display
ASCII	American Standard Code for Information Interchange
BW1	Burst Waveform 1
CMD	ALE preamble word COMMAND
CRC	cyclic redundancy check
DBM	data block message
DO	design objective
DODISS	Department of Defense Index of Specifications and Standards
DTM	data text message
FEC	forward error correction
HF	high frequency
ICD	interface control document
LP	linking protection
LPCM	linking protection control module
ms	millisecond
NSA	National Security Agency
NT	Not Tested
PDU	protocol data unit
PI	protection interval
REP	Repeat preamble in 2G ALE
TOD	time of day

B.3.2 Definitions of timing signals.
The abbreviations and acronyms used for timing symbols are contained in Annex A to Appendix A.

B.4 GENERAL REQUIREMENTS.

B.4.1 LP overview.

The LP procedures specified herein shall be implemented as distinct functional entities for control functions and bit randomization functions. (Unless otherwise indicated, distinct hardware for each function is not required.) Figure B-1 shows a conceptual model of the MIL-STD-188-141 data link layer functions, showing the placement within the data link layer at which LP shall be implemented. The linking protection control module (LPCM) shall perform all control functions specified herein and interface to the ALE controller as shown on figure B-2. Scrambler(s) shall perform all cryptographic operations on ALE words, under the control of the LPCM. Use of LP shall neither increase the time to establish a link compared to the non-protected radio, nor degrade the probability of linking below the standard set for non-protected linking in Appendix A, table A-II. A means shall be provided to disable the LP functions and operate the radio in the clear unprotected application level (AL-0). Hardware scramblers shall be removable without impairment of the unprotected application level functionality of a radio.

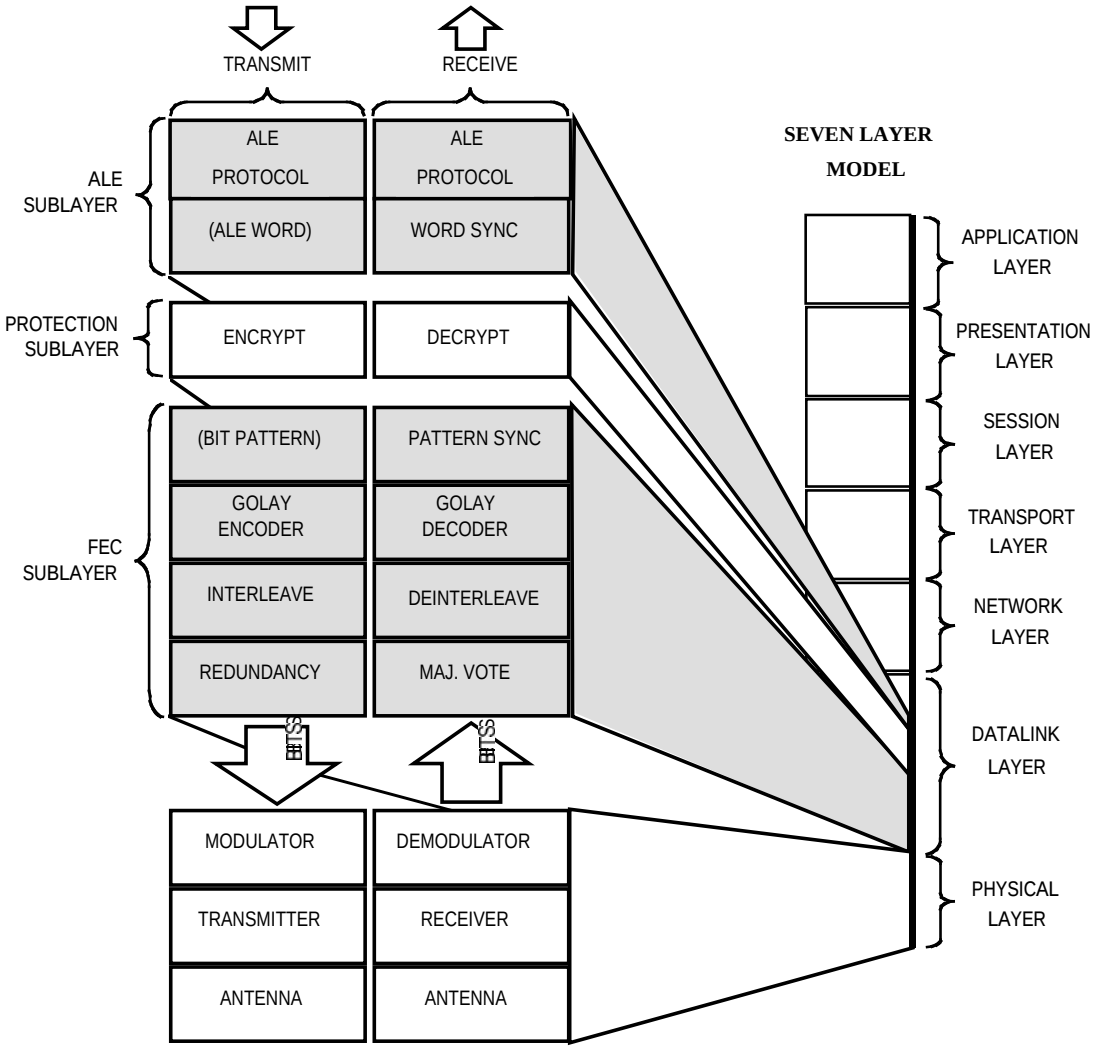


FIGURE B-1. Data link layer with linking protection sublayer.

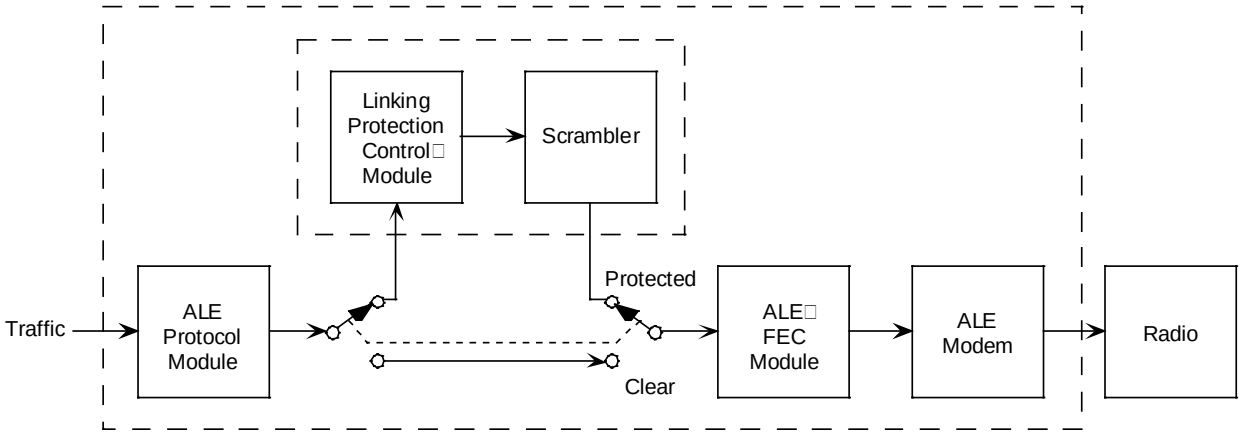


FIGURE B-2. Data flow in a protected radio.

B.4.1.1 Linking protection application levels.
The application levels of LP are defined herein. The classified application level (AL-4), which offers the highest degree of protection, and the unclassified but sensitive application level (AL-3) use National Security Agency (NSA) controlled algorithms described in classified documents. This standard can only make reference to these documents with very little other descriptive material. All protected radios shall be capable of operation at the unclassified application level (AL-1). A means 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 unclassified enhanced application level (AL-2) shall be able to disable the receiver from listening for linking attempts at unprotected application level (AL-0) and AL-1. (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.

B.4.1.1.1 AL-0.
Assignment of the AL-0 indicates that no linking protection is being employed. No protection is provided against interfering, unintentional, or malicious linking attempts. All protected HF radios shall be capable of operation in the AL-0 mode.

B.4.1.1.2 AL-1.
The AL-1 unclassified application level is mandatory for all protected radio systems, and therefore, provides protected interoperability within the U.S. Government. All protected radios shall be capable of operation in the AL-1 mode even if they also provide application levels with greater protection. The AL-1 scrambler shall employ the lattice encryption algorithm as specified in B.5.6, 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-1 protection interval (PI) is 60 seconds, which provides slightly lower protection than any of the other available protected modes but allows for relaxed synchronization requirements.

B.4.1.1.3 AL-2.
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-specific interfaces. This scrambler is for general U.S. Government and commercial use. The AL-2 PI is 2 seconds.

B.4.1.1.4 AL-3.
AL-3 shall use distinct hardware scramblers and shall employ an algorithm and the corresponding interface control document (ICD) developed by the NSA. Systems employing the AL-3 LP shall meet NSA security requirements. The AL-3 PI is a maximum of 2 seconds.

B.4.1.1.5 Classified application level AL-4.
AL-4 shall use distinct hardware scramblers and shall employ an algorithm and the corresponding ICD developed by NSA. An AL-4 scrambler may be used to protect classified orderwire traffic. Systems employing classified application level LP shall meet NSA security requirements. The AL-4 PI is a maximum of 1 second.

B.4.2 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 datalink layer. In particular, this means that achieving and maintaining crypto sync shall occur transparently to the ALE waveform and protocols, and that scanning radios shall be able to acquire cypto 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 shall acquire crypto sync without the use of synchronization preambles or message indicator bits.

B.4.3 Transmit processing.
The LP module in a sending station shall encrypt each 24-bit ALE word to be sent using the seed data then in use (frequency, PI number, word number, etc. See B.5.2.3.) and delivers the encrypted word to the FEC module. (Data Block Mode is a special case. See B. 5. 3. 4.)

B.4.4 Receive Processing.
The receiver side of an LP module is responsible for achieving crypto sync with transmitting stations, and for decrypting protected ALE words produced by 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 three errors, or once every 78 ms when correcting one error per Golay word.)

The receive LP module shall then decipher the candidate word, and pass it to the receiving ALE module, which will determine 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 at the receiver, requiring the receiving LP module to decrypt each candidate word under several seeds.

A further complication is the possibility, though small, 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, are used to decrypt the next word, and each result is evaluated in the context of the corresponding first word. The probability is vanishingly small 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 scanning call or sound, a word following "DATA SNV" must have three ASCII-38 characters and a THRU, REPEAT, TIS or TWAS preamble. All valid preamble sequences may be found in Appendix A (table A-VIII).

B.4.5 Time of day (TOD) synchronization.
Because LP employs PIs (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.

The approach taken here is to rely on operators to get station times synchronized to within 1 minute (plus or minus 30 seconds), and then to employ a protocol to synchronize stations to within 1 or 2 seconds (fine sync) for full linking protection. While it is possible to operate networks with only coarse (1 minute) time synchronization, this reduces the protection offered by this system against playback (tape recorder) attacks.

Synchronization of local times for LP requires some cooperation between the protocol entity and the LP time base. For this reason, the LP module, which already has access to the time base for its normal operations, appears to be the logical entity to execute the synchronization protocols, although these protocols are logically at a higher layer in the protocol stack than the LP procedure. In this case, the LP module would need to examine the contents of received transmissions to extract relevant message sections.

If, instead, the synchronization protocols are executed by the ALE entity, the division of function by level of abstraction is cleaner. One concept of how the coordination across the ALE-LP sublayer boundary may be effected in this case is as follows:

a. TOD is maintained by the ALE entity, and is provided to the LP entity as required.

b. The transmit LP entity uses the TOD provided by the transmit ALE entity to form seeds during T_{sc} and for the initial time setting for T_{lc}. Thereafter, the TOD from ALE is ignored, and the transmit LP entity sequences seeds in accordance with the state diagram in figure B-4.

c. 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}, and so on).

d. For authentication of clear mode time exchanges, the ALE module must be able to call upon the LP module to encrypt and decrypt individual ALE words "off line."

B.5 DETAILED REQUIREMENTS

B.5.1 Linking protection.

The following requirements apply to both second generation automatic link establishment (2G ALE) and third generation automatic link establishment (3G ALE) unless otherwise stated.

B.5.2 LPCM.

The LPCM shall execute the LP procedure specified in B.5.3 and control the attached scrambler(s) as specified below.

B.5.2.1 Scrambler interfaces.

The LPCM shall interact with the scrambler(s) in accordance with the circuits and protocols specified in the interface control document (ICD) for each scrambler (see B.4.1.1.4 and B.4.1.1.5). For AL-1, the ICD is prepared and controlled by the manufacturer.

B.5.2.2 TOD.

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.

B.5.2.2.1 TOD entry.

A means shall be provided for entry of TOD (date and time) via either an operator interface or an electronic fill port or time receiving port (DO: provide both operator interface and electronic port). This interface should also provide for the entry of the 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. Default time uncertainty shall be determined by the procuring agency or manufacturer. Default uncertainty of ± 15 seconds is suggested.

B.5.2.2.2 Time exchange protocols.

After initialization of TOD, the LPCM shall execute the time protocols of B.5.5 as required, to maintain total time uncertainty less than the PI length of the most secure LP mode it is using. The LPCM shall respond to time requests in accordance with B.5.5.3 unless this function is disabled by the operator.

B.5.2.3 Seed format.

The LPCM shall maintain randomization information for use by the scrambler(s), and shall provide this information, or "seed," to each scrambler in accordance with the applicable ICD. The 64-bit seed shall contain the frequency, the current PI number, the date, and a word number

in the format shown on figure B-3, where 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. The date field shall be formatted in accordance with figure B-3. 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. The PI field shall be formatted in accordance with figure B-3. The coarse time field shall contain an 11-bit integer which counts minutes since midnight (except that temporary discrepancies may occur as discussed in B.5.3). The 6-bit fine time field shall be set to all 1s when time is not known more accurately than within 1 minute (i.e., time quality of six or seven). When a time synchronization protocol (see B.5.5) 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 B.5.3. The fine time field shall always 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). The word field shall be used to count words within a PI, as specified in B.5.3. The frequency field shall be formatted in accordance with figure B-3. Each 4-bit field shall contain one binary-coded decimal digit of the frequency of the current protected transmission. Regardless of time quality, the fine time field shall be set all 1s for the unclassified application level of LP.

B.5.3 Procedure for 2G ALE.

The procedure to be employed in protecting transmissions consisting entirely of 24-bit ALE words is presented in B.5.3.1 and B.5.3.2. When a radio is neither transmitting nor receiving, the PI number shall be incremented as follows. When using linking protection level AL-2 and local time quality (see Appendix A, A.5.6.4.6) is “5” or better, the fine time field shall be incremented at the end of each PI by the length of the PI, modulo 60. When the fine time field rolls over to “0,” the coarse time field shall be incremented, modulo 1440. At midnight, the coarse and fine time fields shall be set to “0,” and the date and month fields updated. When using linking protection level AL-1, or when the local time quality (see appendix A, A.5.6.4.6) is “6” or “7,” the fine time field shall contain all “1s,” and the coarse time field shall be incremented once per minute, modulo 1440. At midnight, the coarse time field shall be set to “0”, and the date and month fields updated. Whenever the local time uncertainty is greater than the PI, the system shall:

a. Present an alarm to the operator.

b. Optionally, also attempt resynchronization (if enabled). The first attempt at resynchronization shall use the current fine seed. If this fails, the system shall use a coarse seed for subsequent attempts.

Example Seed

Date=8 May Time=15:57:34 Word=0 Frequency=1755 kHz

a.

9	17	8	2	28
Date	PI	Word	0 0	Frequency
0101 01000	01110111101 100010	000000 00	0 0	0000 0000 0001 0111 0101 01010000
1 9	10 26	27 34		37 64

TOD

b.

4	5
Month	Day
0101	01000
1 4	5 9

c.

11	6
Coarse Time	Fine Time
01110111101	100010
10 20	21 26

d.

4	4	4	4	4	4	4
100 MHz	10 MHz	1 MHz	100 kHz	10 kHz	1 kHz	100 Hz
0000	0000	0001	0111	0101	0101	0000
37 40	41 44	45 48	49 52	53 56	57 60	61 64

FIGURE B-3. Seed formats.

B.5.3.1. Transmitting station.
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 discrepancy shall be allowed to persist until the conclusion of each transmission, whereupon the TOD fields of the seed shall be corrected. The word number field "w" shall be as follows:

a. During the scanning call phase (T_{sc}) of a call, or throughout a sound, the calling stations shall alternate transmission of words encrypted using w = 0 and w = 1. The first word of T_{sc} shall begin with w = 0 or w = 1, as required, such that the last word of T_{sc} is encrypted using w = 1. The TOD used during T_{sc} shall change as required to keep pace with real time, except that TOD shall only change when w = 0. Words encrypted with w = 1 shall use the same TOD as the preceding word.

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

c. All succeeding words of the call shall use succeeding word numbers up to and including $w = w_{max}$. For the word following a word encrypted with $w = w_{max}$, the TOD shall be incremented and w shall be reset to 0.

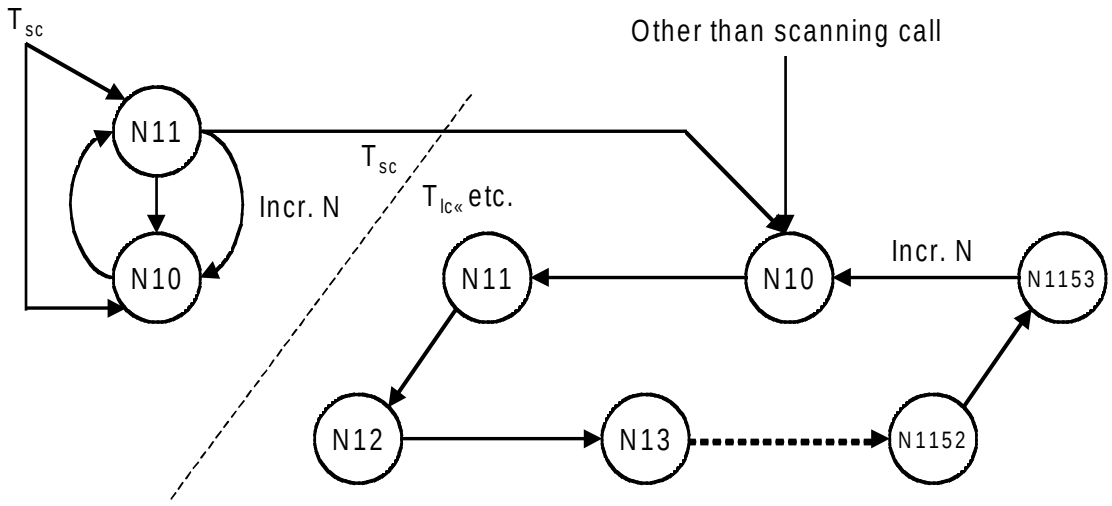
(1) $W_{max} = 2$ for a 1-second PI.

(2) $W_{max} = 5$ for a 2-second PI.

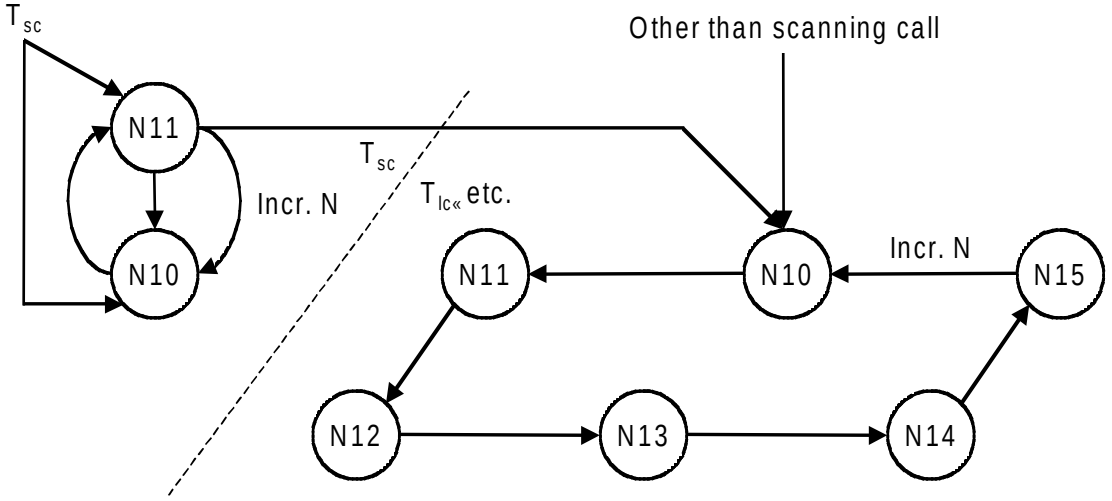
(3) $W_{max} = 153$ for a 60-second PI.

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

Figure B-4 illustrates the permissible TOD with combinations for a transmitting station using a 60 second (w_{max}=153) and a 2-second PI (w_{max} = 5), and the permissible sequences of these combinations. Sounds are protected in the same fashion with T_{rs} in place of T_{lc}.

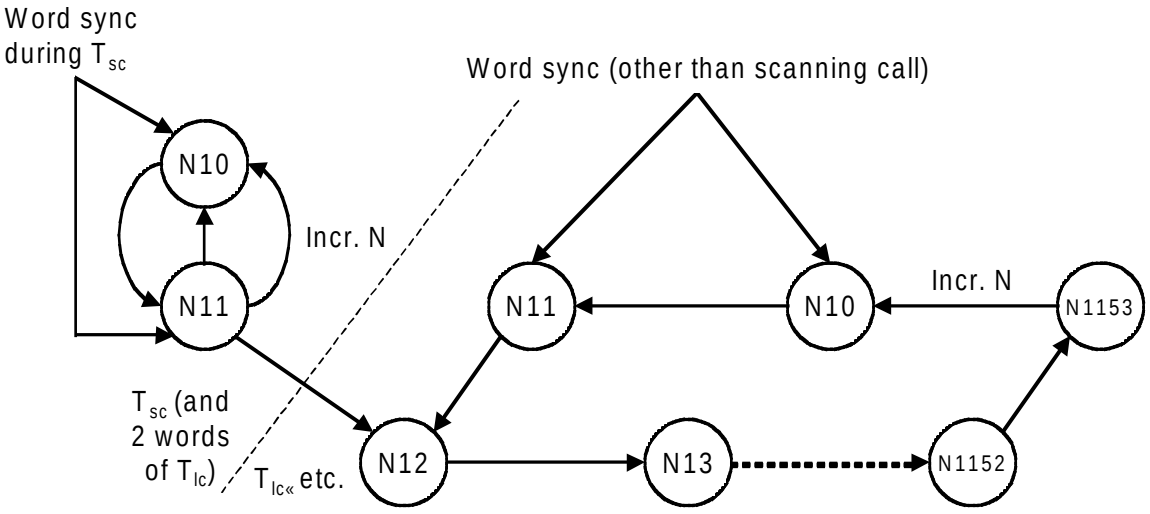


a. Transmitting station state diagram (60 second PI)

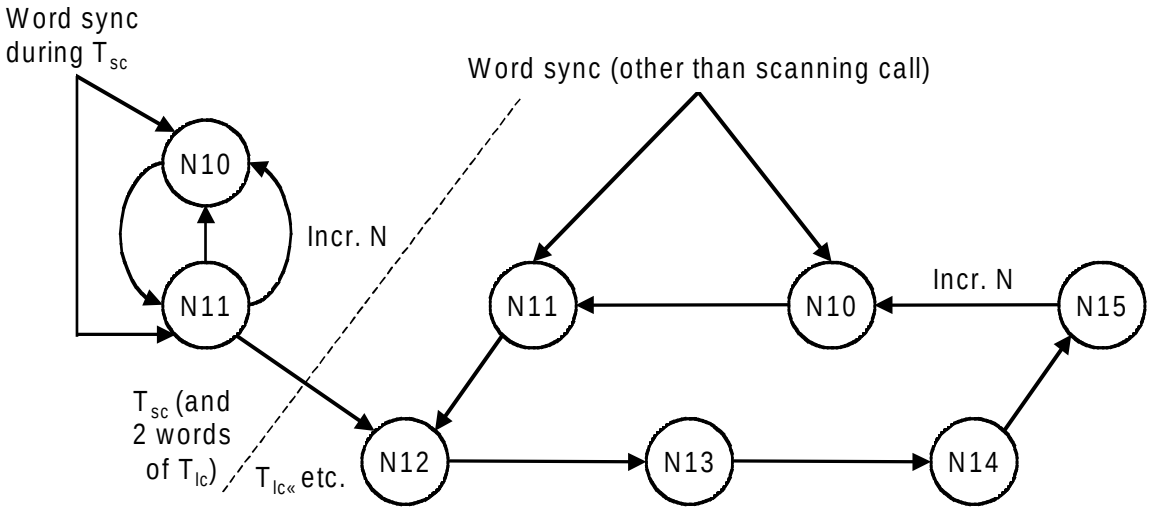


b. Transmitting station state diagram (2 second PI)

FIGURE B-4. Transmitting and receiving stations state diagram.



c. Receiving station state diagram (60 second PI)



d. Receiving station state diagram (2 second PI)

FIGURE B-4. Transmitting and receiving stations state diagram (continued).

B.5.3.2 Receiving station.
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 B.5.5.2.2) shall also attempt to decode received words using coarse TOD (fine time = all 1s, 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 linking protection

protocol. Figure B-4 illustrates the permissible TOD/w sequences for a receiving station using a 60-second PI and a 2-second PI respectively, 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 N/1, a received word may yield valid preambles and ASCII when decrypted using all of the valid combinations: N/0, (N + 1)/0, and N/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 under the valid successor states to these three states. Stations using a PI of 2 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 = N, no TOD before N+1 is valid for the acknowledgment.

B.5.3.3 Message sections.
All ALE words shall be protected including message text.

B.5.3.4 Data block message (DBM) mode.

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 three 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.

B.5.4 Procedure for 3G ALE.
See STANAG 4538.

B.5.5 Time protocols.
The following shall be employed to synchronize LP time bases. The time service protocols for active time acquisition, both protected (B.5.5.2) and non-protected (B.5.5.3), are mandatory for implementations of LP providing AL-2 or higher.

B.5.5.1 Time exchange word format.
See Appendix A, A.5.6.4.3.

B.5.5.2 Active time acquisition (protected).
A station that knows the correct date and time to within 1 minute may attempt to actively acquire time from any station with which it can communicate in protected mode by employing the protocol 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 1 minute may nevertheless employ this protected protocol by repeatedly guessing the time until it successfully communicates with a time server.

B.5.5.2.1 Time Request call (protected).
A station requiring fine time shall request the current value of the network time by transmitting a Time Request call, formatted as follows. (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. Thus, multiple servers may need to be tried before sufficient time quality is achieved.)

TO <time server> CMD Time Is <time> DATA <coarse time>
REP <authenticator> TIS <requester>.

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 Appendix A, A.5.6.4.4. The Time Request call transmission shall be protected using the procedure specified in B.5.3.1 and B.5.3.2. When acquiring time synchronization, the coarse seed (fine time field in the seed set to all 1s) 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.

B.5.5.2.2 Time Service response (protected).
A station which 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> TWAS <time server>.

The Time Is command shall be immediately followed by a coarse time word and an authentication word. The authenticator shall be generated by the three-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 requester, as specified in Appendix A, A.5.6.4.5. The entire Time Service response shall be protected as specified in B.5.3.1 and B.5.3.2 using the time server's current coarse seed if the request used a coarse seed, or the current fine seed otherwise. The seed used in protecting a Time Service response may differ from that used in the request that caused the response. A time server shall respond only 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 time request may be disabled by the operator. Stations prepared to accept coarse Time Request commands shall decrypt the initial words of incoming calls under eight (vs. 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 vs. three fine TODs.)

B.5.5.2.3 Time Server request (protected).
A time server may request authenticated time from the original requestor by returning a Time Server request, which is identical to the Time Service response as given above except that the TWAS termination is replaced by TIS. The original requester shall then respond with a Time Service response, as above, with an authenticator generated by the three-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 Appendix A, A.5.6.4.5.

B.5.5.2.4 Authentication and adjustment (protected).
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 1 minute later. If the request used a fine seed, the waiting station shall try the usual six seeds: w = 0 and w = 1, and those corresponding to 1 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. 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 in accordance with Appendix A, A.5.6.4.6.

B.5.5.3 Active time acquisition (non-protected).
A station that does not know the correct date and time to within 1 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 decryption.

B.5.5.3.1 Time Request call (non-protected).
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 #> TIS <requestor>.

The Time Request command shall be immediately followed by a coarse time word, followed by an authentication word containing a 21-bit number, generated by the requesting station 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 is retained while the radio is powered off) may meet this requirement.

B.5.5.3.2 Time Service response (non-protected).
A station that receives and accepts 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> TWAS <time server>.

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 three-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 Appendix A, A.5.6.4.5. The encryption shall employ the AL-1 and AL-2 algorithm and a seed containing the time sent and w = all 1s. The least-significant 21 bits of this encryption shall be used as the authenticator. A time server shall respond only to 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.

B.5.5.3.3 Authentication and adjustment (non-protected mode).
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. Then exclusive-or the result with the entire random number word it sent in its Time Request call, and encrypt this result using w = all 1s 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 in accordance with Appendix A, A.5.6.4.6.

B.5.5.4 Passive time acquisition (optional).
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:

a. 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.

b. Local time quality 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.

A passive time acquisition mechanism may also be used to maintain network synchronization once achieved. Passive time acquisition is optional, and if provided, the operator shall be able to disable it.

B.5.5.5 Time broadcast.
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> TWAS <time server>.

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 Appendix A, A.5.6.4.4. If the broadcast is made without LP (i.e., in the clear), the authenticator must be encrypted as described in Appendix A, A.5.6.4.5 to provide any authentication. The use of an authenticator that does not depend on 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 the broadcasts contain are consistent with the local time and uncertainty before such received time is at all useful.

B.5.5.6 Advanced time distribution protocols.
Advanced time exchange protocols for application levels 3 and 4 will be addressed as required with future upgrades of MIL-STD-188-141.

B.5.6 The Lattice Algorithm.
The Lattice Algorithm is designed specifically for the encryption of 24-bit ALE words. It uses a 56-bit key (7 bytes), and the 8-byte seed described in B.5.2.3, Seed format.

NOTE: The author makes no claim of proprietary rights in this algorithm. All are free to implement it without royalty.

B.5.6.1 Encryption using the Lattice Algorithm.
A schematic representation of the algorithm is shown in figure B-5. The algorithm operates on each of the 3 bytes of the 24-bit word individually. At each step, here termed one “round” of processing, each byte is exclusive-ored with one or both of the other data bytes, a byte of key, and a byte of seed, and the result is then translated using the 256x8 bit substitution table ("S-box") listed in table B-I. Eight rounds shall be performed. Mathematically, the encryption algorithm works as follows:

1. Let f(•) be an invertible function mapping {0..255} -> {0..255}.

2. Let V be a vector of key variable bytes and S be a vector of TOD/frequency "seed" bytes. Starting with the first byte in each of V and S, perform eight "rounds" of the sequence in 4 below, using the next byte from V and S (modulo their lengths) each time a reference to V[ ] and S[ ] is made.
3. Let A be the most significant of the three-byte input to each round of encryption, B be the middle byte, and C be the least significant byte, and A', B', and C' be the corresponding output bytes of each round.
4. Then for each round,
   A' = f(A + B + V[ ] + S[ ])
   C' = f(C + B + V[ ] + S[ ])
   B' = f(A' + B + C' + V[ ] + S[ ])

The 24-bit output of the encryption algorithm consists of, in order of decreasing significance, the bytes A', B', and C' resulting from the eighth round of encryption.

B.5.6.2 Decryption using the Lattice Algorithm.
The decryption algorithm simply inverts the encryption algorithm. Note that the starting point in the V and S vectors must be pre-computed, and that the V and S bytes are used in reverse order.

1. Let g(•) be the inverse of the f(•) used for encryption (see table B-II).
2. Starting with the last elements of the V and S vectors used in encryption, perform eight rounds of the following decryption steps, working backward through the V and S vectors.
3. Let A' be the most significant of the 3-byte input to each round of decryption, B' be the middle byte, and C' be the least significant byte, and A, B, and C be the corresponding output bytes of each round.
4. B = g(B') + A' + C' + V[ ] + S[ ]
   C = g(C') + B + V[ ] + S[ ]
   A = g(A') + B + V[ ] + S[ ]

The 24-bit output of the decryption algorithm consists of, in order of decreasing significance, the bytes A, B, and C resulting from the eighth round of decryption.

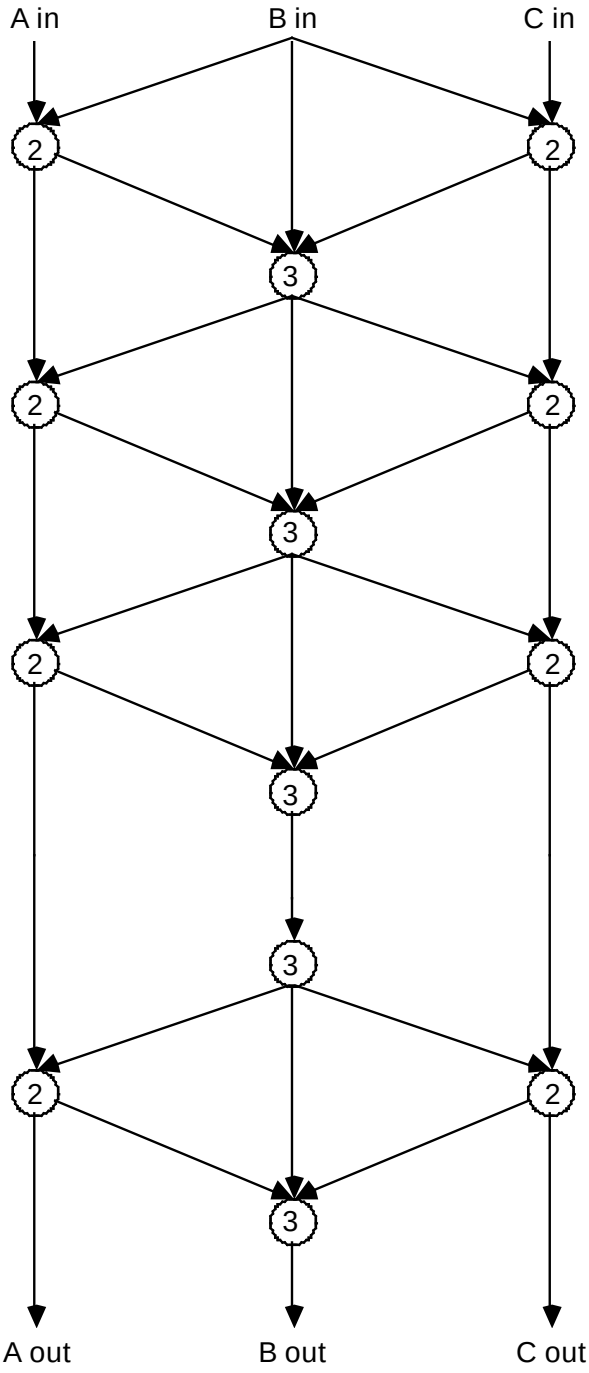


FIGURE B-5. Lattice Algorithm schematic diagram (encryption).

B.5.6.3 Encryption and decryption tables.
The 256 -> 256 mapping tables B-I and B-II for use in linking protection are given below. To use these tables, use the most significant 4 bits of the input byte to select a row in the table, and the least significant 4 bits to select a column. The output byte is contained at the selected location.

TABLE B-I. Encryption table.

9c	f2	14	c1	8e	cb	b2	65	97	7a	60	17	92	F9	78	41
07	4c	67	6d	66	4a	30	7d	53	9d	b5	bc	c3	ca	f1	04
03	ec	d0	38	B0	ed	ad	c4	dd	56	42	bd	a0	de	1b	81
55	44	5a	e4	50	DC	43	63	09	5c	74	cf	0e	ab	1d	3d
6b	02	5d	28	e7	c6	ee	b4	d9	7c	19	3e	5e	6c	d6	6e
2a	13	a5	08	b9	2d	BB	a2	d4	96	39	e0	ba	d7	82	33
0d	5f	26	16	fe	22	af	00	11	c8	9e	88	8b	a1	7b	87
27	E6	c7	94	d1	5b	9b	f0	9f	db	e1	8d	d2	1f	6a	90
f4	18	91	59	01	b1	FC	34	3c	37	47	29	e2	64	69	24
0a	2f	73	71	a9	84	8c	a8	a3	3b	E3	E9	58	80	a7	D3
b7	c2	1c	95	1e	4d	4f	4E	fb	76	fd	99	c5	C9	e8	2e
8a	df	f5	49	f3	6f	8f	e5	EB	F6	25	d5	31	c0	57	72
aa	46	68	0b	93	89	83	70	ef	a4	85	f8	0f	b3	AC	10
62	cc	61	40	f7	fa	52	7f	ff	32	45	20	79	ce	ea	be
cd	15	21	23	D8	b6	0c	3f	54	1A	bf	98	48	3a	75	77
2b	ae	36	da	7e	86	35	51	05	12	b8	a6	9a	2C	06	4b

TABLE B-II. Decryption table

67	84	41	20	1f	f8	fe	10	53	38	90	c3	e6	60	3c	cc
cf	68	f9	51	02	e1	63	0b	81	4a	E9	2e	a2	3e	a4	7d
db	e2	65	E3	8f	ba	62	70	43	8b	50	f0	Fd	55	af	91
16	bc	D9	5f	87	F6	F2	89	23	5a	ed	99	88	3f	4b	e7
d3	0f	2a	36	31	da	c1	8a	ec	b3	15	ff	11	a5	A7	a6
34	f7	d6	18	e8	30	29	BE	9c	83	32	75	39	42	4c	61
0a	d2	d0	37	8d	07	14	12	c2	8e	7e	40	4d	13	4f	b5
c7	93	bf	92	3a	EE	a9	ef	0e	dc	09	6e	49	17	f4	d7
9d	2f	5e	c6	95	ca	F5	6f	6b	c5	b0	6c	96	7b	04	b6
7F	82	0c	c4	73	a3	59	08	EB	ab	fc	76	00	19	6a	78
2c	6d	57	98	c9	52	fb	9e	97	94	c0	3d	CE	26	f1	66
24	85	06	cd	47	1a	e5	a0	fa	54	5c	56	1b	2b	df	ea
bd	03	a1	1c	27	ac	45	72	69	AD	1d	05	d1	e0	dd	3b
22	74	7c	9F	58	bb	4e	5d	E4	48	f3	79	35	28	2d	b1
5b	7a	8c	9A	33	b7	71	44	ae	9B	de	B8	21	25	46	c8
77	1e	01	b4	80	b2	B9	d4	cb	0D	d5	a8	86	aa	64	d8

B.5.6.4 Lattice Algorithm examples.

Key variable = c2284a1ce7be2f

seed = 543bd88000017550 (**w**=0)
Encrypt 54e0cd (<TO> SAM)

Step	A	B	C
0	54	E0	CD
1	D0	72	1D
2	1D	48	3C
3	41	DB	0C
4	98	7C	6D
5	39	10	3D
6	13	AA	E4
7	FC	82	27
8	C0	D7	05

Result: C0D705

seed = 543bd88040017550 (**w**=1)
Encrypt 54E0CD (<TO> SAM)

Step	A	B	C
0	54	E0	CD
1	D0	72	1D
2	1D	3D	EF
3	E1	F8	6B
4	11	A0	A2
5	6E	32	A0
6	B0	B4	E2
7	CF	CB	11
8	70	84	34

Result: 708434

seed = 543bd88080017550 (**w**=2)
Encrypt b2a7c5 (<TIS> JOE)

Step	A	B	C
0	B2	A7	C5
1	59	47	E6
2	91	BF	83
3	D1	B8	E8
4	53	ED	A9
5	F4	55	9E
6	32	25	FA
7	DD	5D	15
8	28	ED	4A

Result: 28ED4A

```
Decrypt  C0D705

      Step    A     B     C
        0    C0    D7    05
        1    FC    82    27
        2    13    AA    E4
        3    39    10    3D
        4    98    7C    6D
        5    41    DB    0C
        6    1D    48    3C
        7    D0    72    1D
        8    54    E0    CD

Result:  54E0CD

Decrypt  708434

      Step    A     B     C
        0    70    84    34
        1    CF    CB    11
        2    B0    B4    E2
        3    6E    32    A0
        4    11    A0    A2
        5    E1    F8    6B
        6    1D    3D    EF
        7    D0    72    1D
        8    54    E0    CD

Result:  54E0CD

Decrypt  28ED4A

      Step    A     B     C
        0    28    ED    4A
        1    DD    5D    15
        2    32    25    FA
        3    F4    55    9E
        4    53    ED    A9
        5    D1    B8    E8
        6    91    BF    83
        7    59    47    E6
        8    B2    A7    C5

Result:  B2A7C5
```

APPENDIX C

THIRD-GENERATION HF LINK AUTOMATION

CONTENTS

FIGURES

C.1 GENERAL

C.1.1 Scope.

This appendix contains the requirements for third generation (3G) high frequency (HF) radio technology including advanced automatic link establishment (ALE), automatic link maintenance, and high-performance data link protocols. The inter-relationship of the technology specified in this appendix to other HF automation standards is shown in figure C-1.

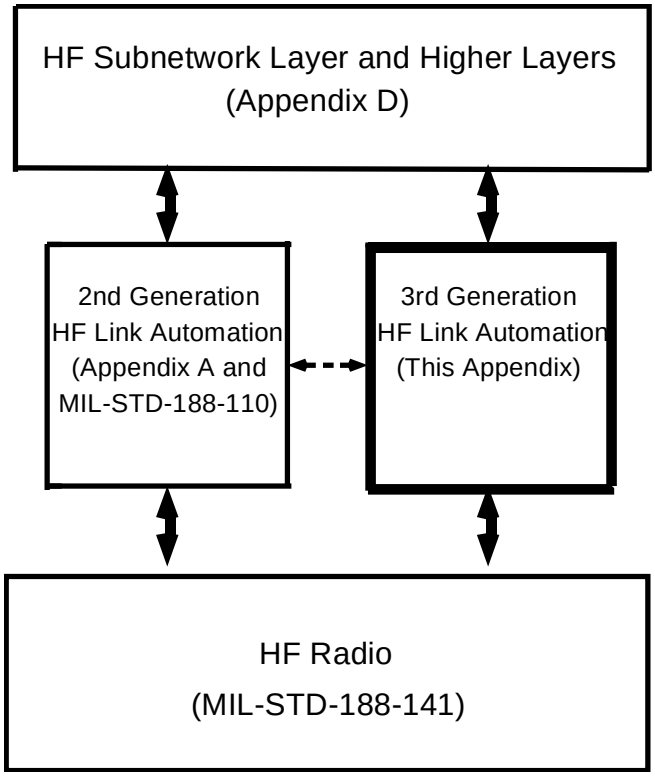


FIGURE C-1. Scope of 3G technology.

C.1.2 Applicability.

3G technology provides advanced technical capabilities for automated HF radio systems. This advanced technology improves on the performance of similar techniques described elsewhere in this standard. Thus, 3G technology may not be required by some users of HF radio systems. However, if the user has a requirement for the features and functions described herein, they shall be implemented in accordance with the technical parameters specified in this appendix.

C.2 APPLICABLE DOCUMENTS

C.2.1 General.

The documents listed in this section are specified in C.4 and C.5 of this appendix. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in C.4 and C.5 of this appendix, whether or not they are listed here.

C.2.2 Government documents.

C.2.2.1 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 cited in the solicitation or contract.

INTERNATIONAL STANDARDIZATION DOCUMENTS

STANAG 4538	Technical Standards For An Automatic Radio Control System For HF Communication Links

(Copies of these documents are available online at http://quicksearch.dla.mil.)

C.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.

C.3 DEFINITIONS

None.

C.4 GENERAL REQUIREMENTS

The third-generation automatic link establishment (3G-ALE) protocol, the Traffic Management (TM) protocol, the High-Throughput Data Link (HDL) and Low-Latency Data Link (LDL) protocols, and the Circuit Link Control (CLC) protocol form a mutually-dependent protocol suite (see Figure C-2). Compliance with this appendix requires compliant implementations of all of the protocols shown in shaded box in Figure C-2, as specified in STANAG 4538.

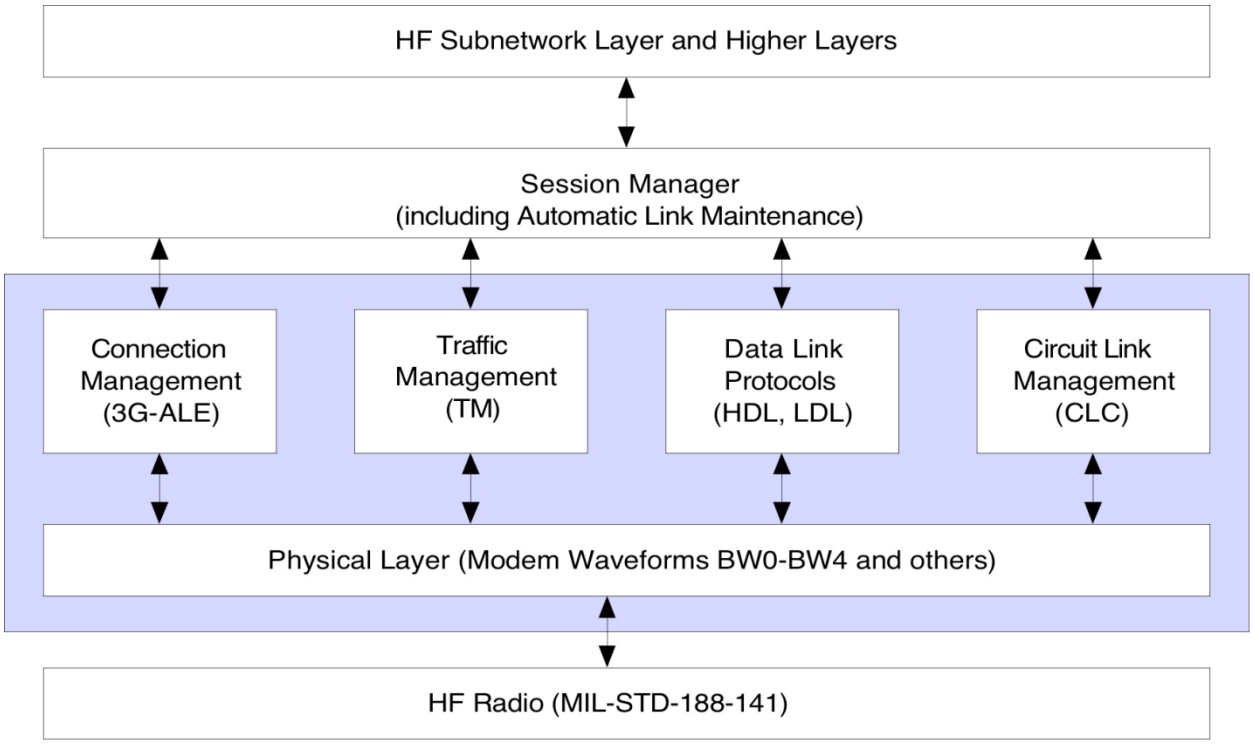


FIGURE C-2. 3G HF protocol suite.

C.5 DETAILED REQUIREMENTS

C.5.1 Choice of 3G-ALE Protocol.

Third-generation ALE is termed Link Set-Up (LSU) in STANAG 4538. Two non-interoperable protocols for link establishment are specified in STANAG 4538: "Fast" LSU (FLSU) and "Robust" LSU (RLSU). RLSU is intended for large networks and heavy traffic, while FLSU is intended for smaller, lightly-loaded tactical networks.

- Because 3G technology is most frequently deployed in tactical applications, all systems shall implement FLSU and its integrated traffic management protocol IAW STANAG 4538.
- RLSU is optional.

C.6 NOTES

The specifications previously contained in this appendix have been replaced with reference to the essentially identical NATO STANAG 4538.

APPENDIX D

HF RADIO NETWORKING

CONTENTS

HF RADIO NETWORKING

D.1 GENERAL.

D.1.1 Scope.
This appendix contains recommendations for the implementation of adaptive networking functions for high frequency (HF) radio

D.1.2 Applicability.
This appendix is for information only.

D.2 APPLICABLE DOCUMENTS.

D.2.1 General.
The documents listed in this section are specified in D. 3, D. 4, and D. 5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in D. 3, D. 4, and D. 5 of this standard, whether or not they are listed.

D.2.2 Non-Government publications.
The following documents form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

INTERNET ENGINEERING TASK FORCE DOCUMENTS

RFC-3626	Optimized Link State Routing Protocol (OLSR)

(Copies of this document obtained from http://www.ietf.org.)

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

IEEE CONFERENCE PAPERS

“Routing in HF Ad-Hoc WANs”	Proceedings, MILCOM 2004
“Performance of Routing Protocols in HF Wireless Networks”	Proceedings, MILCOM 2005

(Copies of these publications may be obtained from http://www.ieee.org.)

D.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.

D.3 DEFINITIONS
None.

D.2 GENERAL OBSERVATIONS

Networked operation supports indirect routing to deliver traffic when propagation does not support direct links between nodes that need to communicate. High Frequency (HF) radio networks are often fully connected (requiring no relaying), especially in surface-wave applications. However, environmental effects can produce intermittent or extended link outages and even network partitions. Thus an indirect routing capability is sometimes required to ensure connectivity within HF networks. In many cases, full connectivity may be provided by a simple single-relay mechanism rather than the more complex routing protocols used in the Internet.

The goal for HF networking is to provide indirect routing transparently (i.e., without requiring operator intervention to switch from direct to indirect routing) while minimizing any on-air overhead transmissions required to support networking.

D.3 DETAILED RECOMMENDATIONS

The Wireless Address Resolution and Routing Protocol (WARRP) is defined in "Routing in HF Ad-Hoc WANs," *Proceedings of the 2004 IEEE Military Communications Conference, MILCOM 2004*. WARRP is an integrated address resolution and routing functionality originally developed for mobile HF WANs (interconnecting IP-based sub-networks). WARRP is an on-demand routing scheme that extends the Internet Address Resolution Protocol (ARP) to provide additional routing capabilities, tailored to the needs of an ad-hoc HF network.

The Optimized Link State Routing (OLSR) protocol (RFC-3626) is an optimization of the classical link state routing algorithm, designed to suit mobile ad-hoc networks. OLSR is generally appropriate for large and dense wireless networks, where it outperforms traditional link-state routing schemes due to its novel mechanisms for reducing routing overhead transmissions.

In a comparison of WARRP and OLSR published in "Performance of Routing Protocols in HF Wireless Networks," *Proceedings of the 2005 IEEE Military Communications Conference, MILCOM 2005*, WARRP was found to require fewer overhead transmissions on the HF channels, but OLSR is more scalable and is a more mature product. Therefore, OLSR is recommended for HF networking except when its extra burden would be prohibitive.

D.4 NOTES

The specifications previously contained in this appendix have been removed due to obsolescence and absence of use in fielded systems.

APPENDIX E

APPLICATION PROTOCOLS FOR HF RADIO NETWORKS

TABLE OF CONTENTS

FIGURES

APPLICATION PROTOCOLS FOR HF RADIO NETWORKS

E.1 GENERAL

E.1.1 Scope.

This appendix contains recommendations for the implementation and use of communications applications such as file transfer and electronic mail in HF radio networks.

E.1.2 Applicability.

This appendix is for information only

E.2 APPLICABLE DOCUMENTS

E.2.1 General.

The documents listed in this section are specified in sections E.3, E.4, and E.5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in sections E.3, E.4, and E.5 of this standard, whether or not they are listed.

E.2.2 Government documents.

E.2.2.1 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 cited in the solicitation or contract.

INTERNATIONAL STANDARDIZATION AGREEMENTS

STANAG 5066	Profile for High Frequency (HF) Radio Data Communications

FEDERAL STANDARDS

FED-STD-1037	Telecommunications: Glossary of Telecommunications Terms

(Copies of these documents are available online at http://quicksearch.dla.mil.)

E.2.3 Non-Government publications.

The following documents form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those cited in the solicitation or contract.

INTERNET ENGINEERING TASK FORCE DOCUMENTS

RFC-2060	Internet Message Access Protocol - Version 4
RFC-2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC-2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
RFC-2047	Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text
RFC-2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC-2616	Hypertext Transfer Protocol - HTTP/1.1
RFC-4251	SSH Protocol Architecture
RFC-4301	Security Architecture for Internet Protocol
RFC-4346	The TLS Protocol Version 1.1
STD 8	Telnet Protocol specification
STD 9	File Transfer Protocol
STD 10	Simple Mail Transfer Protocol
STD 53	Post Office Protocol - Version 3
STD 60	SMTP Service Extension for Command Pipelining

(Internet documents may be obtained from http://www.ietf.org or http://www.rfc-editor.org/rfcsearch.html . The current Request For Comments for each Internet standard (STD) listed above may also be found at the IETF web site. Note that RFCs are often updated, and the latest updates should be applied when appropriate.)

E.2.4 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.

E.3 DEFINITIONS.

E.3.1 Standard definitions and acronyms.
None.

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

ALE	automatic link establishment
ALM	automatic link maintenance
ARQ	automatic repeat request
CFTP	compressed file transfer protocol
COMSEC	communications security
e-mail	electronic mail
FTP	file transfer protocol
HF	high frequency
HMTP	HF mail transfer protocol
HTTP	hypertext transfer protocol
IMAP4	internet mail access protocol – version 4
IP	internet protocol
Ipsec	IP security
LAN	local area network
MTA	mail transfer agent
PDU	protocol data unit
POP3	post office protocol – version 3
SAP	service access point
SMTP	simple mail transfer protocol
SSL	secure sockets layer
TCP	transmission control protocol
TLS	transport layer security
UDP	user datagram protocol
WAN	wide area network

E.4 GENERAL RECOMMENDATIONS

E.4.1 Introduction.

Data applications such as electronic mail (e-mail), file transfer, remote login, and limited web browsing can employ HF links either for communication among hosts directly connected to HF stations, or for wireless access to other data networks.

E.4.1.1 HF subnetwork service.

Interoperation among applications in use at different stations requires that the applications *and all supporting protocols* at the stations interoperate. Performance will then be determined by how well the protocol stacks work with each other and with the HF medium. Systems that implement any application from this appendix should implement the HF subnetwork service described in E.4.1.1.1 and E.4.1.1.2 to convey the corresponding application protocol data units (PDUs) over the HF medium.

E.4.1.1.1 HF subnetwork protocols.

To simplify the task of ensuring interoperability among applications using the HF medium, a small number of lower-layer protocols is recommended for use with the application protocols specified in this appendix:

- HF radio in accordance with MIL-STD-188-141.
- EITHER

  the second-generation (2G) HF data link suite: Automatic Link Establishment (ALE) in accordance with Appendix A and the Automatic Repeat Request (ARQ) data traffic protocol in accordance with STANAG 5066,
  — OR —
  the third-generation (3G) HF data link suite: ALE, ARQ, and Automatic Link Maintenance (ALM) in accordance with Appendix C.

E.4.1.1.2 HF subnetwork interface.

Application clients of the HF subnetwork should interact with the HF subnetwork using the Service Data Units (SDUs) specified in STANAG 5066 Annex A: Subnetwork Interface Sublayer. As a design objective, an Ethernet interface should be provided for exchange of SDUs with clients external to the subnetwork interface device.

Subnetwork interface PDUs (S_PDUs) should be conveyed over the air by the subnetwork protocols specified in E.4.1.1.1.

E.4.1.1.3 Indirect routing support.

The optional indirect routing capability described in Appendix D can improve connectivity within a network by routing traffic through relay stations. However, the overhead traffic required to manage and support indirect routing can be substantial. Use of the Appendix D protocols should be restricted to those cases when indirect routing is required for acceptable network performance.

E.4.1.2 Support for HF-native applications.

In many cases, an application requires communication solely between host computers that communicate using only local connections and HF links. In such cases, an application protocol that

is optimized for the characteristics of HF networks may be used to improve performance over protocols not designed for HF networks. The protocol stack in Figure E-1 illustrates the relationship of such HF-native application-layer protocols to the protocols defined elsewhere in this standard.

NOTE: Encryption of traffic for Communications Security (COMSEC) is not shown in Figures E-1 through E-3. Security is discussed in E.4.1.4.

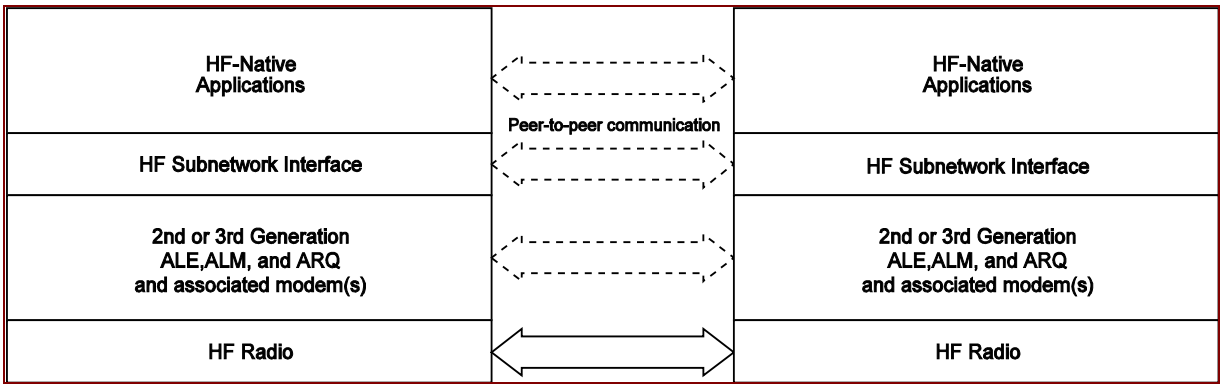


FIGURE E-1. HF-native application interoperation.

E.4.1.3 Support for Internet applications.
For access via HF radio to distant local area networks (LANs) or wide-area networks (WANs) such as the Internet, the application protocols already in use within those networks must either be used within the HF network as well, or terminated at HF gateways that employ alternate HF-oriented protocols over the HF medium.

E.4.1.3.1 Gateway support for Internet applications.

An application-layer gateway at the boundary between an HF network and non-HF networks allows the use of dissimilar protocols at every layer within each subnetwork (Figure E-2).

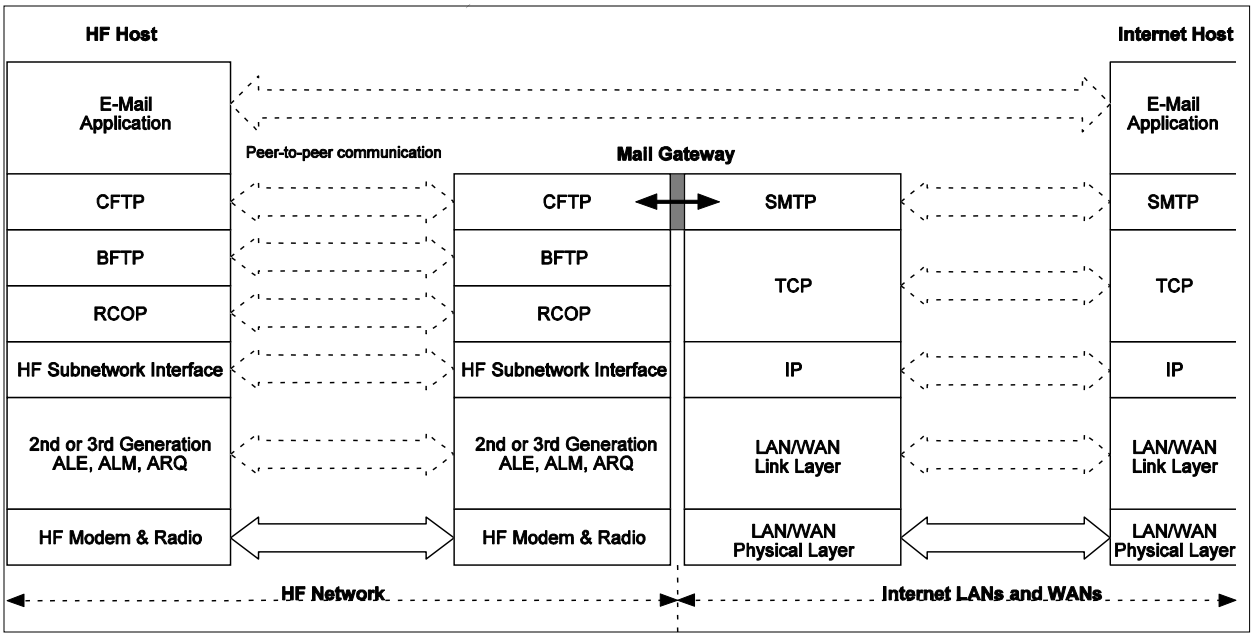


FIGURE E-2. Application-layer mail gateway.

This permits the use of protocols optimized for operation over HF links (e.g., the HF mail transfer protocol HMTP in STANAG 5066), and the exclusion from the HF network of protocols that can work poorly under some propagation conditions (e.g., the transmission control protocol TCP).

Gateways that operate in store-and-forward fashion introduce delays that may be undesirable in interactive applications. However, e-mail transfer is designed to operate in store-and-forward fashion, and naturally accommodates the gateway approach.

E.4.1.3.2 Transparent support for Internet applications.
For interactive applications such as remote login, file transfer, and web browsing, a router (IP gateway) at the boundary of the HF network serves to interface the distinct media-dependent protocols and hardware while allowing application and transport protocols to flow transparently through the HF subnetwork (Figure E-3). The Router function shown here may be more easily implemented in an automated HF radio or its external controller than in a commercial router because it includes components not usually found in commercial routers:

4. driver software that executes HF-specific protocols
5. hardware interfaces for the HF radio and modem.

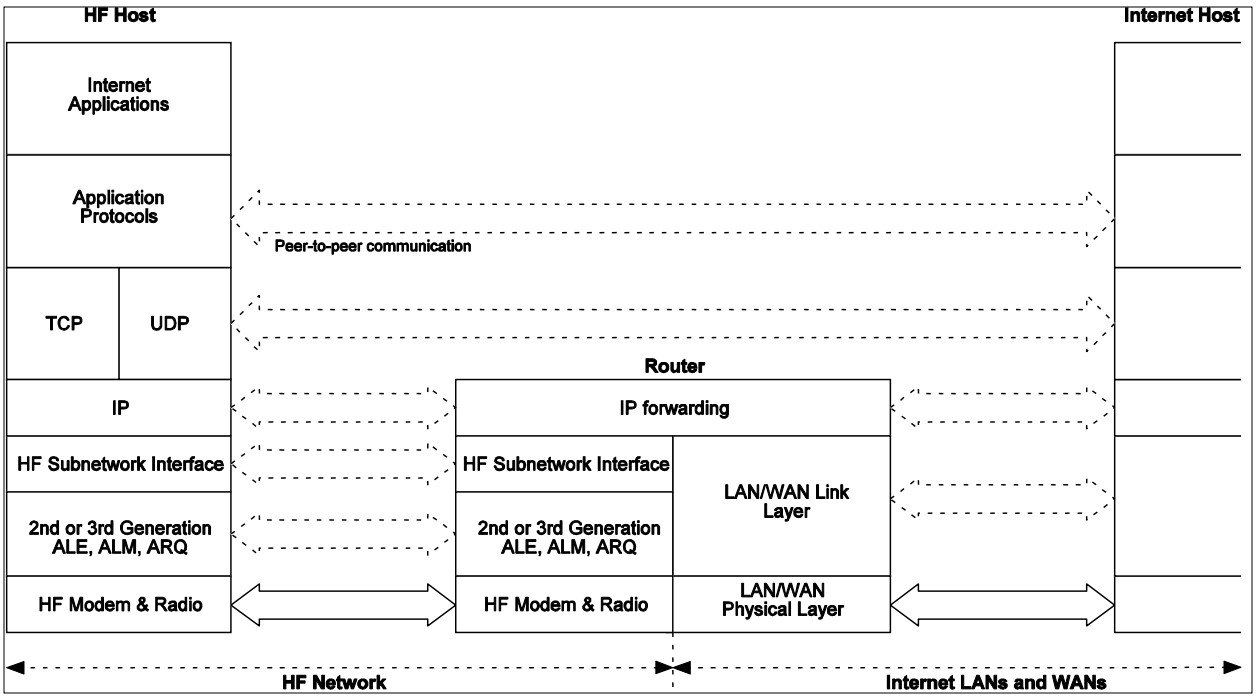


FIGURE E-3. Transparent support of Internet-native applications.

When a host computer is connected to the Internet via an HF network (e.g., HF Host in figure E-3), most Internet applications will call upon the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) for end-to-end transport service to the distant Internet Host. These two protocols, in turn, require the services of the Internet Protocol (IP) for routing packets through the Internet. HF network designers should be aware of several potential performance problems that arise when TCP and IP are used in an HF network:

a. The two protocols together add 40 bytes of overhead to each application PDU sent.

b. TCP connection setup requires an additional three-way handshake after the link establishment handshake and data link protocol startup. Each link turnaround consumes at least three interleaver times. For example, when using a MIL-STD-188-110 serial-tone modem with a 4.8 s interleaver, this three-way handshake will add at least 43 s to the time to establish a link (at least 58 s if the data rate is 75 bps).

c. The TCP congestion avoidance mechanisms can significantly reduce throughput each time the HF data link throughput changes abruptly.

E.4.1.4 Security.

Many military applications require encryption of application data. Figures E-4a through d show four alternatives for implementing Communications Security (COMSEC) for applications (including e-mail) that communicate over HF networks:

3. Application-layer security encrypts application data within each application before it is delivered to the application-layer protocol for delivery (see Figure E-4a). This offers end-to-end protection in application-specific fashion, but requires secured applications. Compression of application data will be useful only if applied before encryption.

4. Transport-layer security (e.g., the Secure Socket Layer, SSL) provides end-to-end application-independent security (see Figure E-4b). The TLS protocol [RFC-4346] was derived from SSL, and also offers optional in-line compression.

5. IPsec [RFC-4301] provides secure "tunnels" through IP networks for any higher-layer protocol, including TCP, UDP, ICMP, BGP, etc. (see Figure E-4c).

6. Link encryption (see Figure E-4d) individually secures each link in the end-to-end path. For illustration, Figure E-4d depicts a local area network (LAN) that operates in a secure area and does not require COMSEC, and an encrypted HF link.

Note that COMSEC key management is evolving towards use of the Public Key Infrastructure (PKI). Further COMSEC considerations are beyond the scope of this appendix.

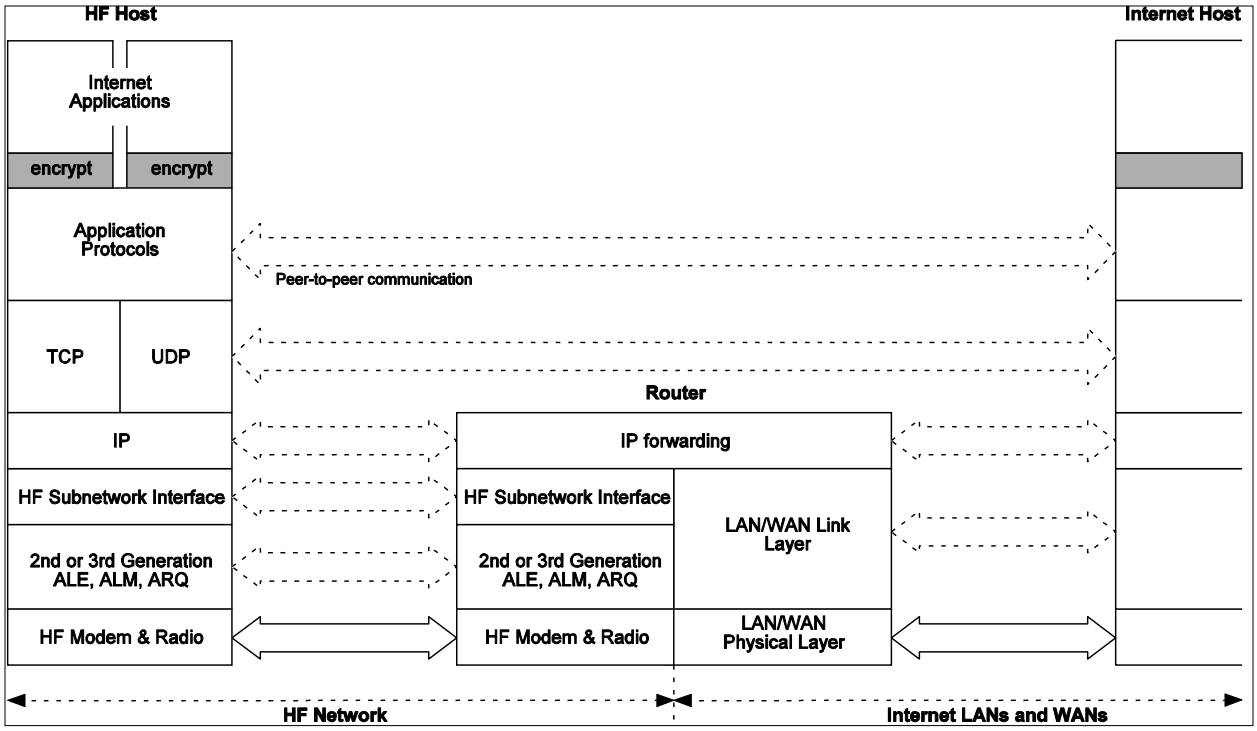


FIGURE E-4a. Application-layer security.

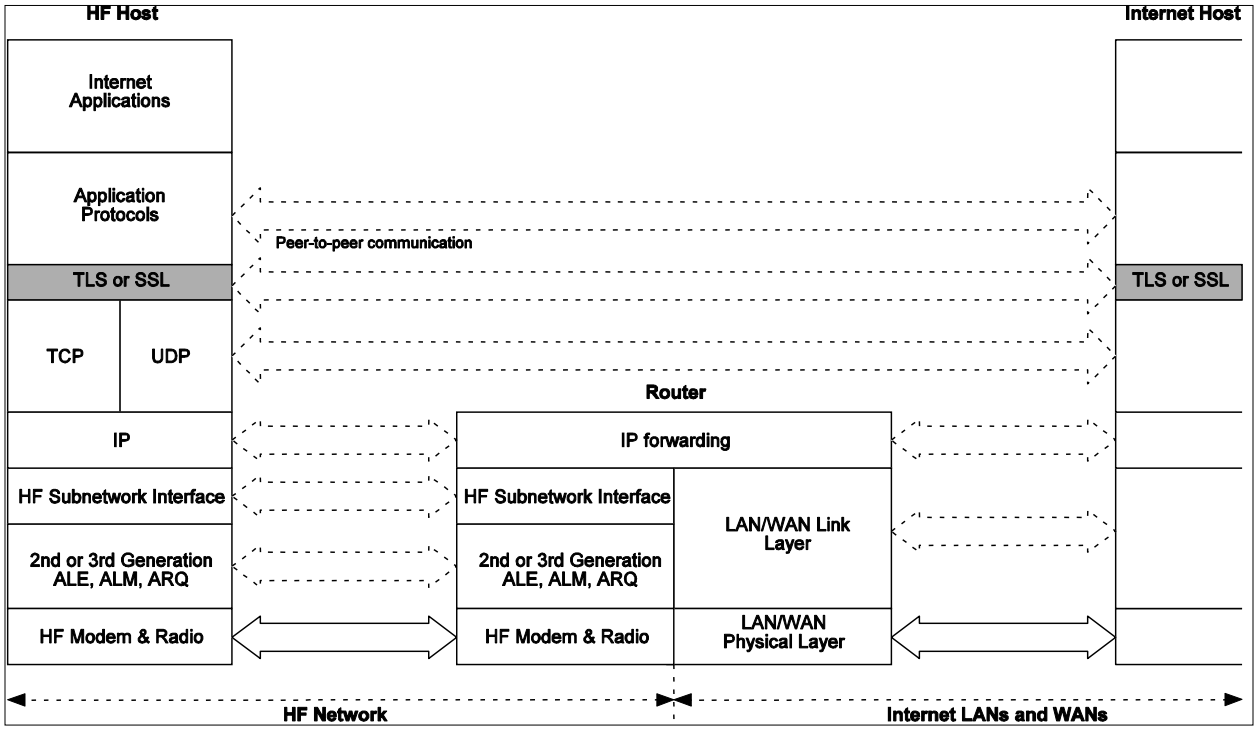


FIGURE E-4b. Transport-layer security.

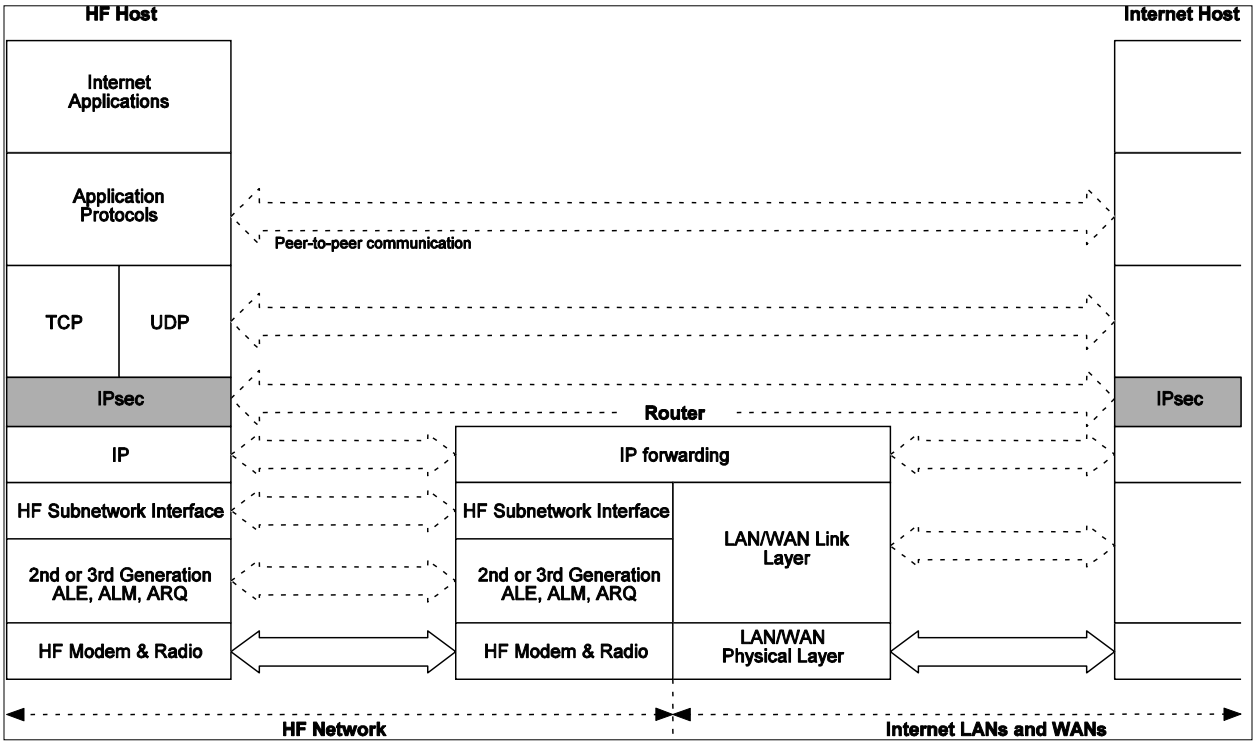


FIGURE E-4c. IPsec security.

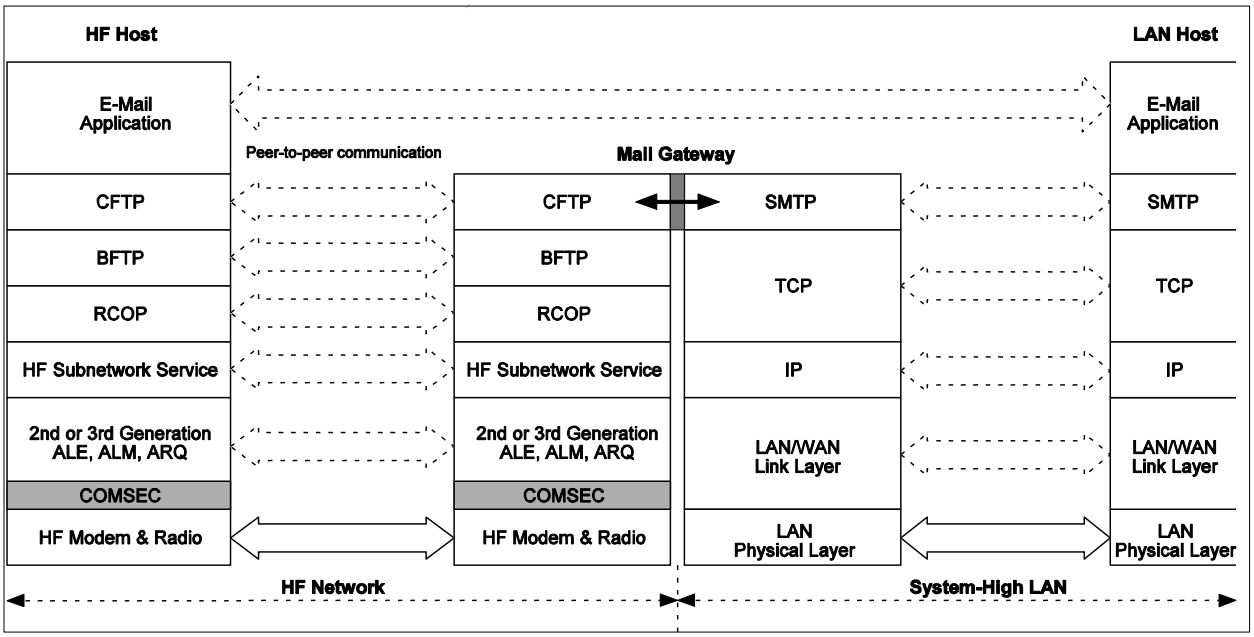


FIGURE E-4d. Link encryption.

E.4.2 Electronic mail transfer.
An HF e-mail system will be found to comply with this appendix if it conveys e-mail through HF networks using the required HF subnetwork protocols (see E.4.1.1 Required HF subnetwork service) and the Compressed File Transfer Protocol (CFTP) described in E.5.2.1 (Compressed FileTransfer Protocol). E-mail transfer on the non-HF side of mail gateways may use any suitable protocol.

E.4.2.1 Mail transfer within HF networks.
Mail should be transferred within HF networks using CFTP, except as provided in the following two paragraphs.

E.4.2.2 Mail retrieval by call-in users.
When connectivity to a user is too infrequent to use CFTP to push messages to that user's host computer, a mail drop should be created at a host that can usually be reached by that user over a single HF link. One of the mail retrieval protocols from E.5.2.2 (HF mail retrieval protocols) should be used to pull mail from the mail drop host to the user's host.

E.4.2.3 Mail transfer to and from NATO HF networks.
When interoperation with NATO networks employing the HF Mail Transfer Protocol (HMTP) is required, HMTP in accordance with E.5.2.3 should be employed.

E.4.3 Digital imagery transfer. (not yet standardized)

E.4.4 Digital voice operation. (not yet standardized)

E.4.5 Other applications.
Interactive applications such as file transfer and hypertext transfer (in support of the worldwide web) should employ the usual Internet application protocols for those applications:

Application	Protocol	Reference
Remote terminal	telnet	STD 8
Secure remote terminal	ssh	RFC 4251
File transfer	File Transfer Protocol (FTP)	STD 9
Hypertext transfer	Hypertext Transfer Protocol (HTTP)	RFC-2616

TCP should be implemented at the client and server hosts that support these applications. IP and related protocols should be implemented at client and server hosts and at routers that interconnect HF subnetworks with other subnetworks (see Figure E-3). IP should bind as a client to the HF Subnetwork Interface at the SAP ID specified for IP in STANAG 5066, Annex F. HF-Subnetwork Client Requirements.

E.5 DETAILED REQUIREMENTS

E.5.1 Introduction.

The functions supported by the protocols specified in this section are optional. However, when the functionality provided by one of these protocols is required, that protocol should be implemented as specified herein to provide such functionality.

E.5.2 Electronic mail protocols.

All implementations of HF e-mail should implement client and server CFTP; this is the interoperability mode for HF e-mail. CFTP should be used to "push" e-mail messages from one mail transfer agent (MTA) to the next. The Post Office Protocol version 3 (POP3) or the Internet Mail Access Protocol version 4 (IMAP4) should be used when retrieving ("pulling") e-mail messages from servers. For e-mail delivery within HF networks, the HF mail transfer protocol (HMTP) may be used as an alternative to CFTP. An e-mail server that implements more than the default protocol should simultaneously listen for, and correctly process, incoming e-mail requests in any of its supported protocols.

E.5.2.1 Compressed file transfer protocol.

The Compressed File Transfer Protocol (CFTP) sends compressed e-mail over an HF link using a file transfer protocol, rather than a mail transfer protocol, as depicted earlier in Figure E-2. CFTP should be implemented as specified in STANAG 5066 Annex F. HF-Subnetwork Client Requirements.

E.5.2.2 HF mail retrieval protocols.

When a user is usually not reachable (i.e., the user connects sporadically to pick up e-mail), CFTP will not be appropriate for delivery of mail *to* that user. In such cases, POP3 in accordance with STD 53 or IMAP4 in accordance with RFC 2060 should be used to retrieve mail from a mail drop server (see E.4.2.2). Messages *sent* by such users should be conveyed to the server in accordance with E.4.2.1.

E.5.2.3 HF mail transfer protocol.

The HF Mail Transfer Protocol (HMTP) is an extended version of the Simple Mail Transfer Protocol (SMTP). HMTP clients and servers should implement SMTP with the SMTP service extension ("EHLO") protocol in accordance with STD 10, command pipelining in accordance with STD 60 as modified in the following paragraphs, and MIME Extensions for SMTP, as defined in RFCs 2045, 2046, 2047, and 2049.

E.5.2.3.1 HMTP server requirements.

An HMTP server should comply with STD 60 to ensure a reliable implementation of the basic SMTP protocol.

a. The server should not lose buffered incoming commands in its transport layer (or equivalent) queue. This rule ensures that servers will correctly process arbitrarily long batches of commands.

b. The server should send all buffered responses whenever its queue of incoming commands is emptied. This rule ensures that responses to a batch of commands will always be sent after the end of the batch, no matter how short the batch, providing backward interoperability with SMTP clients.

For improved performance over HF subnetworks, HMTP servers may depart from the rules in STD 60 in the following regard.

c. The server may buffer responses to all incoming commands until the queue of incoming commands is empty.

The HMTP server should provide a relay capability for the client in accordance with STD 10. This relay capability may be used to provide an application-level gateway capability between the HF subnetwork and other networks, for example, those with lower latency and higher throughput for which the other protocols are more suited. With respect to relay and routing, the argument to the SMTP MAIL command is in the form “user@hostname”, which specifies who the mail is from. The argument to the RCPT command is in the same form and specifies the ultimate destination of the mail. The HMTP server should forward mail in accordance with STD 10. A destination may be rejected only if the server can not understand it. Source routing should not be used, as the HMTP model requires the server to have mail-routing information.

E.5.2.3.2 HMTP client requirements.
When connected to a server that supports command pipelining, HMTP clients should group commands to the maximum extent permitted in STD 60:

4. All setup commands, including RSET (if required), MAIL, RCPT, and DATA, for each message should be sent as a single group.

5. Multiple messages sent to a single server should be chained by appending the setup commands for each subsequent message to the message body of the preceding message.

For improved performance over HF subnetworks, HMTP clients connected to an HMTP server may depart from the rules in STD 60 in the following regard.

6. Any number of the commands sent to a single server, including the initial EHLO, may be grouped for transmission.

   Unlike ESMTP with command pipelining, which first checks for a valid response that confirms a peers capability to use the pipelined commands, HMTP proceeds under the assumption that the peer process is fully compliant with its pipelined SMTP commands. This streamlines the process by using the minimum number of transactions between the client and server. The disadvantage is that if the peer-level mail process is not compliant with HMTP, then the transactions are lengthy to no purpose, since the mail will not be transferred correctly but the transmissions could take significant time on the channel before this is determined.

When connected to a server that does not support command pipelining, HMTP clients should execute SMTP in its basic interlocked mode in accordance with STD 10.

E.5.2.3.3 HMTP over TCP.
When HMTP uses TCP transport services, it should listen on TCP port 25 (the well-known SMTP port), and, in general, use TCP in the same manner as does SMTP.

E.5.2.3.4 HMTP without TCP.
When TCP is not used to transport HMTP data, the HMTP server should bind to the SAP ID of the HF subnetwork service specified for HMTP in in STANAG 5066 Annex F. HF-Subnetwork Client Requirements.

E.6 NOTES

None.

APPENDIX F

RADIO REQUIREMENTS FOR CO-LOCATED INSTALLATION

TABLE OF CONTENTS

PARAGRAPH **PAGE**

TABLES

TABLE **PAGE**

FIGURES

FIGURE **PAGE**

RADIO REQUIREMENTS FOR CO-LOCATED INSTALLATION

F.1 GENERAL.

F.1.1 Scope.
This appendix contains requirements for MF and HF radio systems that are installed in close proximity to each other.

F.1.2 Applicability.
This appendix is mandatory for MF and HF radio systems installed on mobile platforms (such as ships or aircraft) that carry more than a single such radio system. It is optional (but recommended) for fixed sites having multiple radio systems.

F.2 APPLICABLE DOCUMENTS.

F.2.1 General.
The documents listed in this section are specified in sections F.3, F.4, and F.5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in sections F.3, F.4, and F.5 of this standard, whether or not they are listed.

F.2.2 Government documents.

F.2.2.1 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 cited in the solicitation or contract.

FEDERAL STANDARDS

FED-STD-1037	Telecommunications: Glossary of Telecommunication Terms

(Copies of these documents are available online at http://quicksearch.dla.mil.)

F.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.

F.3 DEFINITIONS.

F.3.1 Terms.

Broadband system. A system that contains combiners and multicouplers so that two or more circuits can simultaneously use a common antenna(s).

Narrowband transmitting system. A transmitting system in which each transmitter (exciter and power amplifier) is attached to a separate antenna, often via a tunable impedance matching device.

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

ALE	automatic link establishment
dBc	decibels referenced to full-rated peak envelope power
PEP	peak envelope power

F.4 GENERAL REQUIREMENTS.

F.4.1 Introduction.
When multiple radio systems operate within close proximity of each other, their emanations may couple into adjacent antennas or radio equipment, resulting in undesired intermodulation and other effects. Radio systems intended for such co-sited operation shall meet additional requirements as detailed in the following paragraphs.

F.4.2 Measurements.
RF performance for these systems shall be measured at the receive and transmit antenna ports.

F.5 DETAILED REQUIREMENTS.

F.5.1 Common equipment characteristics.
The following requirements replace the corresponding requirements in section 5.2 in the indicated applications.

F.5.1.1 Frequency accuracy of Navy shipboard radio systems.
The accuracy of the radio carrier frequency (see 5.2.3 Frequency accuracy) of Navy shipboard radio systems shall be within ±1.0 Hz when the frequency accuracy of the internal standard is ±1 part in 10^9 or better.

F.5.1.2 Transmitter characteristics.
The following requirements replace the corresponding requirements in section 5.3 in the indicated applications.

F.5.2.1 In-band noise for co-sited transmitters.
For co-sited installations, broadband noise in a 1-Hz bandwidth within the selected sideband shall be at least 85 decibels referenced to full-rated peak envelope power (dBc) below the level of the rated PEP of the HF transmitter. (This is a more stringent requirement than paragraph 5.3.1.1 In-band noise.)

F.5.2.2 Broadband emissions limits for co-sited transmitters.
When a transmitter for co-sited installation is driven to rated PEP with a single tone in the center of the necessary bandwidth, the power spectral density of the transmitter broadband emission shall not exceed the level established in Table F-I and as shown in Figure F-1. (This is a more stringent requirement at frequencies more than 5% removed from the center frequency than paragraph 5.3.2.1 Broadband emissions.)

Discrete spurs shall be excluded from the measurement, and the measurement bandwidth shall be 1 Hz. In cases where the necessary bandwidth causes a conflict with limits based on percentage offset from f_c, the less stringent limit shall apply.

F.5.2.3 Discrete frequency spurious emissions limits for shipboard transmitters.
When a transmitter for co-sited shipboard installation is driven with a single tone to produce an RF output of 25 percent rated PEP, all discrete frequency spurious (non-harmonic) emissions shall be suppressed as follows:

- Inside the information bandwidth for broadband and narrowband systems with transmit circuit keyed and modulated, at least -40dBc
- For broadband systems when measured over any 3kHz bandwidth beyond ±5% from the carrier frequency with transmitter driven with a single tone to produce an RF output at rated PEP, transmitter output terminated, keyed with no drive applied: no more than two spurious outputs per circuit not to exceed -120dBc with all other spurious outputs per circuit not to exceed -130dBc.
- For narrowband systems beyond ±5% from the carrier frequency with transmitter driven with a single tone to produce an RF output at rated PEP, transmitter output terminated, keyed with no drive applied: no more than two spurious outputs per circuit not to exceed -146dBc with all other spurious outputs per circuit not to exceed -156dBc.

(NOTE: These are more stringent requirements than paragraph 5.3.2.2 Discrete frequency spurious emissions.)

TABLE F-I. Out-of-band power spectral density limits for co-sited radio transmitters.

Measurement Frequency (Hz)	Power Spectral Density Limit (dBc/Hz) for Co-sited Transmitters		
	Shipboard Narrowband Transmitters	Shipboard Broadband Transmitters	All Other Co-Sited Transmitters
$f_m = f_c \pm (0.5\ B + 500)$	–75	–75	–75
$f_m = f_c \pm 1.0\ B$	–80	–80	–80
$f_m = f_c \pm 2.5\ B$	–95	–95	–95
$(f_c + 4.0\ B) \leq f_m < 1.05\ f_c$ $0.95\ f_c < f_m \leq (f_c - 4.0\ B)$	–105	–105	–105
$f_m \leq 0.95\ f_c$ $f_m \geq 1.05\ f_c$	–181	–175	–155
Where f_m = frequency of measurement (Hz) f_c = center frequency of bandwidth (Hz) B = necessary bandwidth (Hz)			

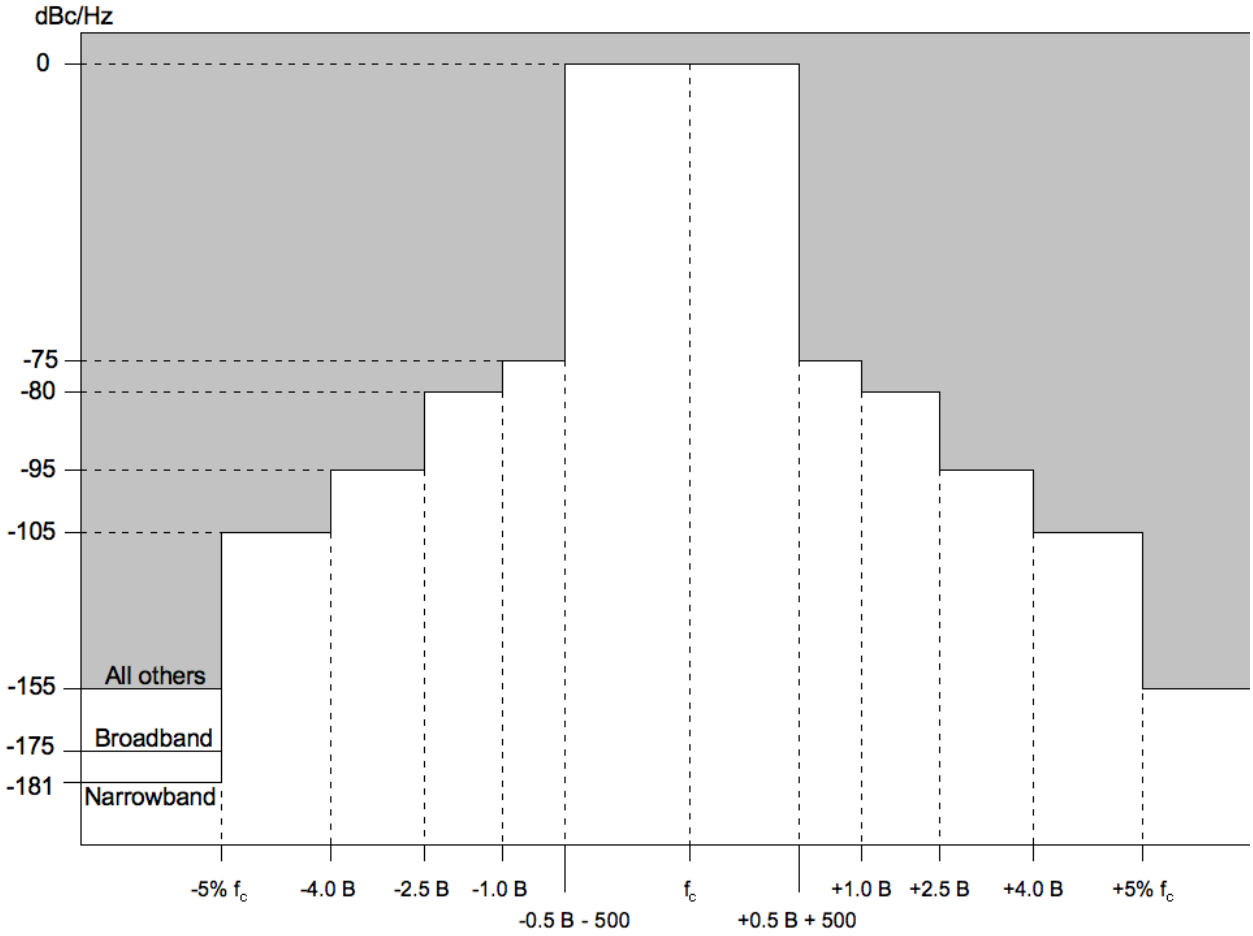


Figure F-1. Out-of-band spectral power density limits for co-sited radio transmitters.

F.5.2.4 Discrete frequency harmonic emissions limits for shipboard transmitters.
For shipboard HF transmission systems, when driven with a single tone to produce 100% rated PEP, harmonic emissions shall be suppressed as follows:

a. For narrowband transmitting systems
   - Second and third harmonics shall not exceed -90dBc
   - Fourth and higher harmonics shall not exceed -140dBc

b. For broadband transmitting systems (output terminated in 50 ohms)

   1. For harmonic frequencies within the 3dB bandwidth of the transmit antenna circuit
      - Second and third harmonics shall not exceed -50dBc
      - Fourth and higher harmonics shall not exceed -70dBc

2. All harmonic frequencies outside the 3dB bandwidth of the transmit antenna circuit shall monotonically decrease in level from the highest in-band order at a rate of at least 36dB per octave to a floor no greater than -140dBc.

F.5.3 Receiver characteristics.
The following requirements replace the corresponding requirements in section 5.4.1 in the indicated applications.

F.5.3.1 Shipboard receive system sensitivity.
The sensitivity of receive systems for shipboard environments over the operating frequency range, in the sideband mode of operation (3kHz bandwidth), shall be such that a -108dBm unmodulated signal at the receive system RF antenna input, adjusted for a 1000 Hz audio output, produces an audio output with a SINAD of at least 10dB over the operating frequency range. (NOTE: this is reduced sensitivity compared to 5.4.1.7 Receiver sensitivity.)

F.5.3.2 Other signal-frequency external spurious rejection for shipboard systems.
In addition to the requirements of 5.4.1.4 Other signal-frequency external spurious responses, for co-sited shipboard operation, receive system rejection of spurious frequencies, other than IF and image, shall be at least 156 dB for frequencies beyond ±5% of the center frequency.

F.5.3.3 Desensitization dynamic range for co-site receive systems.
The following requirement shall apply to the receiver for a co-sited system in an SSB mode of operation with an IF passband setting providing at least 2750 Hz (nominal 3 kHz bandwidth) at the 2 dB points. With the receiver tuning centered on a sinusoidal input test signal and with the test signal level adjusted to produce an output SINAD of 10 dB, a single interfering sinusoidal signal, offset from the test signal by an amount equal to ±5 percent of the carrier frequency, is injected into the receiver input. The output SINAD shall not be degraded by more than 1 dB when the interfering signal is equal to or less than 136 dB above the test signal level. (Note: this is a more stringent requirement than 5.4.1.6 Desensitization dynamic range.)

APPENDIX G

WIDEBAND AUTOMATIC LINK ESTABLISHMENT SYSTEM (WALE)

(FOURTH GENERATION (4G))

TABLE OF CONTENTS

TABLES

TABLE **PAGE**

FIGURES

FIGURE **PAGE**

WIDEBAND AUTOMATIC LINK ESTABLISHMENT SYSTEM

G.1 GENERAL

G.1.1 Scope.

This appendix provides details of the prescribed waveforms, signal structures, protocols, and performance requirements for the fourth generation (4G) automatic link establishment (ALE) system, also known as Wideband ALE (WALE). Optional design objectives are noted as DO.

G.1.2 Applicability.

This appendix is a mandatory part of MIL-STD-188-141 whenever WALE is a requirement to be implemented in a high frequency (HF) radio system. The functional capability described herein includes automatic signaling, selective calling, automatic answering, and radio frequency (RF) scanning with link quality analysis (LQA). The capability for manual operation of the radio in order to conduct communications with existing, older generation, non-automated manual radios, shall not be impaired by implementation of these automated features.

G.2 APPLICABLE DOCUMENTS

G.2.1 General.

The documents listed in this section are specified in G.3, G.4, and G.5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in G.3, G.4, and G.5 of this standard, whether or not they are listed.

G.2.2 Government documents.

G.2.2.1 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 cited in the solicitation or contract.

INTERNATIONAL STANDARDIZATION AGREEMENTS

STANAG 4538	Technical Standards for an Automatic Radio Control System For HF Communication Links
STANAG 5066	Profile for HF Radio Data Communications

FEDERAL STANDARDS

FED-STD-1037	Telecommunications: Glossary of Telecommunications Terms

DEPARTMENT OF DEFENSE STANDARDS

MIL-STD-188-110	Interoperability and Performance Standards for Data Modems

(Copies of these documents are available online at http://quicksearch.dla.mil.)

G.3 DEFINITIONS

G.3.1 Terms.
Definitions of terms used in this document shall be as specified in the current edition of FED-STD-1037 except where inconsistent with the use in this standard. In addition, the following definitions are applicable for the purpose of this standard.

Assigned frequency	The center of a frequency band assigned to a station
Assigned frequency band	A frequency band within which the emission of a station is authorized (by a national administration)
Individual address	binary number that refers to a single station
Multipoint address	binary number that refers to multiple stations
User process address	alphanumeric designator that corresponds to an individual or multipoint address

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

Acronym	Meaning	Reference
2G	second generation	G.4.1.7
3G	third generation	G.4.1.8
3GWB	third-generation with wideband extensions	G.4.1.8, G.5.5.7
4G	fourth generation	G.1.1
ALE	automatic link establishment	G.1.1
ASCII	American standard code for information interchange	G.4.1.7, G.5.6.3
dB	decibel	G.4.3.2, G.5.5.1.6
DO	design objective (optional)	
EC	equipment capability (maximum supported bandwidth)	G.5.5.1.3
FLSU	fast link set-up (a 3G ALE protocol)	G.4.1.8
HF	high frequency	G.1.2
IAW	in accordance with	
LBR	listen before responding	G.5.5.2, Table G-II
LBT	listen before transmitting	G.5.5.2, Table G-II
LQA	link quality analysis	G.4.2.3, G.5.5.10
NATO	North Atlantic Treaty Organization	
PDU	protocol data unit	G.4.1
PTM	point-to-multipoint	G.5.5.8
PTP	point-to-point	G.5.5.4
PU	participating unit	G.4.1.1
SDS	synchronous dwell speed	G.4.1.2.2
SNR	signal to noise ratio	G.4.1.5
WALE	wideband automatic link establishment	G.1.1

G.4 GENERAL REQUIREMENTS

G.4.1 WALE Operation.

The technology specified in this appendix includes waveforms ("Deep WALE" and "Fast WALE") and protocols for conveying fixed-size (96-bit) protocol data units (PDUs) over an HF channel. The exchange of such PDUs according to the specified protocols supports channel evaluation, selective calling, traffic bandwidth negotiation, and passing data and text messages. The following paragraphs specify the general requirements for WALE operation.

G.4.1.1 WALE Addressing.

Systems compliant with this appendix shall support two forms of addressing: User Process addressing and PDU addressing.

User Process addresses are alphanumeric addresses that contain from 3 to 15 printable ASCII characters. These addresses shall be presented to all user applications including, but not limited to the following:

- Equipment front panel displays
- Computer Messaging Application user interfaces.

PDU addresses are 16-bit binary numbers. In NATO applications, a 16-bit binary network number is associated with each PDU address, and shall be used as specified in G.5.3.

An *individual* Participating Unit (PU) address refers to exactly one PU. A *multipoint* address refers to a pre-programmed collection of PUs; this is analogous to the *net* address in 2G ALE (Appendix A). Note that multipoint addresses are in the same code space as individual addresses.

G.4.1.2 Scanning.

Systems compliant with this appendix shall be capable of repeatedly scanning a list of channels (a "scan set") listening for calls and sounding transmissions. Each PU shall scan this list of calling channels in sequential order, from the lowest calling channel ID (G.4.2.1.5) to the highest calling channel ID, then starting over with the lowest calling channel ID. While scanning, the PU shall record calling channel occupancy, and all incoming transmissions shall be evaluated in accordance with (IAW) G.4.1.5.

Both synchronous and asynchronous scanning shall be available. The active scanning mode and scanning dwell times shall be configurable as Initial Net Parameters (INPs; see G.4.2.4).

G.4.1.2.1 Asynchronous scanning.

When scanning asynchronously, systems shall dwell on each channel for the Minimum Dwell Time INP (G.4.2.4), except that the dwell may be extended when evaluating an incoming signal.

G.4.1.2.2 Synchronous scanning.

When scanning synchronously, dwell periods shall be synchronized to the start of a GPS epoch, even for stations without GPS time. The lowest Channel ID shall be visited in the first dwell of the GPS epoch. Synchronized stations shall use the current time to compute the proper dwell channel, such that they are synchronized with dwelling as if it began in the first possible dwell.

The calling channel on which any PU is listening for calls (when indeed it is listening for calls) may be computed at all times when network time and relevant INPs (G.4.2.4) are known:

T = Seconds since midnight (network time)
D = Duration of dwell (seconds)
C = Number of channels in scan set (Channel IDs run from 0 through C–1)

current calling channel = (trunc(T / D)) mod C

where trunc(x) is the largest integer less than or equal to x.

The synchronous dwell time D is specified in terms of a Synchronous Dwell Speed (SDS):

Table G-I Synchronous Dwell Speed.

SDS	Dwell time D (s)	Application
1	1.350	Mixed 3G / 4G networks. Scans at 3G speed.
2	0.675	Supports both Fast WALE and Deep WALE.
3	0.450	For networks emphasizing high-speed data. Supports Fast WALE only.

Dwell time D = 1.35s / SDS.

G.4.1.3 Staring (optional).

Systems that are capable of listening for calls simultaneously and continuously on multiple channels (a “stare set”) may operate in staring rather than scanning mode. Such operation can improve both the speed of link setup and the system’s awareness of other traffic on its channels.

G.4.1.4 Link Setup.

Upon request by the operator or a client process, the system shall execute the appropriate link setup protocol specified in G.5.5. The operator or client process shall be able to override automatic channel selection by specifying a channel for the call.

G.4.1.5 Channel Evaluation.

The system shall measure the signal to noise ratio (SNR) of all WALE PDUs that it processes, whether addressed to that station or to other(s), and store the results, indexed by the channel and the sending station, in the Other Station Table (G.4.2.3).

While scanning or staring, the system shall maintain a record of the recent occupancy (see G.4.3.2) of scan set or stare set channels (G.4.2.1.4).

During link setup handshakes, the system shall automatically measure and report spectrum occupancy of the wideband channel associated with the active calling channel IAW G.5.5.1.5.

The system shall be capable of automatically transmitting ALE sounding transmissions IAW G.5.5.4.

G.4.1.6 Override mode.

The system is designed to detect channels in use and to avoid interfering with such channels. However spurious emissions and other interference could cause this adaptive system to avoid transmitting on channels that are actually usable. A means shall be provided for the operator to put the system into an “override mode” that enables transmission on such channels.

G.4.1.7 Interoperation with 2G ALE.

Systems compliant with this appendix shall be capable of accepting calls and establishing links using the second-generation ALE (2G-ALE) protocol specified in Appendix A. The interoperability mode shall includes individual and net calls and Automatic Message Display (AMD) messages. Addresses containing 1 through 15 Basic-38 ASCII characters (defined in Appendix A) shall be recognized and accepted. Additional 2G-ALE capabilities are optional. A means shall be provided to disable responses to 2G calls.

G.4.1.8 Interoperation with 3G ALE.

Systems compliant with this appendix shall be capable of accepting calls and establishing links using the third-generation (3G) Fast Link Set-Up (FLSU) protocol specified in STANAG 4538. Asynchronous-mode 3G calls can be accepted by a 4G network in any of its operating modes. To interoperate with 3G FLSU radios in synchronous mode, including 3G radios with wideband extensions (3GWB), a 4G network must operate synchronously with SDS = 1. A means shall be provided to disable responses to 3G calls. Additional 3G capabilities are optional.

G.4.2 Required Data Structures.

G.4.2.1 Channel memory.

G.4.2.1.1 Channel definition.

The term “frequency” refers to an assigned frequency. The term “bandwidth” refers to the lesser of the equipment capability (see G.5.5.1.3) and the width of an assigned frequency band. For the communications system specified here a channel is a programmable association of a channel ID with one or two (frequency, bandwidth) pairs.
A simplex wideband channel is a single assigned frequency band, centered on an assigned frequency. (In narrowband HF systems the channel *reference* frequency is the frequency of the carrier or suppressed carrier, and a channel is defined as the upper sideband or lower sideband relative to that reference frequency.)
A duplex wideband channel is two distinct assigned frequency bands, each centered on an assigned frequency. Note that the duplex channel has a single channel ID.

G.4.2.1.2 Sub-channel vector.

WALE manages contiguous channels of up to 48 kHz. Wideband channels are described in WALE PDUs using 16-element “sub-channel” vectors. Each 1-bit element of a sub-channel vector refers to a sub-channel within an assigned wideband channel. For systems capable of using 48 kHz channels (EC = binary 11; see G.5.5.1.3), sub-channel vectors describe 3 kHz sub-channels. For all other systems, sub-channel vectors describe 1.5 kHz sub-channels.

G.4.2.1.2.1 Sub-channel vectors for 1.5 kHz sub-channels.

As shown in Figure G-1, a vector of 1.5 kHz sub-channels covers a range of 24 kHz, centered on the assigned frequency for the channel. Element 0 refers to a 1.5 kHz sub-channel from 12 kHz to 10.5 kHz below the assigned frequency, whether or not that sub-channel is part of the assigned frequency band.

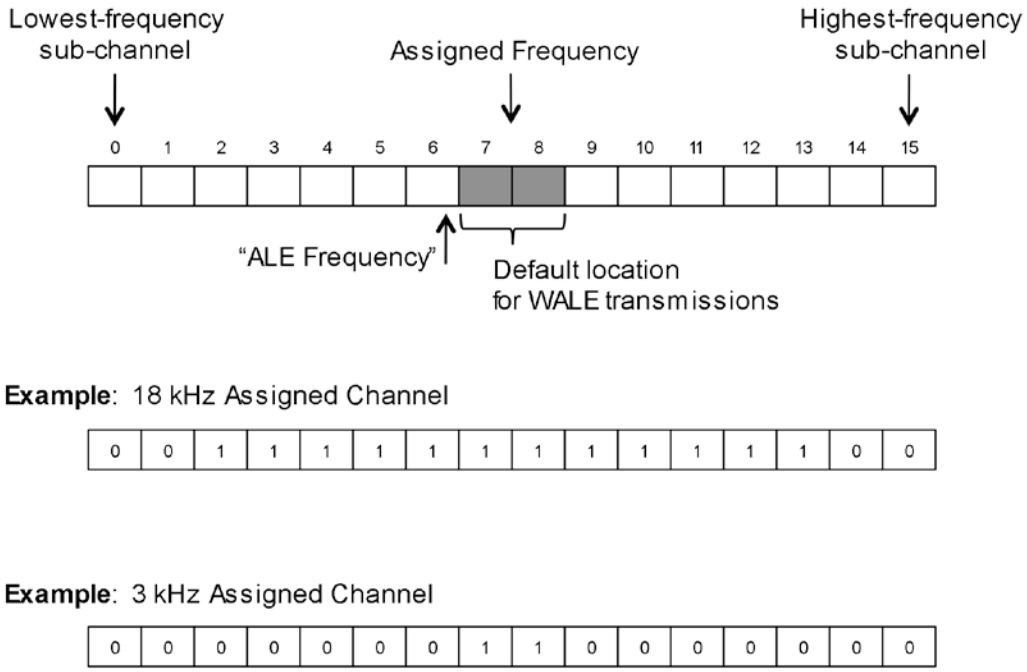


Figure G-1. WALE sub-channel vector for 1.5 kHz sub-channels

The examples in Figure G-1 show how a sub-channel vector is used to indicate the assigned bandwidth for a channel. In the examples, each sub-channel included in the assigned channel is indicated with a 1 bit, while sub-channels outside the assigned channel are indicated with 0s.

G.4.2.1.2.2 Sub-channel vectors for 3 kHz sub-channels.

A vector of 3 kHz sub-channels covers a range of 48 kHz. Element 0 refers to a 3 kHz sub-channel from 24 kHz to 21 kHz below the assigned frequency.

- If the assigned channel bandwidth is an even multiple of 3 kHz (e.g., 6 kHz or 12 kHz), the assigned frequency again falls between elements 7 and 8 of the sub-channel vector as shown in Figure G-2.
- However, if the assigned channel bandwidth is an odd multiple of 3 kHz (e.g., 3 kHz or 9 kHz), the assigned frequency shall fall in the center of sub-channel 8 and sub-channel 0 shall be unused, as shown in Figure G-3.

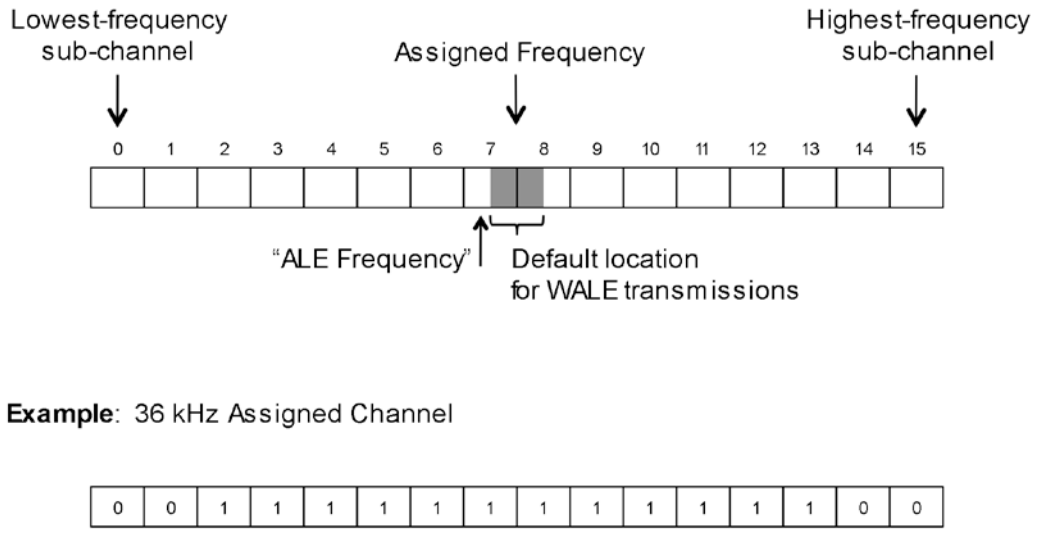


Figure G-2. WALE sub-channel vector for an even number of 3 kHz sub-channels

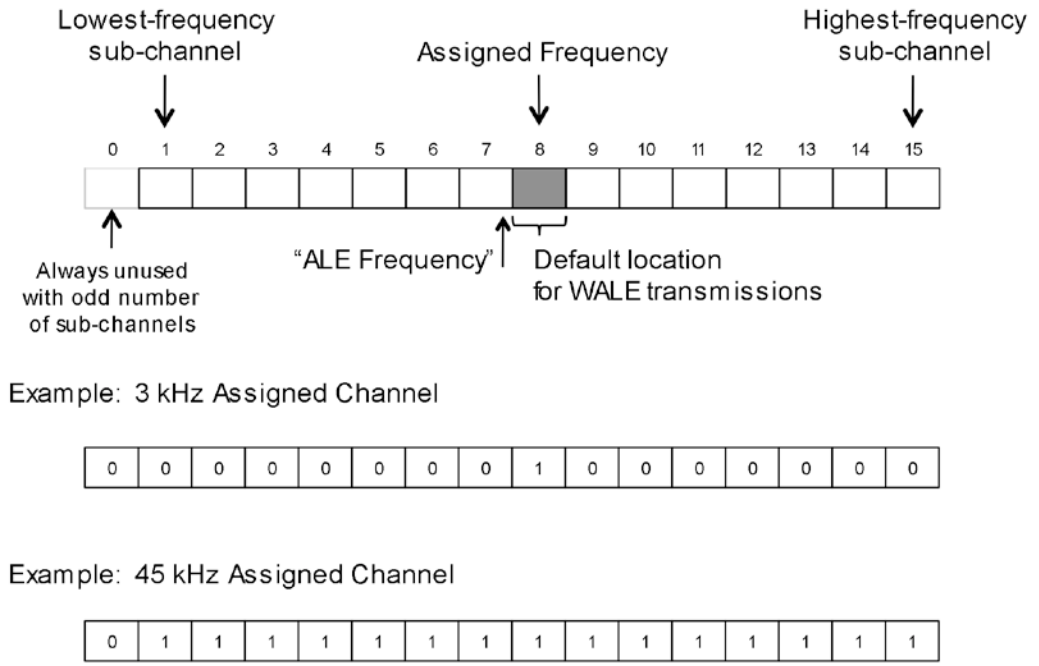


Figure G-3. WALE sub-channel vector for an odd number of 3 kHz sub-channels

G.4.2.1.3 WALE channel.

WALE transmissions use a 3-kHz waveform that is normally sent in a 3 kHz channel centered on the assigned frequency, as shown in the preceding figures. The frequency of the channel used for WALE transmissions is indicated in the channel record (G.4.2.1.4) for each WBHF channel.

G.4.2.1.4 Channel records.

Systems compliant with this appendix shall be capable of storing, retrieving, and employing at least 100 channel records.
A channel record includes at least the following information for a channel:

- Assigned frequency.
- Assigned sub-channel vector, centered on that assigned frequency, which contains a contiguous range of elements set to 1 that indicate the assigned spectrum for the channel (i.e., the sub-channels on which the PU may transmit). Elements outside that contiguous range shall be set to 0. Figure G-4 shows an example sub-channel vector for a 12-kHz assigned channel in a 48 kHz-capable system.
- The frequency on which WALE transmissions will be sent. The frequency shall be that of the suppressed carrier, considering the WALE transmission as USB. By default, this is 1800 Hz below the assigned frequency for the channel, so that the spectrum of the ALE signal is centered on the assigned frequency.
- Record of recent occupancy of the WALE channel, detected during scanning or staring (see G.4.1.5 and G.4.3.2).
- DO: Indication of recent occupancy of each of the assigned sub-channels, detected during scanning or staring (see G.4.1.5 and G.4.3.2).

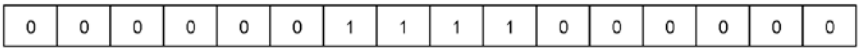


Figure G-4. Example Sub-channel Vector for 12 kHz Assigned Channel

G.4.2.1.5 Channel list.

Systems compliant with this appendix shall be capable of storing, retrieving, and employing at least one list of channel records for use as a scan set (G.4.1.2) or a stare set (G.4.1.3). The channel number (or channel ID) corresponding to each entry is its position in the channel list.

G.4.2.2 Self address memory.

Systems compliant with this appendix shall store exactly one self-address record, which contains at least the following fields:

- User process address
- Individual self address
- Zero or more multipoint addresses
- For each multipoint address, slot number for responses to a multipoint call to that address (set to 0 to disable responses)
- NATO network number (all 0's if not used).

G.4.2.3 Other station table.

Systems compliant with this appendix shall store a table of other stations in the network that includes at least the following in each Other Station record:

- User Process address
- WALE address
- NATO network number (all 0's if not used)
- Scanning mode of that PU (asynchronous, synchronous, or staring)
- Link Quality Analysis (LQA) data for each channel in the active channel list.

Storage shall be provided for at least 100 such Other Station records.

G.4.2.4 Initial network parameters.

The following Initial Network Parameters (INPs) shall be programmable by at least one of the following means: operator interface, external data fill port, or over-the-air data fill protocol.

Table G-II Initial network parameters.

Initial network parameter	Default Value	Range
Active scan or stare set (a channel list and the referenced channel records)		
Search mode: asynchronous scanning, synchronous scanning, or staring		
Synchronous dwell speed SDS (sync dwell time D = 1.35s / SDS)	3	1, 2, or 3
Minimum dwell time d_{min} when scanning in asynchronous mode	200 ms	≥100 ms
Listen before transmitting (LBT) time, t_{LBT}	400 ms	
Listen before responding (LBR) time, t_{LBR}	400 ms	
Transmit level control settling time t_{TLC}	13.33 ms	n x 13.33
Network maximum tune time t_{tune}	40 ms	
Maximum network time uncertainty t_{sync}	36 ms	
Wait for response time $t_{response}$	2 s	G.5.5.11.4
Wait for traffic time $t_{traffic}$	10 s	G.5.5.11.4
Activity timeout $t_{activity}$	30 s	G.5.5.11.4
Net control PU (WALE address)	0x0000	
Ignore broadcast calls?	No	
Accept and respond to 2G calls?	Yes	
Accept and respond to 3G calls?	Yes	

G.4.3 System Performance Requirements.

Systems compliant with this appendix shall demonstrate overall system performance equal to or exceeding the following requirements.

G.4.3.1 Scanning Rate.
Systems compliant with this appendix shall meet all System Performance Requirements when scanning asynchronously with a minimum dwell time of 200 ms.
When scanning synchronously, systems compliant with this appendix shall meet all System Performance Requirements with a dwell time of 450 ms (Fast WALE) or 675 ms (Deep WALE).

G.4.3.2 Occupancy Detection.
An ALE channel or traffic sub-channel should be considered occupied if the energy in that (sub-) channel is at least 10 dB greater than that in the lowest-energy (sub-)channel of the entire wideband channel, which is used as the instantaneous noise floor for that wideband channel.
Systems compliant with this appendix shall meet or exceed a detection probability of 99% for each (sub-)channel having at least 10 dB more energy than the noise floor, when tested as shown in Figure G-5. Test signals will be modem waveforms of varying bandwidths added to wideband noise. The examples illustrate some of the possible situations:

- Example A shows a 3-kHz signal centered in 3 kHz sub-channel number 3. Only that sub-channel is occupied.
- Example B shows a 3-kHz signal that is misaligned with 1.5-kHz sub-channels. There is sufficient energy in sub-channel 2 and 4 that both are occupied (integrated energy is at least 10dB greater than the noise floor), as is sub-channel 3.

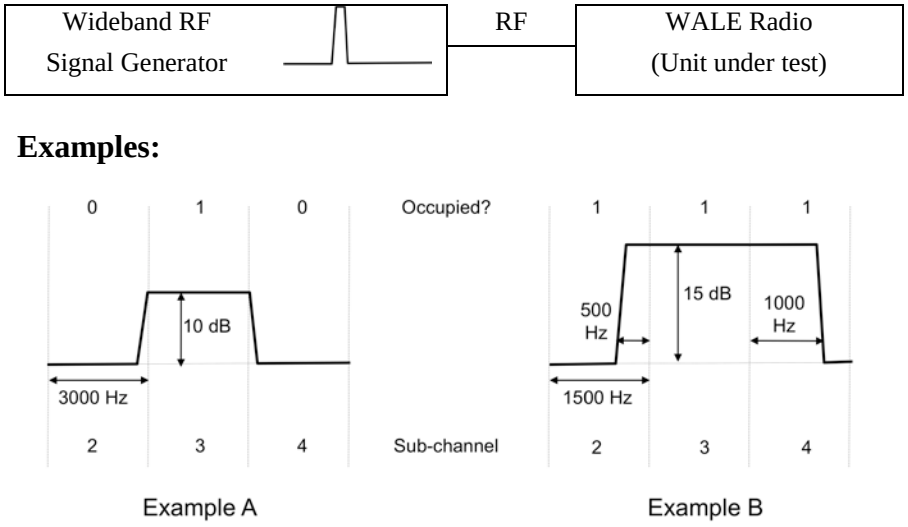
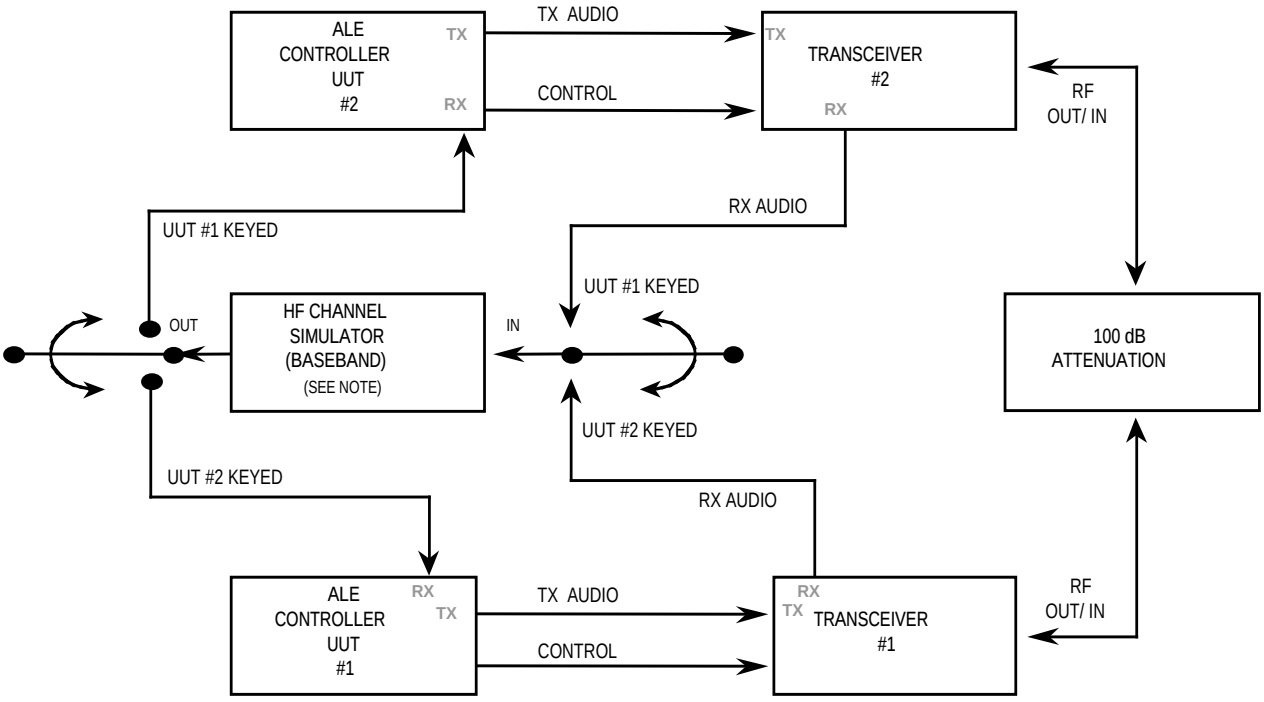


Figure G-5. Occupancy detection test setup.



NOTE: THE SIMULATOR INCLUDES EITHER INTERNAL OR EXTERNAL CAPABILITY TO ADJUST/MONITOR SIGNAL/NOISE/DOPPLER-OFFSET SETTINGS AND SHALL INCORPORATE APPROPRIATE FILTERING TO LIMIT THE AUDIO PASSBAND TO 300 - 3050 Hz.

Figure G-6. System performance measurements test setup.

G.4.3.3 Linking Probability.

Linking attempts made with a test setup configured as shown in Figure G-6, using the specified ALE signal created in accordance with this appendix, shall meet or exceed the probability of linking specifications shown in Table G-III for Deep WALE and Table G-IV for Fast WALE.

Table G-III Probability of linking: Deep WALE waveform.

	Signal-to-noise ratio (dB in 3 kHz)		
Probability of Linking (Pl)	AWGN Channel	Good Channel	Poor Channel
25%	-9	-7	-5
50%	-8	-5	-2
85%	-7	-2	1
95%	-6	2	4

Table G-IV Probability of linking: Fast WALE waveform.

	Signal-to-noise ratio (dB in 3 kHz)

	Signal-to-noise ratio (dB in 3 kHz)		
Probability of Linking (Pl)	AWGN Channel	Good Channel	Poor Channel
25%	0.0	+3	+3
50%	1.0	+5	+5
85%	1.5	+8	+8
95%	2.0	+10	+10

Each of the signal-to-noise (SNR) ratio values shall be measured in a nominal 3 kHz bandwidth. Performance tests of this capability shall be conducted in accordance with MIL-STD-188-110 Appendix E “Characteristics of HF Channel Simulators.”

A link will be declared successful if, in response to the first link request, the PUs execute a 2-way link setup handshake and both PUs enter a linked state.

G.5 DETAILED REQUIREMENTS

G.5.1 WALE Modem Waveforms.

The WALE waveforms are designed to pass through the audio passband of standard SSB radio equipment.

- The Deep WALE waveform is designed for robust communications in challenging channels.
- The Fast WALE waveform is intended for use when the robustness of Deep WALE is not required.

Either of the waveforms may be used in any transmission, but the same waveform shall be used throughout a transmission. The two waveforms are distinguished by the final four symbols in the preamble (see G.5.1.7.1 and G.5.1.8.2).

G.5.1.1 Error correction coding.

A constraint length 9, rate 1/2 convolutional code shall be applied to the 96 PDU bits, with full tail biting, producing a 192-bit coded block to be interleaved. Figure G-7 depicts the encoder.

Polynomials:
(b0) T1 = $x^8+x^6 + x^5 + x^4 + 1$
(b1) T2 = $x^8+x^7 + x^6 + x^5 + x^3 + x^1+1$

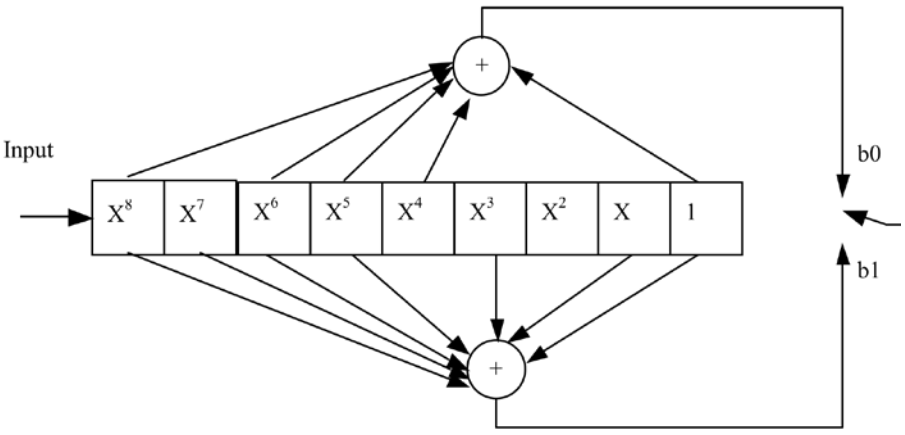


Figure G-7. Constraint length 9, rate 1/2 convolutional encoder.

The two summing nodes in the figure represent modulo 2 additions. For each bit input to the encoder, two bits are taken from the encoder, with the upper output bit b0, generated by polynomial $T_1(x)$, taken first.

To begin encoding each PDU, the encoder shall be preloaded by shifting in the first eight PDU bits without taking any output bits. These eight PDU bits shall be temporarily saved so that they can be used to "flush" the encoder. The first two coded output bits shall be taken after the ninth bit has been shifted in, and shall be defined to be the first two bits of the resulting block code. After the last PDU bit has been encoded, the eight "saved" data bits shall be encoded. Note that the encoder shift register should not be changed before encoding these saved bits; i.e., it should

remain filled with the last nine PDU bits. The eight "saved" PDU bits are encoded by shifting them into the encoder one at a time, beginning with the earliest of the eight. The encoding thus continues by taking the two resulting coded output bits as each of the saved bits is shifted in. These encoded bits shall be the final bits of the resulting block code.

G.5.1.2 Interleaving.

The interleaver shall consist of a single-dimension array, numbered from 0 to 191.
The block code bits shall be loaded into the interleaver array beginning with location 0. The location for loading each successive bit shall be obtained from the previous location by incrementing by 25, modulo 192. Defining the first block code bit to be B(0), then the load location for B(n) is given by:

Load Location = (n * 25) Modulo 192

The bits in the filled interleaver array (A[0] through A[191]) shall be sent to the modulator sequentially: A(0), A(1), and so on.

G.5.1.3 PSK Modulation.

The WALE waveforms employ 8PSK modulation of an 1800 Hz subcarrier at a rate of 2400 PSK symbols per second. The subcarrier frequency and the symbol rate shall be accurate to within 10 ppm. The constellation points used for 8PSK are shown in Figure G-8 and specified in terms of their In-phase and Quadrature components in Table G-V.

Table G-V 8PSK symbol mapping.

Symbol Number	Phase	In-Phase	Quadrature
0	0	1.000000	0.000000
1	$\pi/4$	0.707107	0.707107
2	$\pi/2$	0.000000	1.000000
3	$3\pi/4$	-0.707107	0.707107
4	π	-1.000000	0.000000
5	$5\pi/4$	-0.707107	-0.707107
6	$3\pi/2$	0.0000000	-1.000000
7	$7\pi/4$	0.707107	-0.707107

Note that the complex symbol values = exp[jnπ/4] where n is the symbol number.

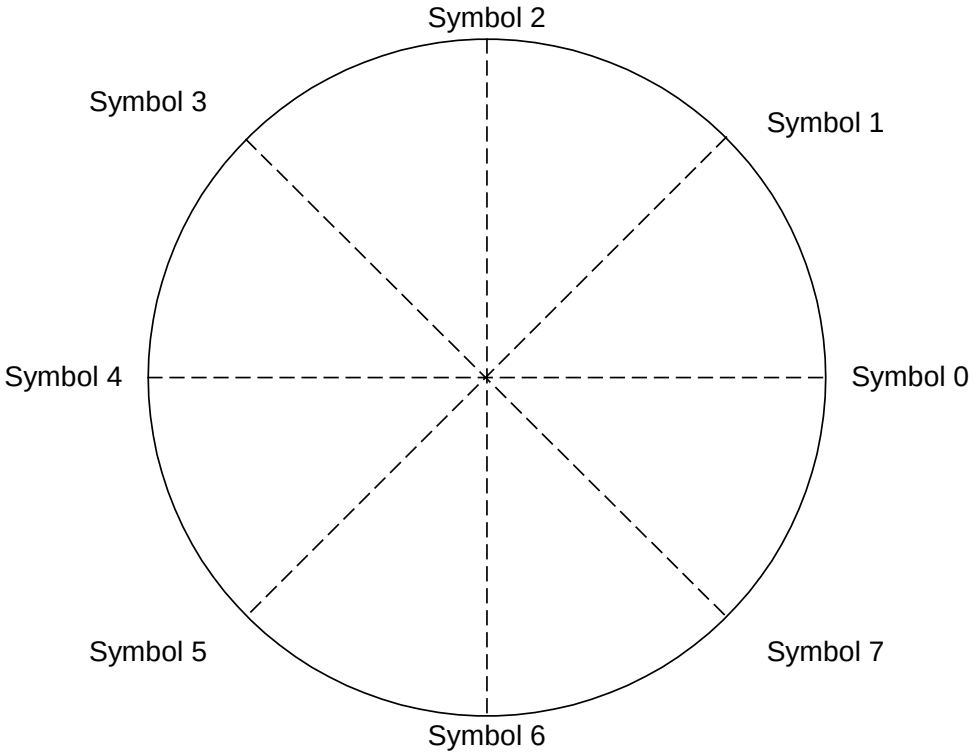


Figure G-8. 8PSK signal constellation and symbol mapping.

G.5.1.4 TLC Section.

The optional first section of a WALE transmission other than asynchronous calls and asynchronous terminations is denoted TLC. The TLC section, comprising zero or more blocks of known symbols, is provided to allow for settling of radio and modem transmitter level control (TLC) and automatic gain control (AGC) circuitry. Each TLC block shall contain 32 8PSK symbols taken sequentially from Table G-VI, starting with `tlc[0]` and wrapping around from the end of the table to the beginning as required.

Table G-VI TLC symbols.

```
int tlc[256] =
{2,4,0,0,6,2,1,4,6,1,0,5,7,3,4,1,2,6,1,7,0,7,3,2,2,2,3,2,4,6,3,6,
 6,3,7,5,4,7,5,6,7,4,0,2,6,1,5,3,0,4,2,4,6,4,5,2,5,4,5,3,1,5,4,5,
 6,5,1,0,7,1,0,1,0,5,3,5,2,2,4,5,4,0,6,4,1,4,0,3,3,0,0,3,3,7,3,4,
 2,7,4,4,4,0,3,4,7,6,4,2,6,2,0,3,5,3,2,2,4,5,2,0,0,3,5,0,3,2,6,6,
 1,4,2,3,6,1,3,0,3,3,2,4,2,2,6,5,5,3,6,7,6,5,6,6,5,2,5,4,2,3,3,3,
 5,7,5,5,3,7,0,4,7,0,4,1,6,2,3,5,5,6,2,6,4,6,3,4,0,7,0,0,5,2,1,5,
 4,3,4,5,7,0,5,3,7,6,6,6,4,5,6,0,2,0,4,2,3,4,4,0,7,6,6,2,0,0,3,3,
 0,5,2,4,2,2,4,5,4,6,6,6,3,2,1,0,3,2,6,0,6,2,4,0,6,4,1,3,3,5,3,6};
```

G.5.1.5 Capture Probe.

The first section of a WALE asynchronous call or termination is called the capture probe. The capture probe comprises repeated blocks of known symbols that will be recognized by scanning receivers so that PUs will stop scanning to receive the following WALE PDU(s). The capture probe is analogous to the scanning call section of 2G or 3G ALE calls. Each capture probe block shall contain the 96 8PSK symbol sequence in Table G-VII, beginning with `capture[0]`.

Table G-VII Capture probe symbols.

```
int capture[96] =
{1,1,4,6,5,5,5,2,4,7,6,7,7,3,3,0,5,5,7,4,2,7,2,5,2,7,2,6,6,6,0,4,
 6,1,0,7,1,2,1,6,3,2,0,2,5,5,2,7,3,1,0,4,7,7,7,7,2,6,5,6,6,7,0,2,
 0,1,2,5,6,1,7,7,4,0,4,7,4,5,4,4,1,4,2,2,2,4,6,7,3,4,5,5,1,0,3,0};
```

G.5.1.6 WALE preambles.

The synchronization preamble is used for rapid initial synchronization and provides time and frequency alignment. 4-ary orthogonal Walsh modulation shall be employed in both the Deep WALE and Fast WALE preambles, using the Walsh sequences in Table G-VIII.
Each di-bit, representing 2 bits of information, is mapped into a 4-element Walsh sequence of symbols 0 and 4 as defined in Table G-VIII.

- The fixed symbols in the preambles shall be mapped using the 4-element “normal set” sequences, repeated 8 times to form 32-chip Walsh sequences.
- The final four preamble symbols shall be mapped using the 8-element “exceptional set” sequences, repeated 4 times to form 32-chip Walsh sequences.

Table G-VIII Walsh Sequences for WALE Preambles

Di-bit	Walsh Sequence
a. Mapping for normal sets	
0 (00)	(0000) repeated 8 times
1 (01)	(0404) repeated 8 times
2 (10)	(0044) repeated 8 times
3 (11)	(0440) repeated 8 times
b. Mapping for exceptional sets.	
0 (00)	(0000 4444) repeated 4 times
1 (01)	(0404 4040) repeated 4 times
2 (10)	(0044 4400) repeated 4 times
3 (11)	(0440 4004) repeated 4 times

Each 32-chip Walsh sequence in a synchronization preamble shall be scrambled by performing a modulo 8 addition between the specified 8-PSK symbol from the sequence below and the corresponding Walsh element.

```
U8 nScramble[32] =
{7,1,1,3,7,3,1,5,5,1,1,6,7,1,5,4,1,7,1,6,3,6,1,0,4,1,0,7,5,5,2,6};
```

G.5.1.7 Deep WALE waveform.

The Deep WALE waveform is designed to set up links in challenging HF channels. Each Deep WALE transmission shall begin with zero or more TLC blocks (G.5.1.4) or a Capture Probe (G.5.1.5) in an asynchronous-mode call, followed by a Deep WALE acquisition preamble (G.5.1.7.1), followed by one or more coded and interleaved WALE PDUs sent using Deep WALE data modulation (G.5.1.7.2).

G.5.1.7.1 Deep WALE preamble.

Deep WALE uses a 240 ms preamble consisting of 18 orthogonal Walsh modulated channel symbols, scrambled IAW G.5.1.6. The first 14 fixed di-bits shall be {0, 1, 2, 1 0, 0, 2, 3, 1, 3, 3, 1, 2, 0}, with 2, 0 being the last two di-bits transmitted. These shall be mapped as normal sets IAW Table G-VIIIa.

The final four di-bits shall be mapped as exceptional sets IAW Table G-VIIIb.

- The first of these di-bits shall be 0, which identifies the Deep WALE waveform.
- The second di-bit shall be 1 if the M bit (G.5.5.1.1) in the first PDU in the transmission is set to 1 (more than one PDU in the transmission); otherwise the second di-bit shall be 0.
- The final two di-bits provide a counter. The di-bits which form this counter shall be C1 and C0, with C0 being the last di-bit sent. C1 shall encode b3 and b2, with b3 being the most significant bit, while C0 encodes b1 and b0 with b0 being the least significant bit. When read as a four bit number, this counter allows for multiple preambles to be sent, with the initial counter value set to the number of preambles minus 1, for up to 16 preambles. The counter decrements by 1 with each preamble transmission, with a value of zero indicating that this is the last preamble in the transmission. If more than 16 preambles are to be sent, the counter value should be set to 15 and not decremented until there are fewer than 15 preambles remaining, so that the counter reaches zero with the final preamble sent.

G.5.1.7.2 Deep WALE data modulation.

When using the Deep WALE waveform, the coded and interleaved PDU bits shall be sent four at a time. Each set of four bits (a “quad-bit”) shall be used to select one of the Walsh sequences in Table G-IX. (The first of the four bits from the interleaver is shown on the left.)
The selected 16-element Walsh sequence is repeated 4 times to yield a 64-element Walsh sequence. For example, if the quad-bit is 0001, the sequence 0404040404040404 is repeated to generate

0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4,
0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4, 0, 4.

Each 64-element channel symbol shall be scrambled using 64 8PSK symbols of a scrambling sequence generated using a 159-bit shift register with a single tap after bit 31. The shift register shall be initialized to the following state for each transmission (and run without re-initialization for all PDUs in a transmission):

```
int bitshift[159] =
{0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1,
 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0,
 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0,
 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1,
 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1,
 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1,
 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0,
 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0,
 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1};
```

The shift register shall be iterated 16 times between the generation of each scrambling symbol:

```
int tri(void)
{
   int bitout, bittap, bitin;
   int i,j;

   for(j=0;j<16;j++)
   {
      bitout = bitshift[158];
      bittap = bitshift[31];
      for(i=158;i>=1;i--) bitshift[i]=bitshift[i-1];
      bitin = bitout^bittap;
      bitshift[0]=bitin;
   }
   return (bitshift[2]<<2)+(bitshift[1]<<1)+bitshift[0];
}
```

Table G-IX Walsh sequences for Deep WALE data block.

Quad-bit	Walsh Sequence
0000	0000000000000000
0001	0404040404040404
0010	0044004400440044
0011	0440044004400440
0100	0000444400004444
0101	0404404004044040
0110	0044440000444400
0111	0440400404404004
1000	0000000044444444
1001	0404040440404040
1010	0044004444004400
1011	0440044040044004
1100	0000444444440000
1101	0404404040400404
1110	0044440044000044
1111	0440400440040440

G.5.1.8 Fast WALE waveform.

The Fast WALE waveform is designed to set up links quickly in relatively benign channels (voice quality or better).

G.5.1.8.1 Fast WALE frame structure.

Each Fast WALE transmission shall begin with zero or more TLC blocks (G.5.1.4), or a Capture Probe (G.5.1.5) in an asynchronous-mode call or termination, followed by the Fast WALE acquisition preamble (G.5.1.8.2), followed by one or more coded and interleaved WALE PDUs sent using Fast WALE data modulation (G.5.1.8.3), as depicted in Figure G-9.

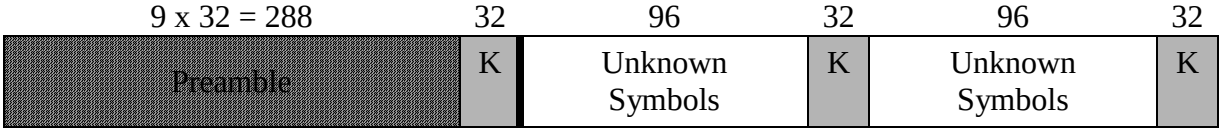


Figure G-9. Fast WALE frame structure.

G.5.1.8.2 Fast WALE preamble.

Fast WALE uses a 120 ms preamble consisting of 9 orthogonal Walsh modulated channel symbols, scrambled IAW G.5.1.6. The first 5 fixed di-bits shall be {3, 3, 1, 2, 0}, with 2, 0 being the last two fixed di-bits transmitted. These shall be mapped as normal sets IAW Table G-VIIIa. The final four di-bits shall be mapped as exceptional sets IAW Table G-VIIIb.

- The first of these di-bits shall be 1, which identifies the Fast WALE waveform.
- The second di-bit shall be 1 if the M bit (G.5.5.1.1) in the first PDU in the transmission is set to 1 (more than one PDU in the transmission); otherwise the second di-bit shall be 0.
- The final two di-bits are unused in Fast WALE, and shall be set to 0.

G.5.1.8.3 Fast WALE data modulation.

The coded and interleaved bits of each WALE PDU shall be sent in alternating blocks of unknown (PDU) symbols and known (probe) symbols as shown in Figure G-9.

G.5.1.8.3.1 Fast WALE probe sequence.

As shown in Figure G-9, a block of known (probe) symbols (labeled K in the figure) shall be sent at the end of the preamble and after each block of 96 coded, interleaved data symbols. Each block of known data shall consist of the following sequence of 16 8PSK symbols, sent twice and without scrambling: {0, 0, 0, 0, 0, 2, 4, 6, 0, 4, 0, 4, 0, 6, 4, 2}.

G.5.1.8.3.2 Fast WALE data symbols.

Each bit of PDU data shall be sent using BPSK, transcoded to 8PSK symbols as shown in Table G-X. The symbols from the table shall be scrambled by modulo 8 addition with a scrambling sequence generated as shown in Figure G-10. The scrambling sequence generator polynomial shall be x^9+x^4+1 and the generator shall be initialized to 1 at the start of each data frame.

Table G-X Transcoding for Fast WALE data symbols

bit	Symbol
0	0
1	4

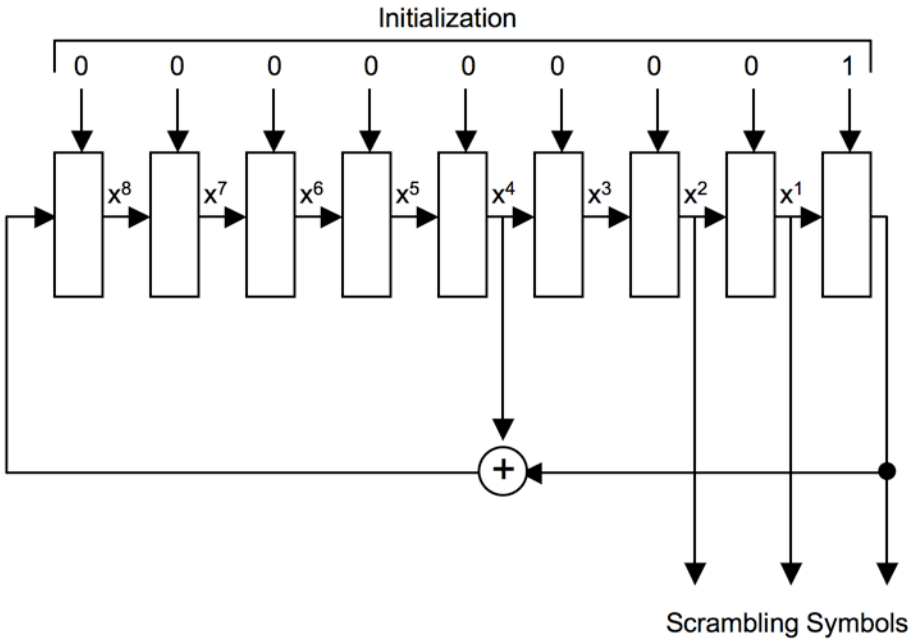


Figure G-10. Scrambling sequence generator for Fast WALE data symbols.

After each data symbol is scrambled, the generator shall be iterated (shifted) 3 times to produce all new bits for use in scrambling the next symbol.

G.5.1.9 Modulation filter.

The transmit waveform shall be spectrally constrained to fall within the specified bandwidth (see MIL-STD-188-141 paragraph 5.2.7.1 “Single-channel SSB or dual-channel (2-ISB) operation in 3 kHz channels”).

A square root of raised cosine filter is recommended with a roll-off factor (excess bandwidth) of 35%. Utilizing this filter as both the modem modulation filter and demodulation filter will maximize the signal to noise ratio and minimize inter-symbol interference. The combined modulation and demodulation filters will have the following frequency response (symmetric around 0 Hz):

$H(f) = 1 \quad \text{for } |f| <= f_n - pf_n$
$H(f) = 0.5(1 - \sin(f-f_n * PI / 2pf_n) \quad \text{for } f_n - pf_n < |f| <= f_n + pf_n$
$H(f) = 0 \quad \text{elsewhere}$

Where:

f_n is the Nyquist frequency ($f_n = 1 / (2T)$ = (1 / 2) * SYMBOL RATE = 1200 Hz)
p is the roll-off factor or excess bandwidth.

The individual modulation and demodulation filters are realized by taking the square root of the above frequency response.

G.5.2 WALE PDU.

The protocol data units (PDUs) used in all 4G protocols have the generic format shown in Figure G-11. The Protocol and CRC fields are specified here. The remaining fields shall be used IAW the specific protocol indicated in the Reference column of Table G-XI.

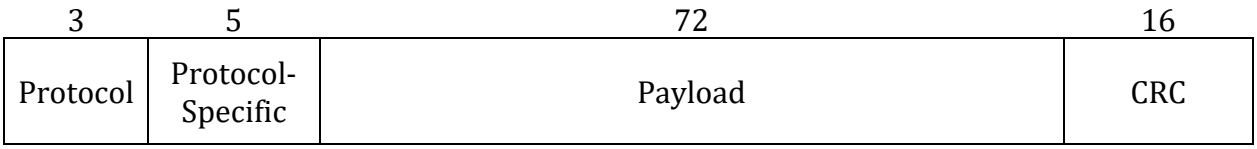


Figure G-11. 4G PDU Structure

PDUs may be sent using either of the WALE waveforms. The octets of the PDU shall be sent in the order shown in the figure for that specific PDU (see for example Figure G-13). In each figure, the octets shall be sent in top to bottom order, and the bits in each octet shall be sent in right to left order (least-significant bit first).

G.5.2.1 WALE PDU Protocol Field.

The Protocol field shall be used as indicated in Table G-XI.

Table G-XI 4G PDU Protocol Field

Protocol Field	Protocol	Reference
000	Text Message	G.5.6.3
001	Binary Message	G.5.6.4
010	Link Setup	G.5.5
011	Utility PDUs	G.5.6.2 and G.5.7
All others	(Reserved. Do not use.)	—

G.5.2.2 WALE PDU Cyclic Redundancy Check.

The CRC field shall contain a 16-bit cyclic redundancy check (CRC) code computed using the polynomial $x^{16} + x^{15} + x^{12} + x^{11} + x^8 + x^6 + x^3 + 1$. When calculating this CRC using the shift register method, the shift register shall be initialized to all 1s, and the CRC shall be inverted before transmission.

The CRC bits shall be mapped into the CRC octets in PDUs by placing the MSB of the CRC into the LSB of the first octet of the CRC field, and the LSB of the CRC into the MSB of the last octet of the CRC field. This will result in the MSB of the most significant byte of the CRC being sent first, followed by the remaining bits in descending order.

The following C code (from STANAG 5066) can be used to calculate the CRC value using the specified polynomial. This code calculates the CRC bytes in the proper order for transmission as defined above; no bit reversal is required with this code.

```
unsigned short
CRC_16_S5066(unsigned char DATA, unsigned short CRC) {
  unsigned char i, bit;
  for (i=0x01; i; i<<=1) {
    bit = (((CRC & 0x0001) ? 1:0)^((DATA&i) ? 1:0));
    CRC>>=1;
    if (bit) CRC^=0x9299;
  }
  return (CRC);
}
```

This function is called to update a running CRC for each octet of the WALE PDU. The first argument is the new octet and the second argument is the running CRC. An example of usage is as follows:

```
#define NUM_OCTETS 10  /* octets in PDU preceding CRC */
unsigned char message[NUM_OCTETS]; unsigned short CRC_result;
unsigned int j;
CRC_result = 0xffff;
for (j=0; j < NUM_OCTETS; j++){
  CRC_result = CRC_16_S5066(message[j], CRC_result);
}
CRC_result ^= 0xffff;
/* CRC_result contains final CRC value */
```

G.5.3 WALE addresses.

Addresses in WALE PDUs are 16-bit binary numbers that designate individual PUs and multipoint groups.

In NATO applications, a 16-bit network number is associated with each individual or multipoint address. Network numbers are not sent explicitly, but shall be combined with WALE PDUs through the Linking Protection process (G.5.7.3.2) as shown in Figure G-12. The network number portion of the address of called PU(s) is replicated to match the width of the key variable used for linking protection.

Denoting the most-significant bit of the network number as N_0 and the most-significant bit of the key as K_0, the next-most-significant bits as N_1 and K_1, and so on, each bit of key K_i is paired with bit $N_{i \bmod 16}$. The key variable KV actually used to encrypt and decrypt WALE PDUs is the result of adding the paired bits modulo-2: $KV_i = K_i +_2 N_{i \bmod 16}$

Note that the network number of the *called* station is used in all transmissions of the link setup handshake.

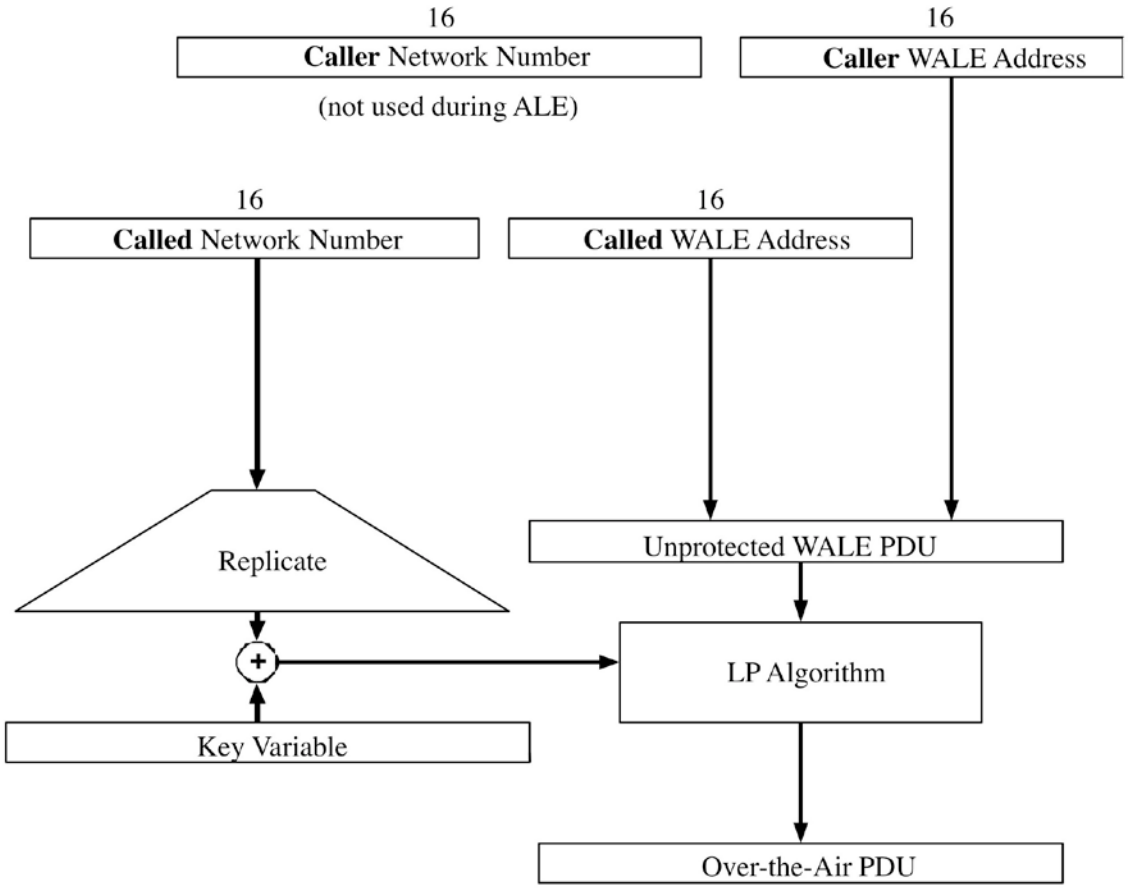


Figure G-12. NATO-Mode Addressing.

G.5.4 Channel Selection.

WALE sets up wideband channels in two steps. Just as in previous generations of ALE, initial contact between unlinked PUs employs a handshake on a 3-kHz channel (a "calling" or "ALE" channel). During this handshake, PUs are able to negotiate a wider channel as appropriate for traffic (a "traffic" channel). After this handshake, traffic commences in the wideband channel.

G.5.4.1 Calling Channel Selection.

The Automatic Channel Selection (ACS) function determines which of the available channels in a network will be used by a PU for calling one or more distant PUs. The ACS function should select channels in a fashion that optimizes overall network performance. This is achieved by using all available information as to propagation and occupancy of each channel and the requirements of the traffic to be supported. Such information may be available from propagation prediction programs, channel measurements made during scanning and traffic (LQA data in the Other Station Table, G.4.2.3), and measurements from external systems.

G.5.4.2 Traffic Channel Negotiation.

The procedure for negotiating a wideband traffic channel is specified in G.5.5.3.

G.5.5 Link Setup Protocols.

The protocols in this section shall be used to set up and manage links.

G.5.5.1 Link setup PDUs.
PDUs used in the link setup protocols are shown in Figure G-13 through Figure G-17. The specific PDU types shown (Request, Confirm, etc.) shall be used as specified in the protocol specifications in the following paragraphs. The fields shown in these figures are described in the following paragraphs.

The octets of each PDU shall be sent in top-to-bottom order, with bit 0 of each octet sent first (right-to-left order).

	7 6 5 4 3 2 1 0
LSU_Req	0 1 0 | 0 0 0 | V M
	Traf Type | EC
Caller Address	MSB – – – – – – – – – – – – – – – – LSB
Called Address	MSB – – – – – – – – – – – – – – – – LSB
Assigned Sub-channels	bin 15 – – – – – – – – – – – – – – – – bin 0
Occupied Sub-channels	bin 15 – – – – – – – – – – – – – – – – bin 0
CRC	– – – – – – – – MSB LSB – – – – – – – –

Figure G-13. Link Setup Request (2-way) PDU

	7	6	5	4	3	2	1	0
LSU_Conf	0	1	0	0	0	1	V	M
	SNR						EC	
Caller Address	MSB – – – – – – – –							
	– – – – – – – – LSB							
Called Address	MSB – – – – – – – –							
	– – – – – – – – LSB							
Tx Sub-channels	bin 15 – – – – – – – –							
	– – – – – – – – bin 0							
Rx Sub-channels	bin 15 – – – – – – – –							
	– – – – – – – – bin 0							
CRC	– – – – – – – – MSB							
	LSB – – – – – – – –							

Figure G-14. Link Setup Confirm PDU

	7	6	5	4	3	2	1	0
LSU_Term	0	1	0	0	1	0	V	M
	Reason						0	0
Caller Address	MSB – – – – – – – –							
	– – – – – – – – LSB							
Called Address	MSB – – – – – – – –							
	– – – – – – – – LSB							
(spare: do not use)	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
CRC	– – – – – – – – MSB							
	LSB – – – – – – – –							

Figure G-15. Link Terminate PDU

	7	6	5	4	3	2	1	0
LSU_Req1	0	1	0	1	0	0	V	M
	Traf Type						EC	
Caller Address	MSB – – – – – – – – – – – – – – – – LSB							
Called Address	MSB – – – – – – – – – – – – – – – – LSB							
Tx Sub-channels	bin 15 – – – – – – – – – – – – – – – – bin 0							
(spare: do not use)	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
CRC	– – – – – – – – MSB LSB – – – – – – – –							

Figure G-16. Link Setup Request (1-way) PDU

	7	6	5	4	3	2	1	0
LSU_Status	0	1	0	1	1	1	V	M
	Status						EC	
Caller Address	MSB – – – – – – – – – – – – – – – – LSB							
Count	MSB – – – – – – – – LSB							
(spare: do not use)	0	0	0	0	0	0	0	0
Assigned Sub-channels	bin 15 – – – – – – – – – – – – – – – – bin 0							
(spare: do not use)	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
CRC	– – – – – – – – MSB LSB – – – – – – – –							

Figure G-17. Sounding and Status Report PDU

G.5.5.1.1 VM Field.

The most-significant bit in the VM field is the “V” bit. It shall be set to 1 to indicate that the PU sending this PDU is operating in override mode (G.4.1.6).

The least-significant bit in the VM field is the “M” bit. It shall be set to 1 to indicate that additional PDUs follow this PDU in the transmission. If this PDU is the last in a transmission, the M bit shall be set to 0.

G.5.5.1.2 Traffic Type Field.

The Traffic Type field (shown as Traf Type) shall be used in link setup requests to indicate the type of traffic that the caller will send on the link after it is set up. This field shall use the codes in Table G-XII.

Table G-XII Traffic Type Codes.

Traf Type	Traffic Type
0	No traffic to send
1	Analog voice
2	Low-latency, fixed-rate 600 bps
3	Low-latency, fixed-rate 1200 bps
4	Low-latency, fixed-rate 2400 bps
5	Best throughput (accepts some errors)
6	Low error rate
7…15	Reserved. Do not use.
16	STANAG 4415 (auto-detect interleaver size)
17	STANAG 4539 (3 kHz only; auto-detect rate & interleaver)
18	STANAG 5069 (wideband; auto-detect rate and interleaver)
19…23	Reserved. Do not use.
24	Adaptive-rate data ≥ 19.2 kbps
25	Adaptive-rate data ≥ 38.4 kbps
26	Adaptive-rate data ≥ 50 kbps
27	Adaptive-rate data ≥ 64 kbps
28 … 50	Reserved. Do not use.
51 … 60	Reserved for vendor use (non-interoperable)
61	Sync check (see G.5.7.5)
62	LQA Exchange (see G.5.5.10.2)
63	TOD (see G.5.7.4)

G.5.5.1.3 EC Field.

The Equipment Capability field (shown as EC) shall be used to indicate the wideband capabilities of the radio equipment at the PU sending the PDU. This field shall use the codes in Table G-XIII.

Table G-XIII Equipment Capability Codes.

EC Code	Equipment Capability	MIL-STD-188-110 Appendix D Equivalent
00	3 kHz only	Block 1
01	Up to 12 kHz	Block 2
10	Up to 24 kHz	Block 3
11	Up to 48 kHz	—

G.5.5.1.4 Addresses.

Addresses in WALE PDUs are 16-bit binary numbers. See G.5.3.

G.5.5.1.5 PDU sub-channel vectors.
Four types of sub-channel vectors (see G.4.2.1.2) are sent in WALE PDUs.

G.5.5.1.5.1 Assigned sub-channels vector.
An Assigned Sub-channels vector is carried in a link setup request PDU or a status PDU. It shall indicate those sub-channels that the calling PU is authorized to use for transmitting (from the channel record for the calling channel). Each element in the vector is one bit. A value of 1 shall indicate an assigned sub-channel, while a 0 indicates that the sub-channel is not assigned.

G.5.5.1.5.2 Occupied sub-channels vector.
An Occupied Sub-channels vector is carried in a link setup request PDU. It shall indicate those sub-channels that the calling PU has determined are occupied (G.4.3.2) at the time of sending the link setup request. Each element in the vector is one bit. A value of 1 shall indicate an occupied sub-channel, while a 0 indicates that the sub-channel is not occupied.

G.5.5.1.5.3 Tx sub-channels vector.
A Tx sub-channels vector is carried in a link setup confirm PDU or a 1-way link setup request, and indicates those sub-channels on which the PU is prepared to transmit. The bit for each sub-channel shall be set to 1 if that sub-channel is assigned and either is not occupied (G.4.3.2) or the override mode is set. Otherwise the bit shall be set to 0.

G.5.5.1.5.4 Rx sub-channels vector.
An Rx sub-channels vector is carried in a link setup confirm PDU. The bit for each sub-channel shall be set to 1 if the confirming PU wishes to include that sub-channel in the wideband channel on which it will receive traffic; otherwise the bit shall be set to 0. In selecting sub-channels for receiving, the confirming PU should consider the traffic type to be carried on the traffic channel, the SNR measured during reception of the most recent WALE PDU from the other PU, and the noise and interference that it has measured on that sub-channel.

G.5.5.1.6 SNR Field.

The SNR field in a LSU_Conf PDU shall indicate the 3 kHz SNR measured during reception of the most recent WALE PDU from the other PU. The numerical value shall indicate the SNR in dB, encoded as follows:

SNR field value = measured SNR (in dB) + 10 (dB)

A measured SNR less than -10 dB shall be encoded as 0, and SNR greater than 53 dB shall be encoded as 63.

G.5.5.1.7 Reason Field.

The Reason field shall be used to indicate the reason for sending a LSU_Term PDU. This field shall use the codes in Table G-XIV

Table G-XIV Reason Codes.

Reason Code	Meaning
000000	NO_MORE_TRAFFIC
000001	NO_RESPONSE
000010	NOT_EQUIPPED
000011	RELINK
000100	PREEMPTED
1xxxxx	Reserved for vendor use (non-interoperable)
(all others)	(Reserved. Do not use.)

G.5.5.1.8 Status Field.

The Status field shall be used to indicate the radio status of the PU sending the PDU *that will prevail after the current transmission*. This field shall use the codes in Table G-XV

Table G-XV Status Codes.

Status Code	PU Status
000000	Off
000001	Receive only (e.g., EMCON)
000011	Normal status
1xxxxx	Reserved for vendor use (non-interoperable)
(all others)	(Reserved. Do not use.)

G.5.5.2 Basic WALE Handshake.
Using the WALE protocol, PUs set up a link via a handshake on a 3 kHz ALE channel. The general procedure is described here. Requirements for specific applications of the WALE link setup procedure are specified in the following sections. Timing requirements are in G.5.5.11.
The WALE link setup procedure is as follows:

1. After the ACS function has selected a calling channel, the calling PU shall determine whether the ALE channel is occupied, and how much of the assigned frequency band associated with that ALE channel can be used for traffic. The PU shall listen on the assigned frequency band for a period of time specified below for the specific application, except that a staring PU that is aware of channel occupancy does not require a listen-before-transmit (LBT) time.
2. If the ALE channel is occupied, the calling attempt fails on this channel (another channel may be selected to try again). If the ALE channel is unoccupied, the caller shall send a LSU_Req PDU that identifies the calling and called PUs, the spectrum available to the caller (sub-channel vectors), the caller's EC, and the type of traffic it wants to send.
3. A called PU shall evaluate the interference characteristics of its assigned frequency band associated with the ALE channel. The PU shall listen on the assigned frequency band for a period of time specified below for the specific application, except that a staring PU that is aware of channel occupancy does not require a listen-before-responding (LBR) time.
4. If the called PU finds the ALE channel to be unoccupied, it shall respond with a LSU_Conf PDU, which includes its EC, Tx and Rx sub-channel vectors, and the SNR measured on the received transmission. Otherwise it shall make no response.
5. If either PU does not receive a timely response to its PDU, the linking attempt has failed on this channel and that PU shall send one or more LSU_Term PDUs to terminate the linking attempt, as specified below for the specific application. Likewise, if the caller determines that too few sub-channels are available, it shall terminate the call.

G.5.5.3 Wideband traffic channel negotiation.

G.5.5.3.1 Two-way traffic channel negotiation.

After completing a two-way handshake, the PUs shall compute the traffic channel for each direction of the link as follows:

For each sub-channel, compute the usability in each direction as follows:

$$Usable_{CallerToResponder} = (Assigned_{Caller} \text{ AND } ((\text{NOT } Occupied_{Caller}) \text{ OR } Override_{Caller})) \text{ AND } RX_{Responder}$$

$$Usable_{ResponderToCaller} = TX_{Responder} \text{ AND } (\text{NOT } Occupied_{Caller})$$

The traffic channel in each direction shall be the widest contiguous usable range that is an integer multiple of 3 kHz. If more than one such range is available, the lowest-frequency such range shall be used.

An example is shown in Figure G-18. Both PUs are 48 kHz-capable. In this example, override mode is not used, so any interference at either PU constrains spectrum use in both directions.

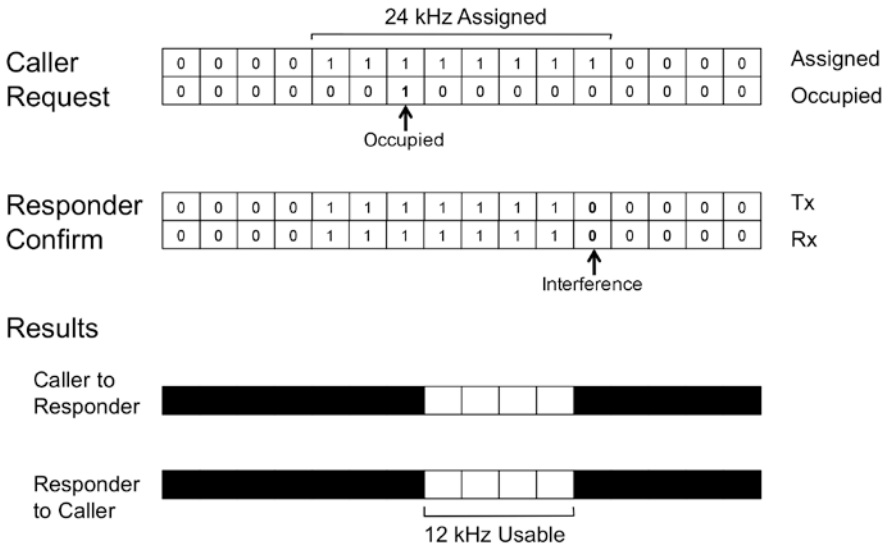


Figure G-18. Example Computation of Traffic Channel: 2-Way, No Override

G.5.5.3.2 Three-way traffic channel negotiation.

When sending a link setup request, the caller is able to measure occupancy in its assigned sub-channels, but will not generally know whether the signal from the other PU will be strong enough to overcome low-level local interference in some sub-channels. However, after measuring the SNR of the LSU_Conf PDU, the caller may compute that there will be adequate SNR on sub-channel(s) that it initially reported as occupied. In such a case, the calling PU should send a Caller Confirm PDU with Rx sub-channel vector bits set to indicate the wider available traffic channel from responder to caller, as shown in Figure G-19.

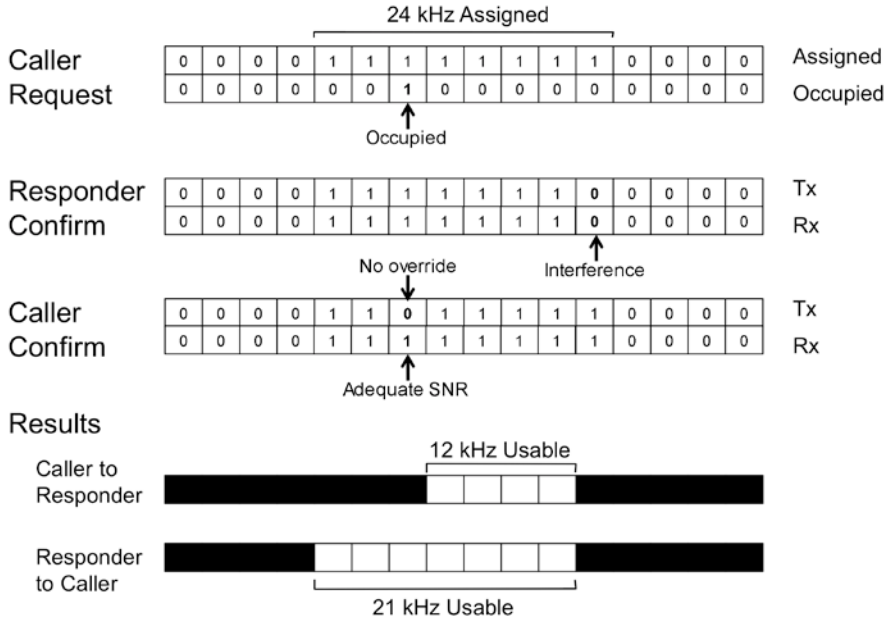


Figure G-19. Example Computation of Traffic Channel: 3-Way, No Override

After completing a three-way handshake, the PUs shall compute the traffic channel for each direction of the link as follows:

For each sub-channel, compute the usability in each direction as follows:

$$Usable_{CallerToResponder} = TX_{Caller} \text{ AND } RX_{Responder}$$
$$Usable_{ResponderToCaller} = TX_{Responder} \text{ AND } RX_{Caller}$$

Just as in the case of a two-way handshake, the traffic channel in each direction shall be the widest contiguous usable range that is an integer multiple of 3 kHz. If more than one such range is available, the lowest-frequency such range shall be used.

G.5.5.3.3 Traffic channel negotiation with override.

Use of override mode is illustrated in Figure G-20. Under the same interference conditions as above, the ability to override local interference for transmitting results (after a two-way handshake) in a 21 kHz channel from the caller to the responder, and a 15 kHz channel in the other direction.

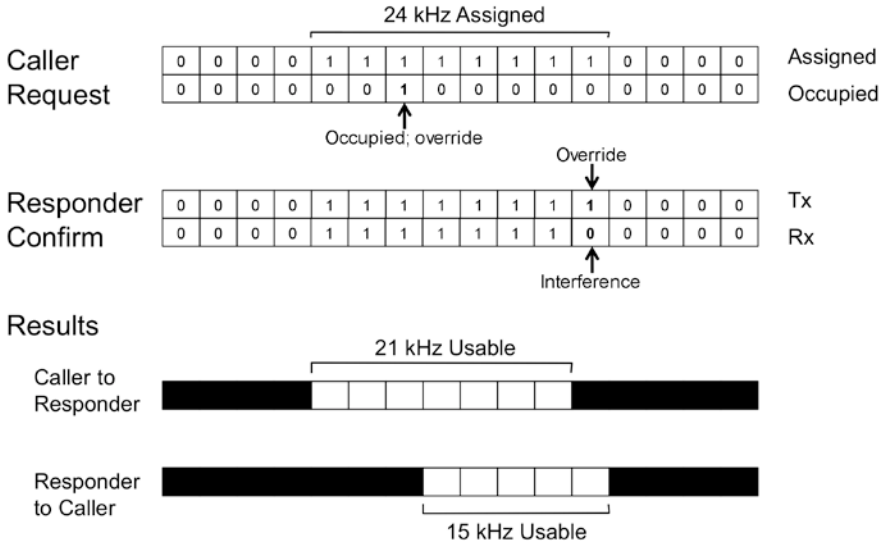


Figure G-20. Example Computation of Traffic Channel: 2-Way, With Override

G.5.5.4 Synchronous two-way point-to-point link setup.
This protocol shall be used to set up a point-to-point (PTP) link in a network of PUs that are scanning synchronously.

G.5.5.4.1 Synchronous two-way point-to-point link setup protocol.
Given the channel on which the call is to be placed, the calling PU shall check that channel for occupancy just before the called station will dwell on that channel (for example, starting at time T–D, where D is the synchronous dwell time), and shall send a LSU_Req PDU in dwell T if the channel is unoccupied.

When operating synchronously, PUs shall send link setup Request PDUs such that the transmission begins $T_{TxOffsetTLC}$ seconds after the beginning of a dwell time (G.5.5.11.1).

If the called PU receives the LSU_Req, it shall do the following:

- record the SNR of that received signal and measure the level of interference of at least those sub-channels that are indicated as Assigned to the caller in the LSU_Req.
- transmit a LSU_Conf starting after a delay of $T_{Confirm}$ after the end of the LSU_Req PDU (G.5.5.11.3).
-

If the calling PU does not receive a LSU_Conf within a timeout of $t_{response} + t_{tune}$ after the end of its LSU_Req PDU, it shall send a LSU_Term(NO_RESPONSE) and return to scanning.

If the called PU has sent a LSU_Conf but no WALE PDUs have arrived and traffic has not commenced within time $t_{traffic}$ after the end of that PDU, the called PU shall send a LSU_Term (NO_RESPONSE) PDU and return to scanning.

G.5.5.4.2 Synchronous two-way point-to-point link setup example.

Beginning at the top left corner, Figure G-21 shows that all PUs in the net synchronously scan the assigned frequencies. During the dwell on frequency 4, a PU is directed to establish a Point-To-Point link with a specific PU on frequency 3 (“F3”). The caller PU continues scanning until LBT time prior to the net PUs dwelling on the desired calling frequency. During this period the caller is still available to respond to higher and equal priority received calls. If this takes place, then the original intended call is deferred. Otherwise, at the end of the period the caller PU skips to Frequency 3, executing a Listen Before Transmit (LBT) process to assure that the channel is unoccupied, and to perform wideband spectrum sensing. The remaining PUs will continue scanning synchronously until they come upon frequency 3.

Note that if the service request specifying F3 was issued just prior to the normal F3 dwell, LBT is not possible during the current scan cycle and the call would have to be delayed until the next scan cycle. However, if the PU has occupancy measurements for this channel from (at least) the preceding scan cycle, the PU may use that occupancy data in place of a current LBT measurement and call immediately.

During the Frequency 3 time slot, the caller PU issues a LSU_Req PDU which conveys the caller PU address, called PU address, traffic type, and locally available sub-channels. All stations in the net will stop scanning if they detect the transmitted preamble. All but the called PDU are free to continue scanning after finding that the called address in the PDU does not refer to them. The called PDU stays on Frequency 3 and performs a listen before response (LBR) to perform wideband spectrum sensing. Then the called PU responds with a LSU_Conf PDU, indicating the ability to continue with the requested traffic service.
After a link inactivity timeout occurs, or upon command by a user process, the link is terminated with a LSU_Term PDU. After terminating the link, both the caller and called rejoin the other net members in synchronous scanning.

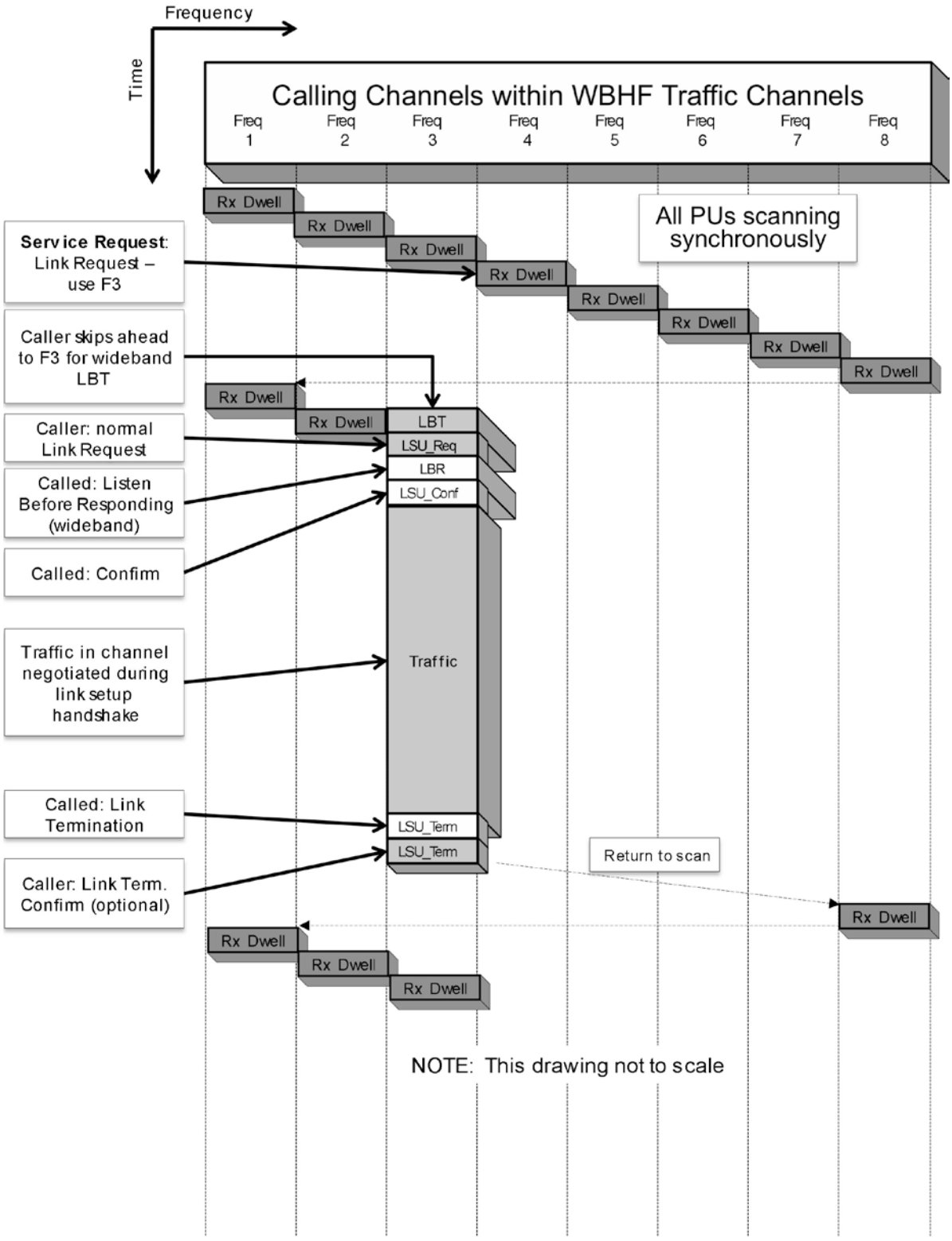


Figure G-21. Synchronous two-way point-to-point link setup example.

G.5.5.5 Asynchronous two-way point-to-point link setup.

The asynchronous two-way point-to-point link setup protocol is used to set up a link between two PUs when one or both of them is scanning asynchronously.

G.5.5.5.1 Asynchronous two-way point-to-point link setup protocol.

The asynchronous two-way point-to-point link setup protocol is the same as the synchronous two-way point-to-point link setup protocol (G.5.5.4.1) except for the following:

a. the LSU_Req may be transmitted at any time.

b. the LSU_Req shall be preceded by a "capture probe" whose duration is as follows:
$t_{capture} \geq d_{min} * (C+2)$
where d_{min} is the asynchronous-mode minimum dwell time INP
and C is the number of channels in the scan set.

The capture probe waveform is specified in G.5.1.5, consisting of 40 ms known-data sequences.

The appropriate preamble for the waveform in use shall immediately follow the capture probe, and shall be followed in turn by the LSU_Req PDU.

In asynchronous-mode networks, a capture probe should also precede link termination transmissions.

G.5.5.5.2 Asynchronous two-way point-to-point link setup example.

Figure G-22 shows an asynchronous call. An unsynchronised calling PU scans the allocated frequencies using the required dwell time; however, it is assumed that it is not scanning synchronously relative to the other net members.

The asynchronous call begins with the LBT, followed by the transmission of the capture probe elements followed by the PDU on the requested link frequency. The probe duration guarantees that all other scanning PUs will scan the calling channel during the async call, even under the worst case time of day offset conditions.

Called PU(s) that receive the capture probe stop scanning and wait for the LSU_Req PDU. After receiving a valid LSU_Req PDU, the addressed PU responds normally with the LSU_Conf PDU and the other PUs return to scanning.

All subsequent elements of the LSU protocol are identical to the synchronous case.

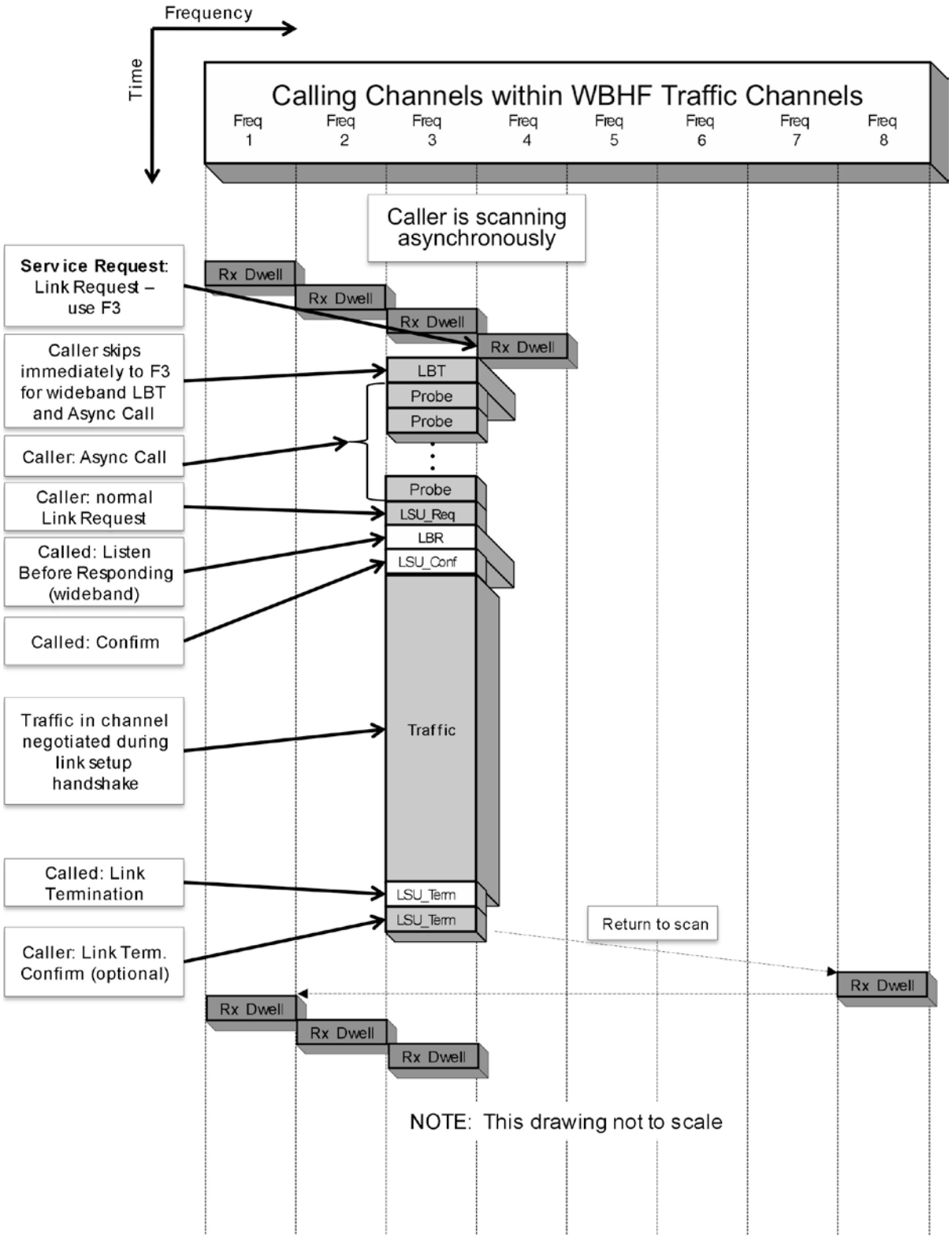


Figure G-22. Asynchronous two-way point-to-point link setup example.

G.5.5.6 Staring link setup (optional).

Staring is an alternative to scanning, in which receivers simultaneously and continuously monitor assigned channels for calls, as well as continuously recording the occupancy of entire wideband channels. Such receivers do not scan, either synchronously or asynchronously. This eliminates various delays that are inherent in *scanning* ALE systems:

- Asynchronous networks require a scanning call (or capture probe) long enough to capture scanning receiver(s).
- In synchronous networks, the call can be short, but it can't be sent until the desired receiver is listening on the selected channel.
- In either case, an LBT interval is required before placing the call because the calling station is usually not aware of current channel occupancy.
- WALE Confirm PDUs require current knowledge of the occupancy of wideband channels, so responding PUs that scan need an LBR period to collect the current channel state.

Staring PUs with continuous knowledge of channel state and that are simultaneously listening on all channels can eliminate all of these delays and thus set up links more quickly.

G.5.5.6.1 Staring link setup protocols.

The staring link setup protocols are identical to the corresponding synchronous link setup protocols, with the elimination of LBT and LBR periods, and with no need for synchronization.

G.5.5.6.2 Staring point-to-point link setup example.

The scenario in Figure G-23 shows a network of staring stations that continuously and simultaneously monitor eight channels. Because the PUs are continually aware of occupancy of those channels, there is no need for LBT or LBR periods, so when a Service Request is presented that requests a link on Frequency 3, the caller immediately tunes and sends the LSU_Req. The called PU immediately tunes and sends its LSU_Conf, followed by the startup of traffic.

G.5.5.7 3G wideband link setup (for information only).

It is possible to set up a narrowband link using 3G FLSU (IAW STANAG 4538), and then to negotiate a wideband channel for traffic via a second handshake that uses 3GWB extensions to the FLSU protocol, as shown in Figure G-24. The extensions for this 3GWB mode are not standardized here.

Networks that use both 4G and 3GWB should scan at the 3G rate, using SDS = 1 (Table G-I).

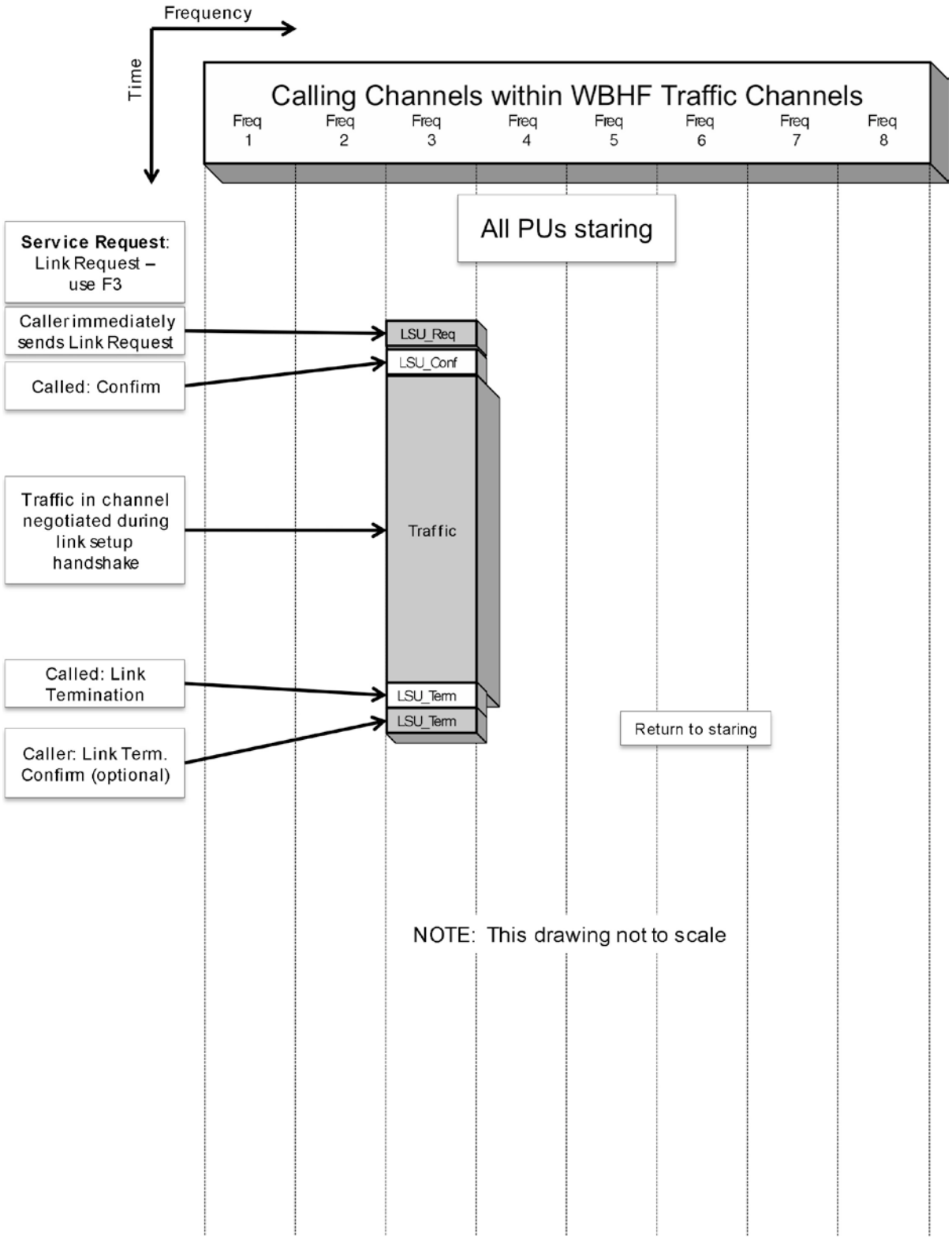


Figure G-23. Staring point-to-point link setup example.

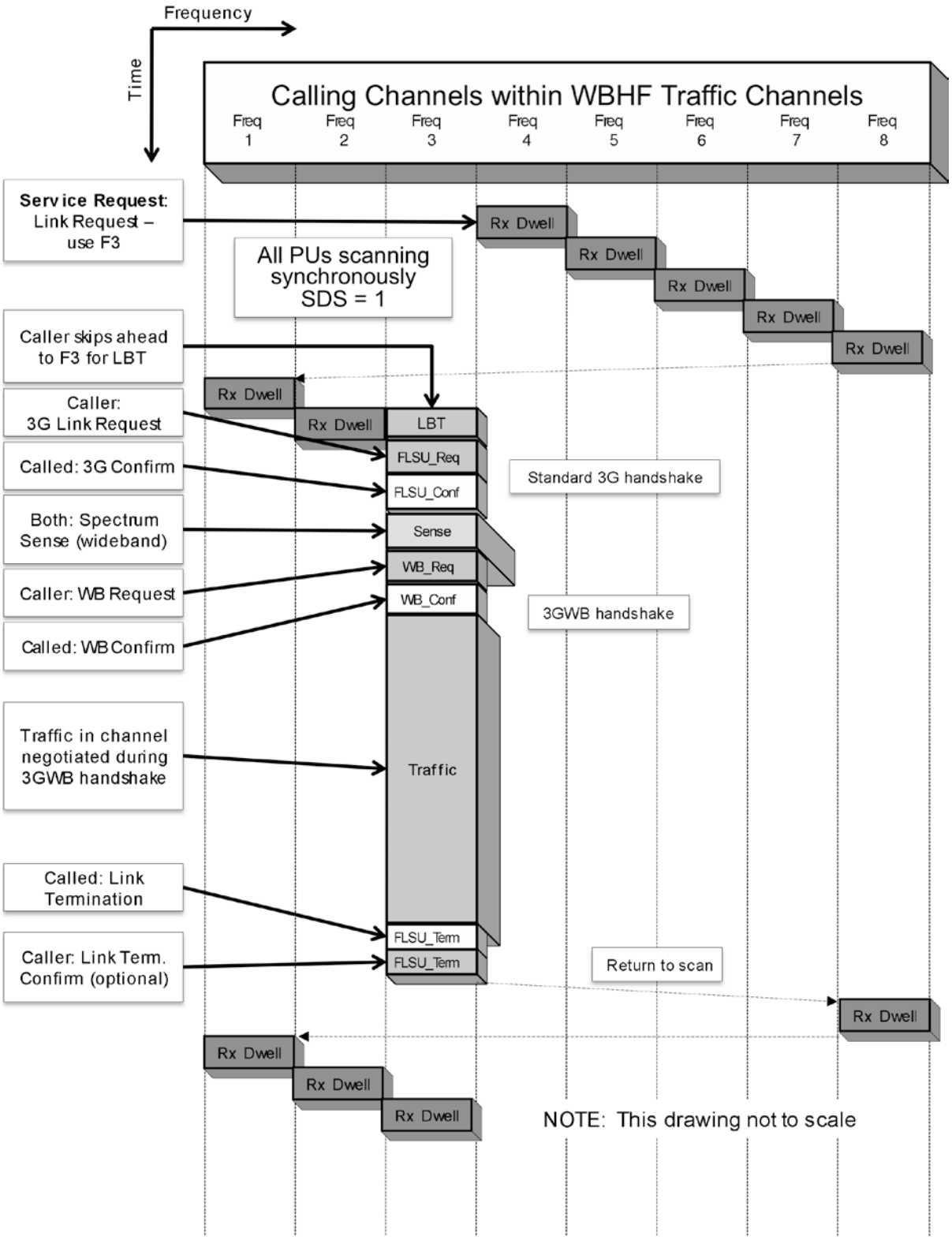


Figure G-24. 3G wideband point-to-point link setup example.

G.5.5.8 Point-to-multipoint link setup.

Point-to-multipoint (PTM) link setup supports the establishment of one-to-many links among pre-programmed collections of PUs. (This is analogous to the Net call in 2G ALE in Appendix A.) A PTM call uses the same request PDU (1-way or 2-way) as a point-to-point call. PUs shall recognize the PTM call by the presence of a pre-programmed multipoint Called Address. Called PUs shall listen before responding during a common LBR period that immediately follows the LSU_Req. Each called PU shall then respond in a pre-programmed slot with its LSU_Conf PDU. The LSU_Conf PDU shall be sent using the same waveform (Fast WALE or Deep WALE) as was used in the LSU_Req, and shall contain the Called PU individual address. The calling PU shall determine the traffic channel to be used, considering the Interference Reports received, and shall send a LSU_Conf PDU that specifies the traffic channel.
If a multipoint or broadcast Called Address is used in a One-way Request PDU (see G.5.5.9), the called PUs shall not respond, but shall silently enter the PTM link and shall listen on the traffic channel designated in the Tx sub-channels vector of the LSU_Req1 PDU.

G.5.5.8.1 Synchronous point-to-multipoint link setup protocol.

The synchronous PTM link setup protocol timing following the LSU_Req PDU shall be as follows:

a. LBR shall occur during the first full dwell that immediately follows the LSU_Req.

b. Called PU response slots shall commence at the slot boundary following LBR. Slot durations for Fast WALE shall be 450 ms. Slot durations for Deep WALE shall be 1.8 s.

G.5.5.8.2 Synchronous point-to-multipoint link setup example.

The PTM scenario in Figure G-25 is identical to the PTP scenario until the slotted responses begin. Within the LSU_Req, the caller address is the address of the caller, and the called PU address is a multipoint address (addresses a group of PUs within the network). This type of call demands that the called PUs respond sequentially (as in a roll-call) in an order specified by their PU address. Each PU responds with an LSU_Conf PDU during its allocated time slot.
Any PU can issue a Terminate (link) PDU, announcing its departure from the link. If the caller PU issues a sequence of Terminate PDUs, using the multipoint address, all stations should return to scan mode (this may follow a confirmation of link termination by each station, if invoked.

G.5.5.8.3 Asynchronous point-to-multipoint link setup protocol.

Asynchronous PTM link setup shall begin with a capture probe, as in asynchronous PTP link setup. Timing of an asynchronous PTM call following the LSU_Req PDU shall be as follows:

a. LBR shall occupy t_{LBR} s (from the LBR INP) immediately following the LSU_Req.

b. Called PU response slots shall commence at the end of the LBR period. Slot durations for Fast WALE shall be 450 ms, and 1.8 s for Deep WALE.

G.5.5.8.4 Asynchronous point-to-multipoint link setup example.

An asynchronous PTM link setup is illustrated in Figure G-26.

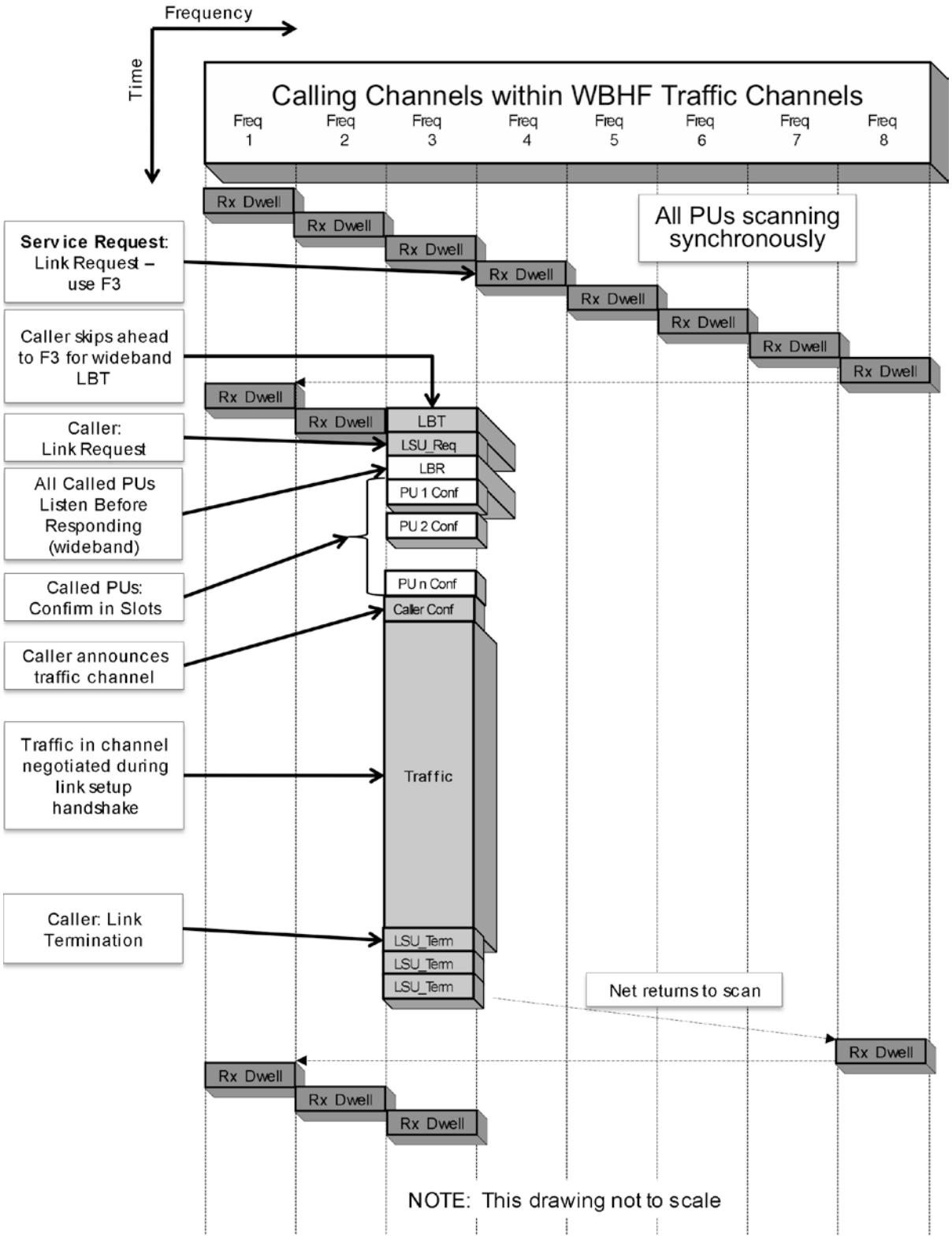


Figure G-25. Synchronous point-to-multipoint link setup example.

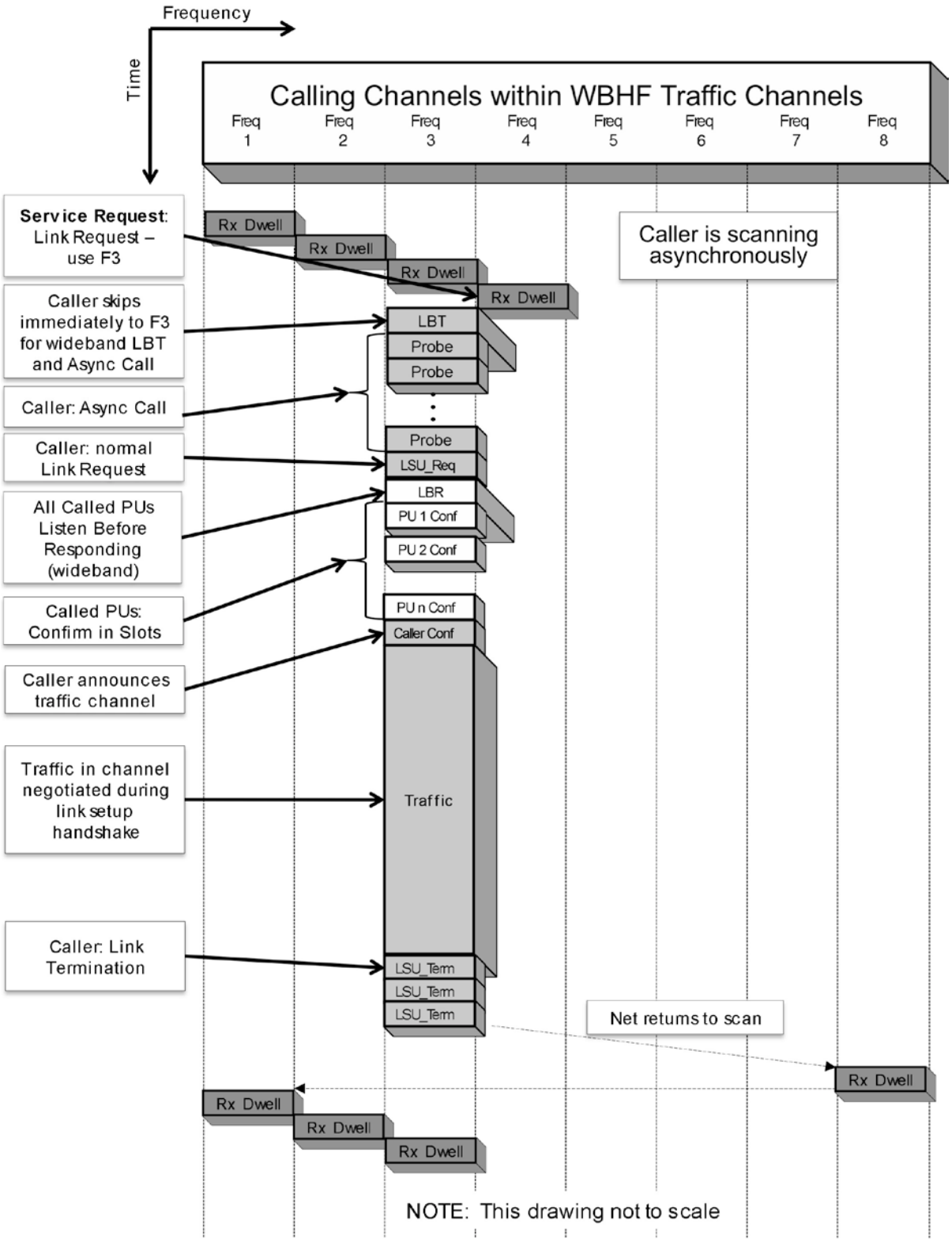


Figure G-26. Asynchronous point-to-multipoint link setup example.

G.5.5.9 One-way link setup.

The one-way link setup protocol may be used by a PU to set up a PTP link, a PTM link, or a broadcast. Following LBT, the calling PU shall transmit a LSU_Req1 PDU that carries its own Caller Address. An all-1's Called address indicates a broadcast call, and all PUs that receive a broadcast call shall enter the link unless programmed to ignore broadcasts. Other Called addresses select either an individual PU or a multicast group of PUs. Called PUs shall not respond to a one-way call but shall silently prepare to receive traffic.

The traffic channel that will be used is indicated in the TX sub-channels vector in the LSU_Req1 PDU, where a bit set to 1 indicates that the corresponding sub-channel will be used in the transmission.

If traffic has not commenced within time $t_{traffic}$ after the end of the LSU_Req1 PDU, the called PUs shall silently depart the link (return to scanning or staring).

The calling PU will terminate the link by sending a series of LSU_Term PDUs. However, if a link inactivity timeout occurs, or upon command by a user process, receiving PUs shall silently depart the link.

G.5.5.10 Link quality analysis.

Link quality analysis (LQA) data are used by the Automatic Channel Selection (ACS) function to rank channels for calling and traffic. In addition to incidental opportunities to measure and record link quality when PDUs are received from other stations (see G.4.1.5), the following active mechanisms are provided for keeping LQA data current.

G.5.5.10.1 One-way LQA: sounding.

Systems compliant with this appendix shall be capable of periodically sending "sounding" transmissions on all channels in the active channel list. A "sound" consists of a LSU_Status PDU that contains the sending PU's address and its status (e.g., Normal; see Table G-XV).

a. Before sounding on any channel, a PU shall listen before transmitting and shall not sound if the channel is occupied.
b. When a network is scanning synchronously, the sound (a single LSU_Status PDU) shall be sent when the network is dwelling on that channel.
c. An asynchronous sound begins with a capture probe (see G.5.5.5.1b), followed by the LSU_Status PDU.

When a PU receives a sound, it shall measure and record the link quality in the Other Station Table (G.4.2.3). Receipt of a sound does not establish (or terminate) a link.
An example of sounding in a synchronous network is shown in Figure G-27.

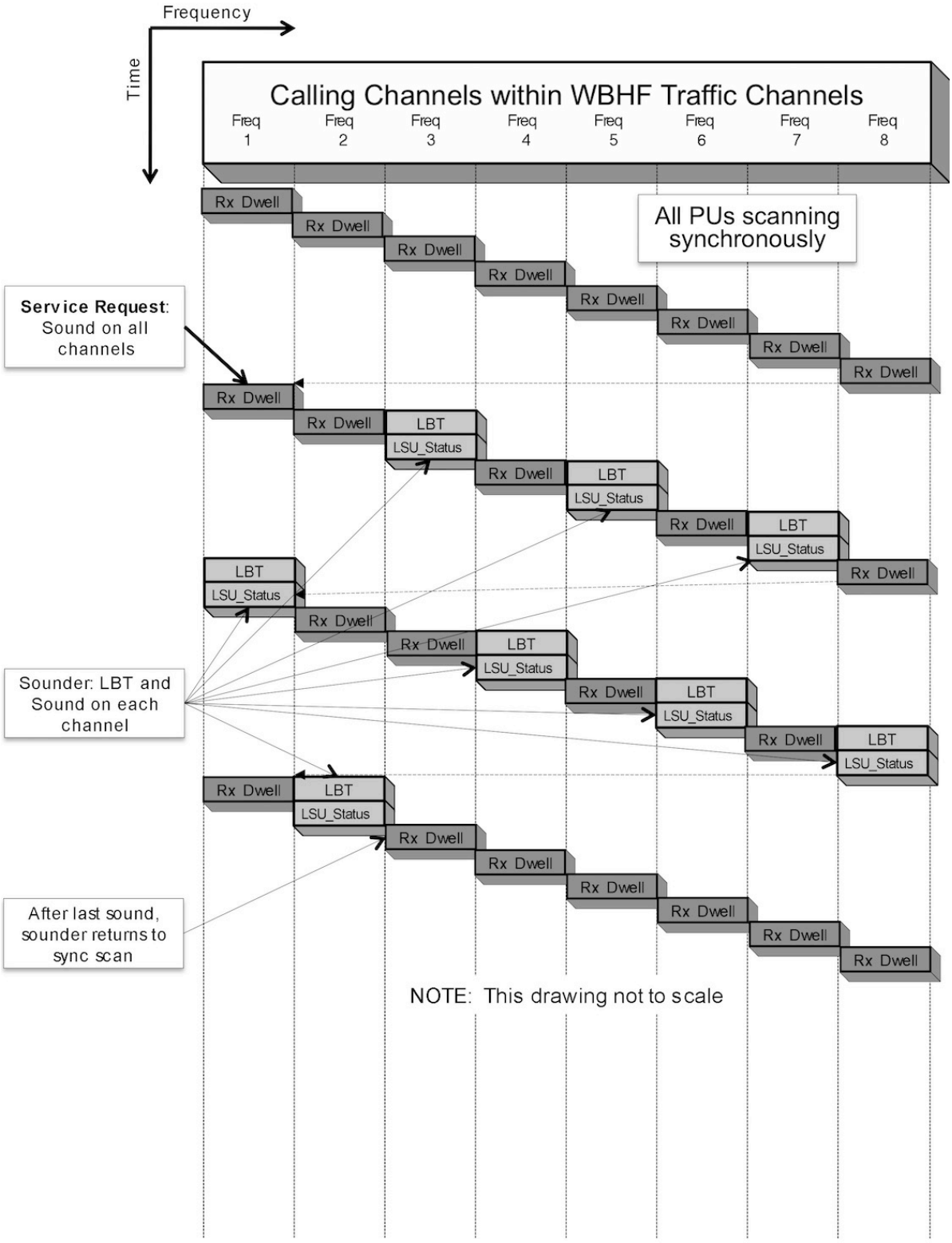


Figure G-27. Synchronous Sounding.

G.5.5.10.2 Two-way LQA exchange.

Systems compliant with this appendix shall, upon command, execute an LQA exchange as described here with another PU on specified channel(s).

a. The initiating PU shall call the other PU using the appropriate PTP protocol, including LBT. The LSU_Req PDU shall have Traffic Type = LQA Exchange.

b. The called PU shall LBR and respond as usual, including a report of the SNR measured during reception of the LSU_Req.

c. The initiating PU shall then terminate the link with a LSU_Term PDU with Reason = NO_MORE_TRAFFIC.

Both PUs shall measure and store LQA measurements from this handshake.

G.5.5.11 WALE Timing.

This section specifies the timing requirements for WALE.

G.5.5.11.1 Synchronous call timing.

When operating synchronously, PUs shall send link setup Request PDUs (LSU_Req or LSU_Req1) such that the transmission begins $T_{TxOffsetTLC}$ after the beginning of a dwell time:

$$T_{TxOffsetTLC} = \max\begin{cases} 2T_{sync} \\ D/2 - \left(T_{TLC} + T_{preamble} + T_{ODT} + 2T_{propMax}\right)/2 \end{cases}$$

Where

T_{sync} = maximum one-way time uncertainty in network (INP; default 36 ms)
D = synchronous dwell time (computed from INP SDS as 1350 ms / SDS)
T_{TLC} = duration of TLC (INP; default 13.33 ms)
$T_{preamble}$ = duration of preamble (120 ms for Fast WALE, 240 ms for Deep Wale)
T_{ODT} = 50 ms allowed from detection of preamble until stop scan is delivered to the receiver
$T_{propMax}$ = 80 ms maximum propagation delay on an HF link.

G.5.5.11.2 Asynchronous call timing.

An asynchronous link setup Request (LSU_Req or LSU_Req1) can begin at any time. It shall be preceded by a capture probe of duration $t_{capture}$, where

$t_{capture} \geq d_{min} * (C+2)$
where d_{min} is the asynchronous-mode minimum dwell time INP
and C is the number of channels in the scan set.

G.5.5.11.3 Response timing.

When responding to a call, a PU shall transmit a LSU_Conf starting after a delay of $T_{Confirm}$ after the end of the request PDU:

$T_{confirm} = T_{tune} + T_{handshake}$

where

T_{tune} = maximum network tuning time (INP; default 40 ms)

$T_{handshake}$ = 100 ms allowed for PDU processing and radio turnaround

When responding to any other WALE PDU (e.g., when sending a Caller Confirm), a PU shall begin its transmission after a delay of $T_{handshake}$ from the end of that preceding PDU.

G.5.5.11.4 Timeouts.

WALE timeouts are determined using four INPs: t_{tune}, $t_{response}$, $t_{traffic}$, and $t_{activity}$.

- A calling PU sets a timeout to wait $t_{response} + t_{tune}$ for a response to its LSU request. The INP $t_{response}$ must allow time for propagation to and from the responder plus $T_{handshake}$ plus the on-air duration of the responding PDU, recognizing that the response may use the Deep WALE waveform.
- A responding PU sets a timeout to wait $t_{traffic}$ for either another WALE PDU or traffic to be detected from the other PU. The INP $t_{traffic} \geq t_{response}$ to allow time for a WALE PDU.
- After traffic has commenced on a link, all participating PUs should start an activity timeout with duration $t_{activity} \geq t_{traffic}$ whenever traffic pauses. If this timeout expires without a re-sumption of traffic, the link should be terminated by sending a LSU_Term.

G.5.6 Message Protocols.

In addition to WALE (link setup), the 4G protocol suite includes simple, unacknowledged message passing protocols for text and binary data. Text and binary messages may be included in any 4G transmission by appending message PDUs to any addressed PDU (e.g., link setup PDUs) in which the M bit in that leading PDU is set to 1. Messages may also be sent “stand alone” by appending them to Message Header PDUs (G.5.6.2).

G.5.6.1 Message protocol PDUs.

PDUs used in the message protocols are shown in Figure G-28 through Figure G-30. The specific PDU types shown shall be used as specified in the protocol specifications in the following paragraphs.

The Control field in the message PDUs is shown in Figure G-31.

- The 3-bit Padding field shall indicate the number of unused octets carried by this PDU. This shall be 0 except in the final PDU of a message, where it ranges from 0 through 7.
- The SOM bit shall be set to 1 if the PDU contains the start of a message; set to 0 otherwise.
- The EOM bit shall be set to 1 if the PDU contains the end of a message; set to 0 otherwise.

The Word (PDU) Countdown field shall be set to one less than the number of PDUs in the message in the first PDU of a message (SOM = 1), and shall count down in each succeeding PDU, reaching 0 in the final PDU of the message (EOM = 1).

Each message PDU can carry up to eight octets of message content, so the maximum length of a message is 2048 octets. Message octets shall be sent in message order over the air. If the message length is not an even multiple of 8 octets, the final message PDU shall be padded after the final message octets with NUL characters for a binary message.

	7 6 5 4 3 2 1 0
Msg_Hdr	0 1 1 | 0 0 0 | 0 1
	0 0 0 0 0 0 0 0
Sender Address	MSB – – – – – – – – – – – – – – – – LSB
Recipient Address	MSB – – – – – – – – – – – – – – – – LSB
Purpose (locally defined)	
CRC	– – – – – – – – MSB LSB – – – – – – – –

Figure G-28. Message Header PDU

	7 6 5 4 3 2 1 0
Text_Msg	0 0 0 Control
	Word (PDU) Countdown
Message Text	earliest octet
	latest octet
CRC	– – – – – – – – MSB LSB – – – – – – – –

Figure G-29. Text Message PDU

	7 6 5 4 3 2 1 0
Binary_Msg	0 0 1 Control
	Word (PDU) Countdown
Data Message	earliest octet
	latest octet
CRC	– – – – – – – – MSB LSB – – – – – – – –

Figure G-30. Binary Message PDU

	3	1	1
Control Field	Padding	SOM	EOM

Figure G-31. Message PDU Control Field

G.5.6.2 Message header.

If a message is to be sent “stand alone” (not part of a link setup handshake) the message PDUs shall be appended to a Message Header PDU, which carries the WALE addresses of the sending and recipient PUs. The Purpose field is not standardized, and may be used as desired by network managers.

G.5.6.3 4G Text Message Protocol.

The Text Message Protocol is provided for conveying human-readable messages. Text messages shall be displayed to the operator upon receipt.
Each octet in the Message Text field of a Text Message PDU shall contain one ASCII character in the seven least-significant bits. The most-significant bit shall be computed from the least-significant bits such that the overall parity of the octet is odd.
Characters received with parity errors should be replaced with a distinctive error indication when displayed to the operator.

G.5.6.4 4G Binary Message Protocol.

The Binary Message Protocol is provided for conveying machine-readable messages.
Each octet in the Binary Data field of a Binary Message PDU shall carry one octet of the binary message. Error detection is provided only via the PDU CRC field.

G.5.7 Utility Protocols.

The 4G utility protocols support late net entry, network time synchronization, and distribution of network operating data (“data fill”).

G.5.7.1 Utility PDUs.

The utility protocol PDUs are shown in Figure G-32 through Figure G-34. The specific PDU types shown shall be used as specified in the protocol specifications in the following paragraphs.

	7	6	5	4	3	2	1	0
TOD_Resp	0	1	1	1	0	1	V	M
	0	0	0	0	0	0	EC	
Caller Address	MSB – – – – – – – –							
	– – – – – – – – LSB							
Responder Address	MSB – – – – – – – –							
	– – – – – – – – LSB							
Sync Offset	TQ			0	0	0	0	Sign
	Magnitude							
Coarse Time	0	0	Minutes					
	0	0	Seconds					
CRC	– – – – – – – – MSB							
	LSB – – – – – – – –							

Figure G-32. Time-of-Day Response PDU

	7	6	5	4	3	2	1	0
Fill_Req	0	1	1	1	1	0	V	M
	0	0	0	0	0	0	EC	
Caller Address or 0xFFxx	MSB – – – – – – – –							
	– – – – – – – – LSB							
Called Address: 0xFFFF	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1
Assigned Sub-channels	bin 15 – – – – – – – –							
	– – – – – – – – bin 0							
Occupied Sub-channels	bin 15 – – – – – – – –							
	– – – – – – – – bin 0							
CRC	– – – – – – – – MSB							
	LSB – – – – – – – –							

Figure G-33. Data Fill Request PDU

	7	6	5	4	3	2	1	0
Fill_Resp	0	1	1	1	1	1	V	M
	SNR						EC	
Caller Address (matches request)	MSB – – – – – – – – LSB							
Called Address	MSB – – – – – – – – LSB							
Tx Sub-channels	bin 15 – – – – – – – – bin 0							
Rx Sub-channels	bin 15 – – – – – – – – bin 0							
CRC	– – – – – – – – MSB LSB – – – – – – – –							

Figure G-34. Data Fill Response PDU

G.5.7.2 Late Net Entry (optional).

A PU seeking to enter a network, but which lacks a complete set of INPs (G.4.2.4) must have at least the following information to join the network:

- the WALE address of a network member PU that is able to provide a full data fill
- at least one channel record for a channel used by that network
- the linking protection key in use (if any)

Using default values for any missing INPs, the entering PU shall call the known PU to request a data fill (G.5.7.3), using a synchronous call if it is synchronized, an asynchronous call otherwise. If the entering PU is not synchronized, it should request Time of Day from the known PU (G.5.7.4).

G.5.7.3 Data fill distribution.

Over-the-air programming of WBHF PUs is accomplished via the transfer of formatted data fill files between RED-side network management entities

G.5.7.3.1 Data fill protocol (optional).

PUs shall request the current data fill by transmitting a Fill Request PDU, using either the synchronous (G.5.5.4.1) or asynchronous (G.5.5.5.1) point-to-point link setup procedure, with the following modifications:

- A Fill Request PDU is sent instead of a LSU_Req PDU. If the requesting PU has not yet been assigned a WALE address in the network, it shall randomly select an address in the range 0xFF00 through 0xFFFE, and use that as the Caller Address in all requests until it is assigned a WALE address. In the Fill Request, M=1 means the call sign (user process address) of the requesting PU follows in Text Message PDU(s).
- A Fill Response PDU is returned instead of a LSU_Conf PDU. The responding PU shall supply its WALE address in the Called Address field. If the Fill Request used a self-assigned (0xFFxx) WALE address, the M bit in the Response shall be set to 1 and the assigned WALE address for the requestor shall immediately follow the Fill Response PDU in a Binary Message PDU.
- The requesting PU shall send a LSU_Conf PDU whose Tx and Rx sub-channel vectors shall be used by both PUs to determine the traffic channel to be used for the data fill transmission. The Caller Address in this LSU_Conf PDU shall be the WALE address of the requestor (possibly just assigned) and the Called Address shall be that of the responding PU (from the Fill Response).

After this 3-way handshake sets up a traffic channel, the responder shall send the current data fill file (G.5.7.3.2) to the requestor using the STANAG 5066 CFTP protocol. The assigned WALE addresses shall be used in the STANAG 5066 data transfer.

G.5.7.3.2 Data fill file format.

The data fill file is formatted using XML.

G.5.7.4 Time of day (TOD) distribution.

GPS shall be the typical and preferred method of achieving TOD synchronization among PUs in a network. GPS TOD is considered accurate net time, and all other methods are considered less accurate. PUs without GPS TOD may request and receive TOD from a synchronized PU by means of the following protocol.
Unsynchronized PUs shall request TOD by transmitting a TOD Request, which may be either *undirected* (implicitly addressed to the current net control station), or *directed* (explicitly addressed to a designated responder).

G.5.7.4.1 Undirected TOD Request.
To transmit an *undirected* TOD Request, a PU shall transmit an asynchronous call according to the asynchronous LSU procedure (G.5.5.5.1), with the following PDU field values:

- Called Address = all ones (broadcast)
- Caller Address = calling PU address, and
- Traffic Type = TOD (per Table G-XII).

G.5.7.4.2 Directed TOD Request.

To transmit a *directed* TOD Request, a PU shall transmit an asynchronous call according to the asynchronous LSU procedure (G.5.5.5.1), with the following PDU field values:

- Called Address = the individual address of the desired responder
- Caller Address = calling PU address, and
- Traffic Type = TOD (per Table G-XII).

G.5.7.4.3 TOD Response.

The PU responding to an *undirected* TOD Request should be the Net Control PU (i.e., the PU whose individual address is equal to the INP value INP_NetControlPU as defined in section G.4.2.4. If this PU is unable to respond, it is permissible for another PU to respond. User doctrine must ensure that only one station will respond, as otherwise the responses from multiple PUs would collide.
The PU responding to a *directed* TOD Request shall be only the PU having an individual address equal to the destination address of the TOD Request.
The PU responding to a TOD Request shall issue a precisely timed TOD_Response PDU, with the following PDU field values:

- Responder Address = responder's individual address.
- Caller Address = calling PU address in response to a directed TOD Request, or
  Caller Address = all ones (broadcast) in response to an undirected TOD Request.
- Min = the minute in the hour when the PDU will begin.
- Sec = the second in the minute when the PDU will begin.
- Sync Offset = time difference between arrival of the end of the preamble of the TOD Request PDU and the time when the preamble of a correctly synchronized PDU would end, encoded IAW Table G-XVI.
- Sign = 1 if the TOD Request PDU was late, Sign = 0 if it was early.
- TQ indicates the time quality of the responding PU time base IAW Table G-XVII.

The milliseconds TOD information shall be conveyed via the timing of the PDU. The Response shall be transmitted starting precisely $T_{Confirm}$ after the end of the TOD Request PDU.

Table G-XVI Sync Offset codes

Sync Offset Code	Magnitude of Offset (ms)	Range of Offsets (ms)
0 - 50	2 x Code	0 – 100
51 – 175	100 + 10 x (Code – 50)	110 – 1,350
176 – 254	1350 + 50 x (Code – 175)	1,400 – 5,300
255	(no report)	

Table G-XVII Time quality codes

Time Quality Code	Total Time Uncertainty
0 (000)	none: UTC PU
1 (001)	1 ms: local GPS receiver or equiv.
2 (010)	5 ms or stand-alone master PU
3 (011)	20 ms
4 (100)	50 ms
5 (101)	200 ms
6 (110)	500 ms
7 (111)	unbounded or unknown

The transmitted TOD and SyncOffset and the precise timing of the TOD_Resp PDU shall be used by the unsynchronized PU to estimate TOD and propagation delay as follows (see Figure G-35):

- $T_{nominal}$ = $T_{TxOffsetTLC} + T_{TLC} + T_{preamble}$
  = offset from start of slot when preamble of correctly timed PDU would end.
- $T_{ReqSlotLate}$ = time difference between start of slot at requester and start of slot at responder (positive if requester slot is later than responder slot).
- T_{prop} = propagation delay between requester and responder.
- $T_{SyncOffset}$ = $T_{prop} + T_{ReqSlotLate}$
- $T_{Confirm}$ = fixed delay at responder between end of Request and start of Confirm
- T_{Burst} = $T_{TLC} + T_{preamble} + T_{payload}$
  = on-air duration of a single PDU (Fast or Deep waveform).
- $T_{Elapsed}$ = $2T_{prop} + T_{Confirm} + T_{Burst}$

Upon receipt of the TOD Response, the requesting PU shall

- Compute and store $T_{prop} = (T_{Elapsed} - T_{Confirm} - T_{Burst}) / 2$.
- Compute $T_{ReqSlotLate} = T_{SyncOffset} - T_{prop}$ and correct its slot timing accordingly.
- Set its local time uncertainty IAW the TQ code plus 1 ms.

G.5.7.5 Synchronization maintenance.

PUs operating in synchronous mode that lack or lose access to GPS time should perform Sync Check handshakes (see Figure G-35) with the Net Control PU as required to compensate for time base drift. The Sync Check handshake is a synchronous LSU_Req with traffic type = Sync Check followed by a TOD Response and time adjustment as described above (G.5.7.4.3).

If a PU's time uncertainty grows past the limit, it must cease synchronous operation and use only asynchronous calls until it is able to reacquire network synchronization.

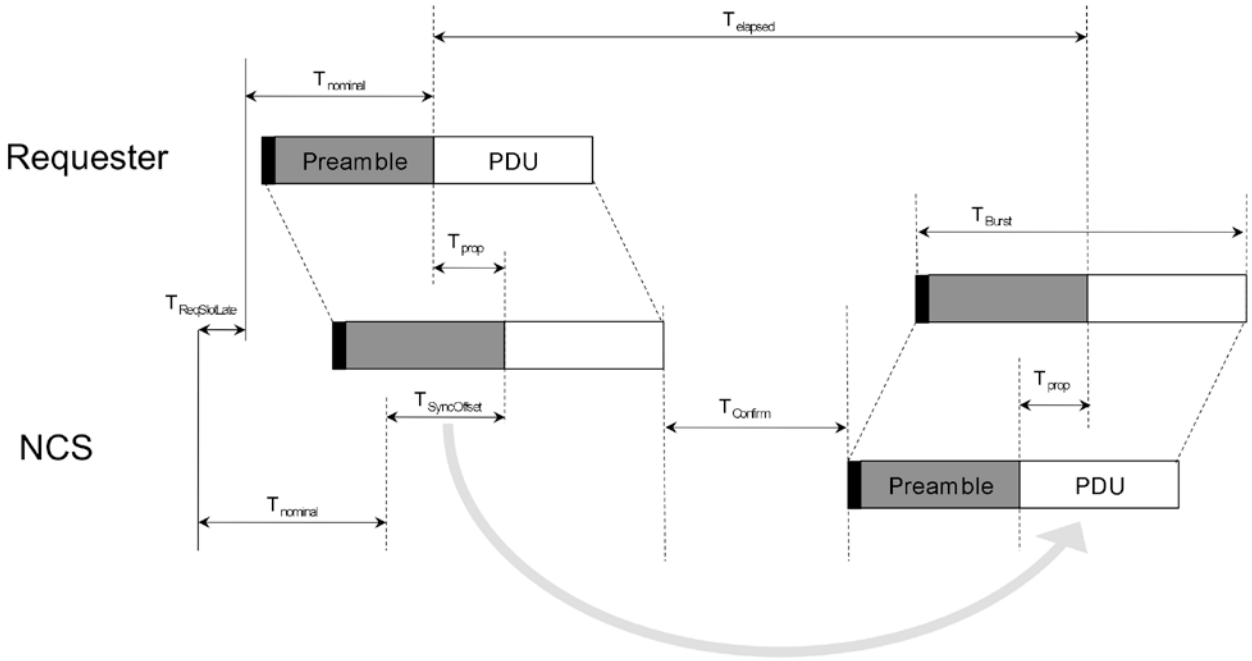


Figure G-35. Sync Check Handshake.

G.5.7.6 Time Broadcast.

Broadcast TOD synchronization, with passive TOD acquisition, shall be achieved as follows:

- The net control station issues both the TOD request and the TOD_Response.
- Any unsynchronized PU that receives a TOD broadcast from its NCS may use the received TOD after adjusting for propagation delay (using previously stored T_{prop}).

G.5.8 Linking Protection.

Linking protection (LP) shall be provided when NATO-mode addressing is required. Otherwise LP is optional. LP encrypts 4G PDUs for authentication, not confidentiality. Note that the security of the network depends on keeping LP key private.
In NATO-mode addressing, the called network number shall be replicated and combined with private key before the key is used by the authentication algorithm (G.5.3).

G.5.8.1 Seed format.

The seed format is shown in Figure G-36. The Time of Day (TOD) fields shall be derived from network time, which is a continuous time scale nominally identical to the GPS time scale. In particular, leap seconds shall not be inserted in the network time scale.

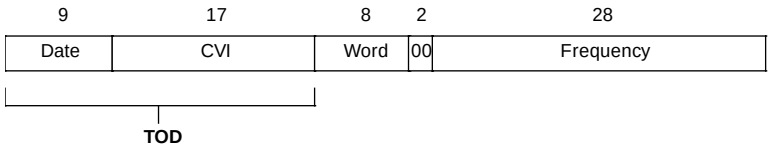


Figure G-36. Linking Protection Seed.

The date field shall contain a 4-bit month field in the most-significant bits (leftmost bits in the figure) and a 5-bit day number in the least-significant bits. 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).
The CVI (code validity interval) field specifies time within each day. Normally, this field contains a count of the number of CVIs that have completely elapsed since midnight network time. In certain applications, this field may be set to all 1's, indicating that time within the day is not specified.

The word field is used to count PDUs within a CVI, as specified in G.5.8.2.
The frequency field shall contain binary-coded decimal digits of the assigned frequency of the current protected transmission. The seven digits shall be, in left to right order: MHz (hundreds, tens, units), kHz (hundreds, tens, units), and Hz (hundreds).

G.5.8.2 Protection of 4G transmissions.

When linking protection is used in a network, PDUs shall be encrypted using the HALFLOOP algorithm (G.5.8.3) before they are passed to the physical layer (i.e., before coding and interleaving) and decrypted after they are received from the receiver physical layer. Capture probes contain no PDUs, and are not encrypted.
The TOD fields in the seed shall be set to the time that the first PDU in a transmission will be sent. The first PDU in a handshake (e.g., a LSU_Req), a Msg_Hdr PDU, or the first LSU_Term PDU in a termination sequence shall be encrypted with the Word field set to 0. Each PDU sent subsequently in the handshake, message, or termination sequence (by any PU) shall use a successively higher word number.

An example of word number sequencing is shown in Table G-XVIII

Table G-XVIII LP Word number sequencing example.

PU	PDU	Word Number
Caller	LSU_Req (multipoint)	0
Called 1	LSU_Conf	1
Called 2	No response (didn't hear call)	–
Called 3	LSU_Conf	3
Caller	LSU_Conf	4

G.5.8.3 HALFLOOP algorithm.

4G PDUs shall be protected using the HALFLOOP algorithm, specified in Appendix H.

APPENDIX H

HALFLOOP LINKING PROTECTION ALGORITHM

TABLE OF CONTENTS

PARAGRAPH **PAGE**

TABLE OF CONTENTS (Continued)

PARAGRAPH **PAGE**

TABLES

TABLE **PAGE**

FIGURES

FIGURE **PAGE**

HALFLOOP LINKING PROTECTION ALGORITHM

G.6 GENERAL

G.6.1 Scope.

This appendix contains the specifications for the HALFLOOP linking protection (LP) algorithm.

G.6.2 Applicability.

This appendix is a mandatory part of MIL-STD-188-141 whenever LP is a requirement to be implemented in fourth-generation (4G) high frequency (HF) radio systems, or when HALFLOOP is specified to replace the earlier Lattice and SODARK LP algorithms in second-generation (2G) or third-generation (3G) systems. The algorithm described herein is intended for use within the LP procedures specified in Appendix B.

G.7 APPLICABLE DOCUMENTS

G.7.1 General.

The documents listed in this section are specified in H.3, H.4, and H.5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information or as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they must meet all specified requirements documents cited in H.3, H.4, and H.5 of this standard, whether or not they are listed.

G.7.2 Government documents.

G.7.2.1 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 cited in the solicitation or contract.

FEDERAL STANDARDS

FED-STD-1037	Telecommunications: Glossary of Telecommunications Terms
FIPS PUB 197	Advanced Encryption Standard

(Copies of these documents are available online at http://quicksearch.dla.mil.)

G.8 DEFINITIONS

G.8.1 Terms.

Definitions of terms used in this document shall be as specified in the current edition of FED-STD-1037 except where inconsistent with the use in this standard. In addition, the following definitions are applicable for the purpose of this standard.

Linking protection	cryptographic authentication of link setup transmissions; neither COMSEC nor TRANSEC.

G.8.2 Abbreviations and acronyms.

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

2G	second generation
3G	third generation
4G	fourth generation
ALE	automatic link establishment
FLSU	fast link setup (a 3G technology)
FTM	fast traffic management (a 3G technology)
HF	high frequency
LP	linking protection
Nb	number of words in plain- or ciphertext block
Nk	number of words in key variable
Nr	number of rounds performed by algorithm
Ns	number of words in seed
PDU	protocol data unit
RLSU	robust link setup (a 3G technology)
WALE	wideband automatic link establishment

G.9 GENERAL REQUIREMENTS.

G.9.1 HALFLOOP overview.

LP authenticates automatic link establishment (ALE) transmissions by encrypting the ALE protocol data units (PDUs) before transmission. LP encryption uses a “key” variable that is known only by authorized users. Any mismatch in the key used by sending and receiving systems will result in received PDUs that are unintelligible after decryption and therefore ignored. A “seed” is also used in LP encryption, which introduces time- and frequency-dependence into the authentication mechanism.

G.9.1.1 HALFLOOP key variable.

Systems compliant with this appendix shall use a 128-bit key: Nk = 4.

G.9.1.2 HALFLOOP seed.

Systems compliant with this appendix shall use a 64-bit seed in accordance with Figure B-3 Seed formats in Appendix B: Ns = 2.

G.9.2 HALFLOOP block sizes.

HALFLOOP is a block algorithm. HALFLOOP variants are specified in section 5 for use in 2G, 3G and 4G systems. The block size parameter Nb for each variant is specified in the respective paragraph in section 5 (G.10.2 through G.10.4).

G.9.2.1 HALFLOOP-96 applications.

4G ALE PDUs shall be encrypted using the HALFLOOP-96 algorithm.

G.9.2.2 HALFLOOP-48 applications.

If HALFLOOP is used in 3G systems using Fast Link Setup (FLSU), the 50-bit FLSU and Fast Traffic Management (FTM) PDUs shall be encrypted using the HALFLOOP-48 algorithm as follows:

- The two most-significant bits shall be sent unencrypted.
- The remaining 48 bits of the RLSU PDU shall be encrypted using the HALFLOOP-48 algorithm.

G.9.2.3 HALFLOOP-24 applications.

If HALFLOOP is used in 2G systems, the 2G ALE words shall be encrypted using the HALFLOOP-24 algorithm.
If HALFLOOP is used in 3G systems using Robust Link Setup (RLSU), the 26-bit RLSU PDUs shall be encrypted using the HALFLOOP-24 algorithm as follows:

- The two most-significant bits shall be sent unencrypted.
- The remaining 24 bits of the RLSU PDU shall be encrypted using the HALFLOOP-24 algorithm.

G.9.3 HALFLOOP Rounds.

The HALFLOOP algorithm uses ten rounds: Nr = 10.

G.10 DETAILED REQUIREMENTS

HALFLOOP is derived from the FIPS PUB 197 Advanced Encryption Standard (AES) and is specified here using similar terminology.

Aspects of HALFLOOP that are common to all block sizes are specified in G.10.1, followed by separate specifications of the requirements peculiar to each block size.

G.10.1 HALFLOOP common elements.

Like AES, the HALFLOOP algorithm operates on a rectangular array of bytes, which is termed the "state." The dimensions of the state array for each variant of HALFLOOP are shown in Figure G-37. The mapping of plaintext and ciphertext blocks to and from the respective state arrays is specified in the requirements for each HALFLOOP variant.

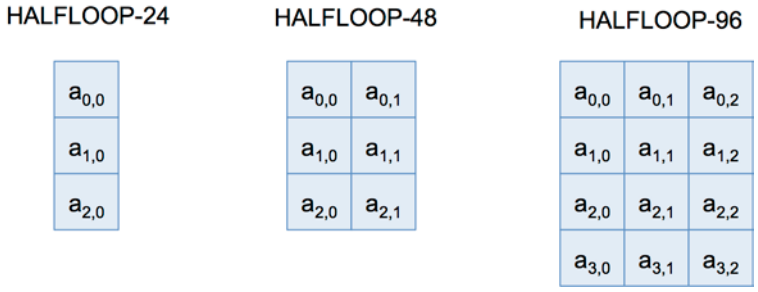


Figure G-37. HALFLOOP State Arrays

G.10.1.1 HALFLOOP Encryption.

A system encrypting a block using HALFLOOP shall execute the following sequence of steps:

Operation	Reference
`GenerateRoundKeys`	G.10.1.2
`AddRoundKey(0)`	G.10.1.3
`for (round=1; round<Nr; round++) {`	
`  SubBytes`	G.10.1.4
`  RotateRows`	G.10.1.5
`  MixColumns`	G.10.1.6
`  AddRoundKey(round*Nb)`	G.10.1.3
`}`	
`SubBytes`	G.10.1.4
`RotateRows`	G.10.1.5
`AddRoundKey(Nr*Nb)`	G.10.1.3

In the following paragraphs, the encryption operations are illustrated using the HALFLOOP-96 state. The operations on smaller arrays are similar, as specified in the requirements for each HALFLOOP variant in G.10.2 through G.10.4.

G.10.1.2 HALFLOOP key schedule.

The HALFLOOP key schedule is a linear array of “round” keys, each of which contains Nb words (32-bit words for HALFLOOP-96; 24-bit words for the others). This key schedule shall be generated by expanding the key variable and seed as indicated in the following pseudocode:

```
GenerateRoundKeys(byte key[4*Nk], seed[4*Ns], word w[Nb*(Nr+1)], Nk)
begin
   word temp

   i=0

   while (i < Ns)
      w[i] = word(key[4*i] xor seed[4*i], key[4*i+1] xor seed[4*i+1],
                  key[4*i+2] xor seed[4*i+2], key[4*i+3] xor seed[4*i+3])
      i = i+1
   end while

   while (i < Nk)
      w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
      i = i+1
   end while

   while (i < Nb * (Nr+1)]
      temp = w[i-1]
      if (i mod Nk = 0)
         temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
      end if
      w[i] = w[i-Nk] xor temp
      i=i+1
   end while
end
```

SubWord() is a function that takes a four-byte input word and applies the S-box in G.10.1.4 to each of the four bytes to produce an output word. The function RotWord() takes a word $[a_0,a_1,a_2,a_3]$ as input, performs a cyclic permutation, and returns the word $[a_1,a_2,a_3,a_0]$. The round constant word array, Rcon[i] contains the values

```
{ 0x8d000000, 0x01000000, 0x02000000, 0x04000000, 0x08000000,
  0x10000000, 0x20000000, 0x40000000, 0x80000000, 0x1b000000,
  0x36000000, 0x6c000000, 0xd8000000, 0xab000000, 0x4d000000 }.
```

This is similar to the AES key schedule, except that the seed is added modulo-2 (exclusive-OR) to the first 64 bits of the main key before that key is expanded.

For HALFLOOP-48 and HALFLOOP-24, the 4-byte words shall be repacked into 3-byte words.

G.10.1.3 HALFLOOP AddRoundKey.

AddRoundKey adds (bitwise, modulo-2) one word of round key (see G.10.1.2) with each column of the state (Figure G-38). The first word of round key shall be added to the first column (a_0) and so on. Note that the order of rounds is reversed in decryption.

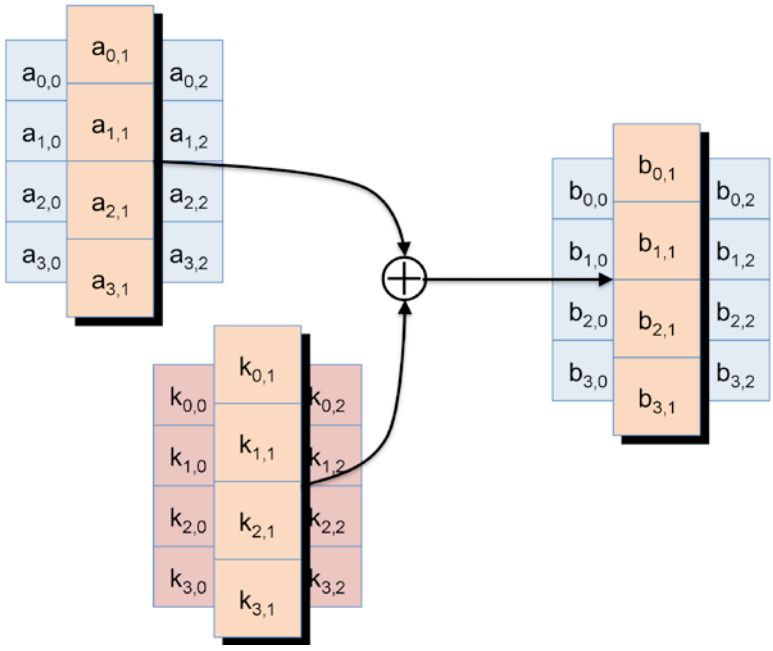


Figure G-38. HALFLOOP-96 AddRoundKey

G.10.1.4 HALFLOOP SubBytes.

SubBytes uses an 8-bit substitution transformation (S-box) to transform each byte in the state, as shown in Figure G-39.

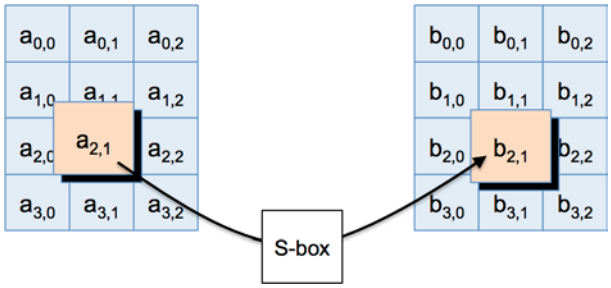


Figure G-39. HALFLOOP-96 SubBytes

For encryption, substitutions shall use the S-box in Table G-XIX The value of the incoming byte shall be used as an index into the table to find the replacement byte (shown in hexadecimal in the table). For example, if the incoming byte is hexadecimal 12, the replacement byte shall be C9.

Table G-XIX HALFLOOP Encryption Substitution

```
unsigned char s[256] =
 {
    63, 7C, 77, 7B, F2, 6B, 6F, C5, 30, 01, 67, 2B, FE, D7, AB, 76,
    CA, 82, C9, 7D, FA, 59, 47, F0, AD, D4, A2, AF, 9C, A4, 72, C0,
    B7, FD, 93, 26, 36, 3F, F7, CC, 34, A5, E5, F1, 71, D8, 31, 15,
    04, C7, 23, C3, 18, 96, 05, 9A, 07, 12, 80, E2, EB, 27, B2, 75,
    09, 83, 2C, 1A, 1B, 6E, 5A, A0, 52, 3B, D6, B3, 29, E3, 2F, 84,
    53, D1, 00, ED, 20, FC, B1, 5B, 6A, CB, BE, 39, 4A, 4C, 58, CF,
```

```
    D0, EF, AA, FB, 43, 4D, 33, 85, 45, F9, 02, 7F, 50, 3C, 9F, A8,
    51, A3, 40, 8F, 92, 9D, 38, F5, BC, B6, DA, 21, 10, FF, F3, D2,
    CD, 0C, 13, EC, 5F, 97, 44, 17, C4, A7, 7E, 3D, 64, 5D, 19, 73,
    60, 81, 4F, DC, 22, 2A, 90, 88, 46, EE, B8, 14, DE, 5E, 0B, DB,
    E0, 32, 3A, 0A, 49, 06, 24, 5C, C2, D3, AC, 62, 91, 95, E4, 79,
    E7, C8, 37, 6D, 8D, D5, 4E, A9, 6C, 56, F4, EA, 65, 7A, AE, 08,
    BA, 78, 25, 2E, 1C, A6, B4, C6, E8, DD, 74, 1F, 4B, BD, 8B, 8A,
    70, 3E, B5, 66, 48, 03, F6, 0E, 61, 35, 57, B9, 86, C1, 1D, 9E,
    E1, F8, 98, 11, 69, D9, 8E, 94, 9B, 1E, 87, E9, CE, 55, 28, DF,
    8C, A1, 89, 0D, BF, E6, 42, 68, 41, 99, 2D, 0F, B0, 54, BB, 16
};
```

G.10.1.5 HALFLOOP RotateRows.

RotateRows rotates the rows of the state to the left by different numbers of bit positions, as shown in Figure G-40. (This differs from AES, which is byte-aligned.)

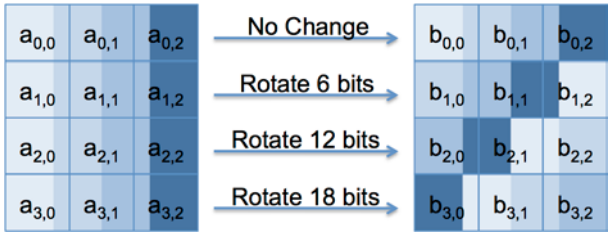


Figure G-40. HALFLOOP-96 RotateRows

G.10.1.6 HALFLOOP MixColumns.

MixColumns combines the bytes in each column using an invertible linear transformation (Figure G-41). Each column, treated as a polynomial over GF(2^8), is multiplied modulo x^4+1 with a fixed polynomial. The polynomial c(x) is specified for each HALFLOOP variant.

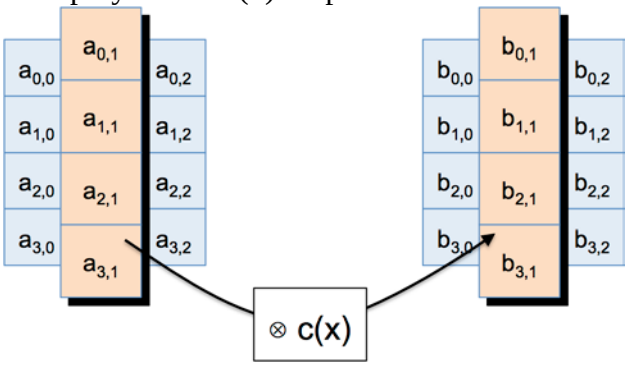


Figure G-41. HALFLOOP-96 MixColumns

G.10.1.7 HALFLOOP Decryption.

A system encrypting a block using HALFLOOP shall execute the following sequence of steps:

Operation	Reference
`GenerateRoundKeys`	G.10.1.2
`AddRoundKey(Nr*Nb)`	G.10.1.3
`for (round=Nr-1; round>0; round--) {`	

```
        InvRotateRows                                   G.10.1.8
        InvSubBytes                                     G.10.1.9
        AddRoundKey(round*Nb)                           G.10.1.3
        InvMixColumns                                   G.10.1.10
    }
    InvRotateRows                                       G.10.1.8
    InvSubBytes                                         G.10.1.9
    AddRoundKey(0)                                      G.10.1.3
```

G.10.1.8 HALFLOOP InvRotateRows.

RotateRows rotates the rows of the state to the right by different numbers of bit positions to invert the rotations performed by RotateRows at the sending station (Figure G-40).

G.10.1.9 HALFLOOP InvSubBytes.

InvSubBytes uses an 8-bit substitution transformation (S-box) to invert the substitution performed by SubBytes at the sending station (Figure G-39). For decryption, substitutions shall use the inverse S-box in Table G-XXThe value of the incoming byte shall be used as an index into the table to find the replacement byte (shown in hexadecimal in the table). For example, if the incoming byte is hexadecimal 12, the replacement byte shall be 39.

Table G-XX HALFLOOP Decryption Substitution

```
unsigned char inv_s[256] =
 {
    52, 09, 6A, D5, 30, 36, A5, 38, BF, 40, A3, 9E, 81, F3, D7, FB,
    7C, E3, 39, 82, 9B, 2F, FF, 87, 34, 8E, 43, 44, C4, DE, E9, CB,
    54, 7B, 94, 32, A6, C2, 23, 3D, EE, 4C, 95, 0B, 42, FA, C3, 4E,
    08, 2E, A1, 66, 28, D9, 24, B2, 76, 5B, A2, 49, 6D, 8B, D1, 25,
    72, F8, F6, 64, 86, 68, 98, 16, D4, A4, 5C, CC, 5D, 65, B6, 92,
    6C, 70, 48, 50, FD, ED, B9, DA, 5E, 15, 46, 57, A7, 8D, 9D, 84,
    90, D8, AB, 00, 8C, BC, D3, 0A, F7, E4, 58, 05, B8, B3, 45, 06,
    D0, 2C, 1E, 8F, CA, 3F, 0F, 02, C1, AF, BD, 03, 01, 13, 8A, 6B,
    3A, 91, 11, 41, 4F, 67, DC, EA, 97, F2, CF, CE, F0, B4, E6, 73,
    96, AC, 74, 22, E7, AD, 35, 85, E2, F9, 37, E8, 1C, 75, DF, 6E,
    47, F1, 1A, 71, 1D, 29, C5, 89, 6F, B7, 62, 0E, AA, 18, BE, 1B,
    FC, 56, 3E, 4B, C6, D2, 79, 20, 9A, DB, C0, FE, 78, CD, 5A, F4,
    1F, DD, A8, 33, 88, 07, C7, 31, B1, 12, 10, 59, 27, 80, EC, 5F,
    60, 51, 7F, A9, 19, B5, 4A, 0D, 2D, E5, 7A, 9F, 93, C9, 9C, EF,
    A0, E0, 3B, 4D, AE, 2A, F5, B0, C8, EB, BB, 3C, 83, 53, 99, 61,
    17, 2B, 04, 7E, BA, 77, D6, 26, E1, 69, 14, 63, 55, 21, 0C, 7D
 };
```

G.10.1.10 HALFLOOP InvMixColumns.

InvMixColumns combines the bytes in each column using the inverse of the linear transformation performed by MixColumns at the sending station (Figure G-39). The polynomial $c^{-1}(x)$ is specified for each HALFLOOP variant.

G.10.2 HALFLOOP-96.

HALFLOOP-96 encrypts and decrypts 96-bit blocks (Nb = 3) using the general procedures in G.10.1. Specific requirements for the HALFLOOP-96 variant are stated in the following subparagraphs.

G.10.2.1 HALFLOOP-96 state mapping.

A 96-bit block comprises 12 bytes. These bytes shall be mapped to and from HALFLOOP-96 state (3 columns by 4 rows as shown in Figure G-37) as follows: the most-significant byte of the 96-bit block shall map to and from $a_{0,0}$, with successive bytes mapping to and from $a_{1,0}$, $a_{2,0}$, $a_{3,0}$, $a_{0,1}$, $a_{1,1}$, $a_{2,1}$, a_{31}, $a_{0,2}$, $a_{1,2}$, $a_{2,2}$, and $a_{3,2}$.

G.10.2.2 HALFLOOP-96 RotateRows.

The rows of the state array shall be treated as 24-bit words and rotated as follows:

Row 0 ($a_{0,0}$, $a_{0,1}$, and $a_{0,2}$) shall not be rotated.
Row 1 ($a_{1,0}$, $a_{1,1}$, and $a_{1,2}$) shall be rotated left by 6 bit positions.
Row 2 ($a_{2,0}$, $a_{2,1}$, and $a_{2,2}$) shall be rotated left by 12 bit positions.
Row 3 ($a_{3,0}$, $a_{3,1}$, and $a_{3,2}$) shall be rotated left by 18 bit positions.

G.10.2.3 HALFLOOP-96 InvRotateRows.

The rows of the state array shall be treated as 24-bit words and rotated as follows:

Row 0 ($a_{0,0}$, $a_{0,1}$, and $a_{0,2}$) shall not be rotated.
Row 1 ($a_{1,0}$, $a_{1,1}$, and $a_{1,2}$) shall be rotated right by 6 bit positions.
Row 2 ($a_{2,0}$, $a_{2,1}$, and $a_{2,2}$) shall be rotated right by 12 bit positions.
Row 3 ($a_{3,0}$, $a_{3,1}$, and $a_{3,2}$) shall be rotated right by 18 bit positions.

G.10.2.4 HALFLOOP-96 MixColumns.

Each 32-bit column shall be treated as a polynomial over $GF(2^8)$ and multiplied modulo x^4+1 with the 4-term polynomial $c(x) = 3x^3 + x^2 + x + 2$.

G.10.2.5 HALFLOOP-96 InvMixColumns.

Each 32-bit column shall be treated as a polynomial over $GF(2^8)$ and multiplied modulo x^4+1 with the 4-term polynomial $c^{-1}(x) = 11x^3 + 13x^2 + 9x + 14$.

G.10.3 HALFLOOP-48.

HALFLOOP-48 encrypts and decrypts 48-bit blocks (Nb = 2) using the general procedures in G.10.1. Specific requirements for the HALFLOOP-48 variant are stated in the following subparagraphs.

G.10.3.1 HALFLOOP-48 state mapping.

The 48-bit block comprises 6 bytes. These bytes shall be mapped to and from HALFLOOP-48 state (2 columns by 3 rows as shown in Figure G-37) as follows: the most-significant byte shall map to and from $a_{0,0}$, with successive bytes mapping to and from $a_{1,0}$, $a_{2,0}$, $a_{0,1}$, $a_{1,1}$, and $a_{2,1}$.

G.10.3.2 HALFLOOP-48 RotateRows.

The rows of the state array shall be treated as 16-bit words and rotated as follows:
Row 0 ($a_{0,0}$ and $a_{0,1}$) shall not be rotated.
Row 1 ($a_{1,0}$ and $a_{1,1}$) shall be rotated left by 6 bit positions.
Row 2 ($a_{2,0}$ and $a_{2,1}$) shall be rotated left by 12 bit positions.

G.10.3.3 HALFLOOP-48 InvRotateRows.

The rows of the state array shall be treated as 16-bit words and rotated as follows:
Row 0 ($a_{0,0}$ and $a_{0,1}$) shall not be rotated.
Row 1 ($a_{1,0}$ and $a_{1,1}$) shall be rotated right by 6 bit positions.
Row 2 ($a_{2,0}$ and $a_{2,1}$) shall be rotated right by 12 bit positions.

G.10.3.4 HALFLOOP-48 MixColumns.

Each 24-bit column shall be treated as a polynomial over GF(2^8) and multiplied modulo x^4+1 with the 3-term polynomial $c(x) = x^2 + 2x + 9$.

G.10.3.5 HALFLOOP-48 InvMixColumns.

Each 24-bit column shall be treated as a polynomial over GF(2^8) and multiplied modulo x^4+1 with the 3-term polynomial $c^{-1}(x) = 8x^2 + 39x + 6$.

G.10.4 HALFLOOP-24.

HALFLOOP-24 encrypts and decrypts 24-bit blocks (Nb = 1) using the general procedures in G.10.1. Specific requirements for the HALFLOOP-24 variant are stated in the following subparagraphs.

G.10.4.1 HALFLOOP-24 state mapping.

The 24-bit block comprises 3 bytes. These bytes shall be mapped to and from HALFLOOP-24 state (1 column of 3 rows as shown in Figure G-37) as follows: the most-significant byte shall map to and from $a_{0,0}$, with successive bytes mapping to and from $a_{1,0}$, and $a_{2,0}$.

G.10.4.2 HALFLOOP-24 RotateRows.

The rows of the state array are 8-bit bytes which shall be rotated as follows:
Row 0 ($a_{0,0}$) shall not be rotated.
Row 1 ($a_{1,0}$) shall be rotated left by 6 bit positions.
Row 2 ($a_{2,0}$) shall be rotated left by 12 bit positions.

G.10.4.3 HALFLOOP-24 InvRotateRows.

The rows of the state array are 8-bit bytes which shall be rotated as follows:
Row 0 ($a_{0,0}$) shall not be rotated.
Row 1 ($a_{1,0}$) shall be rotated right by 6 bit positions.
Row 2 ($a_{2,0}$) shall be rotated right by 12 bit positions.

G.10.4.4 HALFLOOP-24 MixColumns.

The single 24-bit column shall be treated as a polynomial over GF(2^8) and multiplied modulo x^4+1 with the 3-term polynomial $c(x) = x^2 + 2x + 9$.

G.10.4.5 HALFLOOP-24 InvMixColumns.

The single 24-bit column shall be treated as a polynomial over GF(2^8) and multiplied modulo x^4+1 with the 3-term polynomial $c^{-1}(x) = 8x^2 + 39x + 6$.

G.10.5 Examples.

This section provides example computations for checking the correctness of implementations. The first few steps and the final ciphertext are provided.
In each case, the following key and seed are used:

```
Key:  2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
Seed: 54 3b d8 80 00 01 75 50
```

G.10.5.1 HALFLOOP-96 Example.

```
Input plaintext:  01 02 03 04 05 06 07 08 09 0a 0b 0c
```

GenerateRoundKeys()

```
7f45cd96    (key XOR seed)
28afa7f6    (key XOR seed)
abf71588    (key)
09cf4f3c    (key)
f4c12697    (first expanded word)
dc6e8161  ...
```

The following table shows the state after each of the first few steps of the algorithm.

Initial State			Add Round Key			Sub Bytes			Rotate Rows			Mix Columns		
01	05	09	7e	2d	a2	f3	d8	3a	f3	d8	3a	db	d9	5f
02	06	0a	47	a9	fd	a0	d3	54	34	d5	28	ef	2f	5e
03	07	0b	ce	a0	1e	8b	e0	72	07	28	be	4e	1f	59
04	08	0c	92	fe	84	4f	bb	5f	7d	3e	ed	c7	f2	19

```
Output ciphertext:  b3 94 78 31 58 fb 34 9c 45 e6 bd f9
```

G.10.5.2 HALFLOOP-48 Example.

```
Input plaintext:  01 02 03 04 05 06
```

GenerateRoundKeys()

```
      7f45cd96    (key XOR seed)
      28afa7f6    (key XOR seed)
      abf71588    (key)
      09cf4f3c    (key)
      f4c12697    (first expanded word)
      dc6e8161  ...
```

RepackRoundKeys() (only 3 bytes per word)

```
      007f45cd
      009628af
      00a7f6ab
      00f71588
      0009cf4f
      003cf4c1
      002697dc
      006e8161
```

The following table shows the state after each of the first few steps of the algorithm.

Initial State	Add Round Key	Sub Bytes	Rotate Rows	Mix Columns
01 04	7e 92	f3 4f	f3 4f	6c 48
02 05	47 2d	a0 d8	36 28	58 50
03 06	ce a9	8b d3	38 bd	7c 3d

```
Output ciphertext:  5e 5c da 82 d3 7c
```

G.10.5.3 HALFLOOP-24 Example.

```
Input plaintext:  01 02 03
```

GenerateRoundKeys()

```
7f45cd96    (key XOR seed)
28afa7f6    (key XOR seed)
abf71588    (key)
09cf4f3c    (key)
f4c12697    (first expanded word)
dc6e8161  ...
```

RepackRoundKeys() (only 3 bytes per word)

```
007f45cd
009628af
00a7f6ab
00f71588
0009cf4f
003cf4c1
002697dc
006e8161
```

The following table shows the state after each of the first few steps of the algorithm.

Initial State	Add Round Key	Sub Bytes	Rotate Rows	Mix Columns
01	7e	f3	f3	69
02	47	a0	28	36
03	ce	8b	b8	ac

```
Output ciphertext:  f2 8c 1e
```

CONCLUDING MATERIAL

Custodians:
Army – CR
Navy - EC
Air Froce - 71

Preparing activity:
Air Force – 71

(Project TCSS-2018-002)

Review Activities:
Navy – MC
Air Force – 02, 07
DoD – DC, NS

NOTE: The activities listed above were interested in this document as of the date of this document. Since organizations and responsibilities can change, you should verify the currency of the information above using the ASSIST Online database at https://assist.dla.mil.