Understanding Voice and Data Link Networking

Northrop Grumman's Guide to Secure Tactical Data Links

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

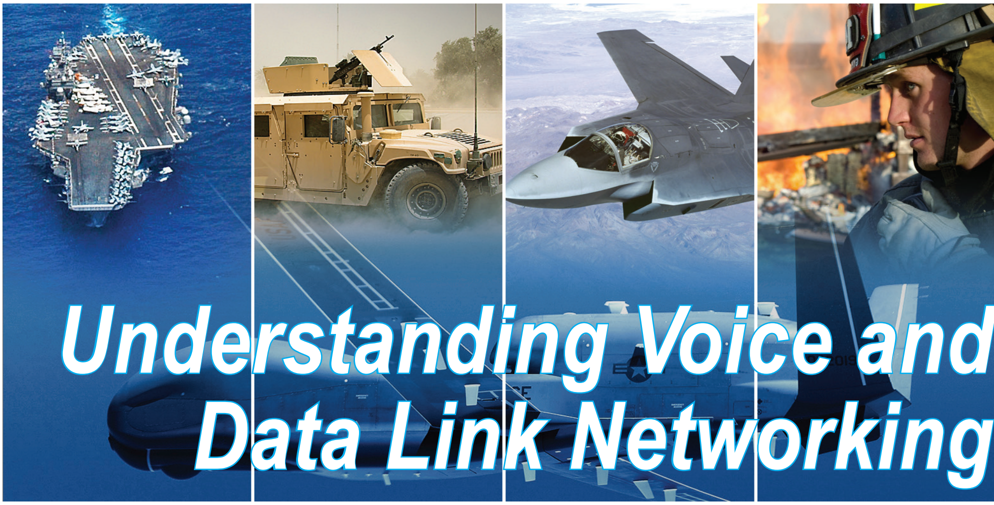
Understanding Voice and Data Link Networking

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

Northrop Grumman
9326 Spectrum Center Blvd.
San Diego, CA 92123

Product Sales/Customer Service:
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com



Understanding Voice and Data Link Networking

Northrop Grumman's Guide to Secure Tactical Data Links

December 2014

Prepared by:

Northrop Grumman
9326 Spectrum Center Boulevard
San Diego, CA 92123-1443, USA

Original edition for public release December 2013
First Revision December 2014

Distributed by

Northrop Grumman
9326 Spectrum Center Boulevard
San Diego, CA 92123-1443

Document number 135-02-005

Dedication

As a warfighter with many years of deployed operational experience, I fully understand the complex environment in which we operate and the importance of tactical data links to mission success. I particularly appreciate the enormous leverage information networks, allied interoperability, and assured communications provide as mission enablers and force multipliers in an era of austere budgets. This Guidebook is for you, the operators, who rely on Northrop Grumman systems every day to achieve mission success. It is a tool that incorporates over 40 years of data link experience to enhance your understanding of tactical data link capabilities and operational reach.

At Northrop Grumman, our mission is to be at the forefront of technology and innovation, delivering superior capability to help protect our nation's freedom and security, as well as the freedom and security of our allies. This Guidebook is one more small but important contribution to that mission.

I join the entire Northrop Grumman team in saluting and thanking you for your service.

P.S. Stanley
VADM, USN (Ret)
VP Cyber & C4 Government Relations
Northrop Grumman Corporation

About This Guidebook

This guidebook, *Understanding Voice and Data Link Networking*, has been developed to be used both for reference and review. Detailed information is presented in the text, with important points summarized in blue notes and in the figure captions. The format of this guidebook incorporates the following features:

- **Bold Type** — Important terms are printed in **bold** typeface the first time they appear, and a definition is given.
- **Illustrations** — Figures and diagrams are intended to complement the text. Their captions, also printed in blue, summarize important points.
- **Tables** — Facts are collected and summarized in tables to allow for quick lookups and comparisons.

A list of acronyms and abbreviations, a glossary, and a summary of training opportunities can be found at the back of the guidebook to enhance its use as a reference.

Acknowledgments

Northrop Grumman would like to acknowledge the following individuals for making this Guidebook possible:

Executive Editor
Daniel Akers

Technical Advisor
John Casey

Cover and Art Design
Mario Ruiz

Publications Head
Charlene Sivertson

Layout and Design
Dora Solorzano

Contributors and Reviewers
Mike Bennet
Bill Eddington
Gary Garcia
Carl Ivancic
David P. Johnson
Reginald Johnson
Tammy Morris
Bill Pigg
Vincenzo Sferra
Brad Van Every
Rose Wright

Editor Emerita
Special thanks to Jeanie Camp who initiated this guidebook and has provided inspiration and editorial leadership to the Understanding Link 16 and related guidebook series over the years until her recent retirement.

Table of Contents

NORTHROP GRUMMAN




Preface

Tactical Data Links (TDLs) provide a means to disseminate information processed from RADAR, SONAR, Identification Friend or Foe (IFF), Electronic Warfare, Self-Reporting, and visual observation. Each TDL uses a data link standard in order to provide communications via radio waves or data cables. These Military Standards (MIL-STD) set the message standards for data link interoperability.

This Guidebook focuses on the current TDLs used by the US Military, NATO, and other allies. Since this Guidebook is intended for public release, the content of this document is limited to overview information concerning TDLs. For more detailed information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Chapter 1: Introduction to Tactical Data Links

Introduction

Put simply, Tactical Data Links (TDLs) are a means to disseminate information processed from RADAR, SONAR, Identification Friend or Foe (IFF), Electronic Warfare, Self-Reporting and visual observation. During the Battle of Britain, RADAR allowed the allied forces to track "pieces of metal" in the sky. These "pieces of metal" were of course enemy bombers and fighters launching from various locations throughout Europe. Dissemination of these tracks at the time was done by voice communications which was difficult and slow.

Over time, aircraft began to fly faster and the need to disseminate that tactical data as quickly as possible became the priority. By the late 1950s, the Tactical Digital Information Link (TADIL) was born. Today we know them as TDL.

Each TDL uses a data link standard in order to provide communication via radio waves or data cables. These Military Standards (MIL-STD) set the message standards for data link interoperability.

Although not all inclusive, this Guidebook will focus on these current TDLs in use throughout the US Military, North Atlantic Treaty Organization (NATO) and by other allies.

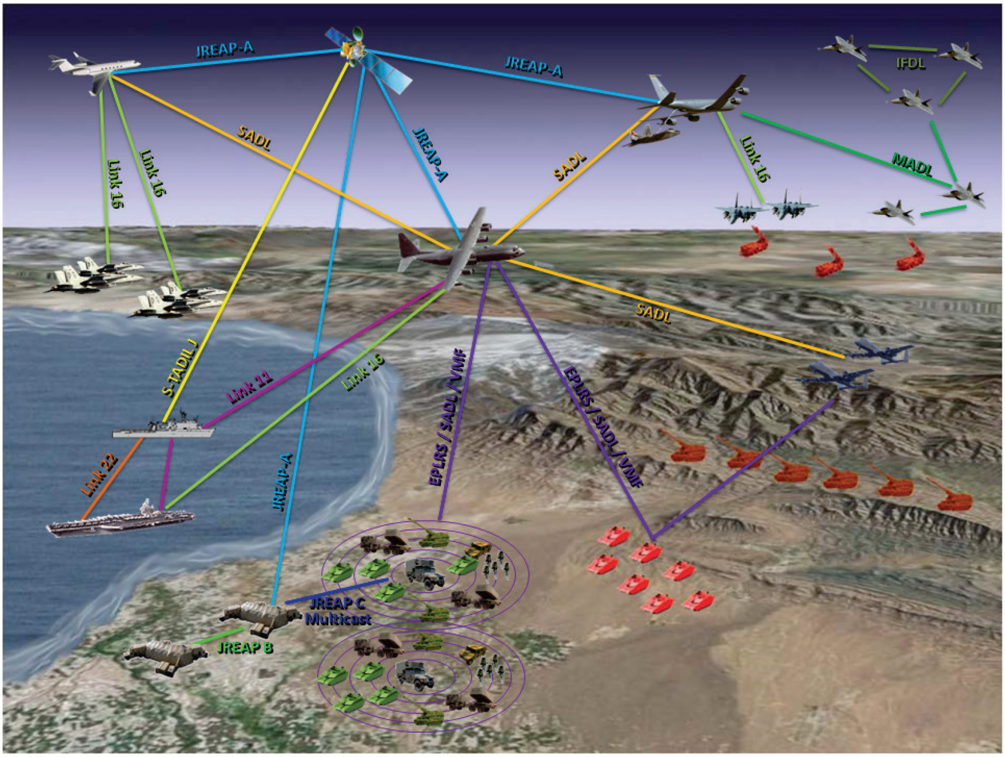


Figure 1-1. Example of Tactical Data Link (TDL) Usage.

□ Link 16

Link 16 employs the Joint Tactical Information Distribution System (JTIDS) and Multifunctional Information Distribution System (MIDS) data link terminals.
Link 16 is a frequency-hopping, jam-resistant, high-capacity data link. Operating on the principle of Time Division Multiple Access (TDMA), wherein 128 time slots per second are allocated among participating JTIDS Units (JUs), time slots are organized into multiple functional Network Participation Groups (NPGs). Link 16 includes elements of Link 11/Link 11B and Link 4A/Link 4C, while providing many new or improved capabilities, including voice.

Link 11

Link 11 employs netted communication techniques and standard message formats for the exchange of digital information among airborne, land-based and ship-board tactical data systems. Providing mutual exchange of information among net participants using high-frequency (HF) or ultra high-frequency (UHF) radios, Link 11 is a half-duplex, netted, secure data link. Link 11 requires a Net Control Station (NCS) and Participating Units (PUs) to operate.

Link 22

Link 22 is a NATO secure radio system that provides Beyond Line-of-Sight (BLOS) communications. It interconnects air, surface, subsurface and ground-based tactical data systems, and is used for the exchange of tactical data among the military units of the participating nations.

VMF

The Variable Message Format (VMF) is a message standard (K-series messages) that uses communication protocols that are transmission media independent.

EPLRS

The Enhanced Position Location Reporting System (EPLRS) is a high capacity TDL that can provide simultaneous voice, data and situation awareness (SA). It is a self forming, self healing mesh network that automatically relays from one radio to another.

SADL

The Situation Awareness Data Link (SADL) is an air-ground EPLRS application used by both the US Air Force and US Army as an anti-fratricide measure. Fully integrated into Close Air Support (CAS) aircraft, SADL can be used in three types of networks:

- Air-to-Air – for airspace SA
- Air-to-Ground – for interoperability with EPLRS-equipped units
- Gateway – two-way exchange of SADL and Link 16 SA/Command and Control (C2)

JREAP

Joint Range Extension Application Protocol (JREAP) is an application protocol that enables the transmission of tactical data link messages over media that was not originally designed for TDLs. Supported communication media are:

- Satellite communications – JREAP A
- Point-to-Point – JREAP B
- IP Networks – JREAP C

IFDL

The Intra-Flight Data Link (IFDL) is a low probability of intercept (LPI), low probability of detection (LPD) secure data link that was developed to provide data connectivity between F-22 aircraft.

MADL

The Multifunctional Advanced Data Link (MADL) is a high data rate, K-band communication link with LPI and LPD characteristics. The objective of MADL is to provide an airborne data link that supports cooperative engagements between stealth aircraft without compromising stealth observability performance.

Tactical Gateways and Voice Bridging

Tactical gateways and voice bridging are not TDLs in themselves; rather, they make the performance of TDLs and radio communications more effective, secure and assured across an entire theatre of operations—whether military or civilian. Tactical gateways and voice bridging can provide a major improvement in communication by leveraging hardware, software and—in the case of airborne tactical gateways—high altitude—to overcome line of sight (LOS) limitations from terrain, and incompatible frequencies among allied forces on the battlefield or emergency responders at the scene of a natural disaster.

OSI Reference Model

The Open Systems Interconnection (OSI) reference model is a conceptual model developed by the International Organization for Standardization (ISO). The model envisions a communication system partitioned into abstraction layers. The OSI reference model has been used for constructing many computer communication protocols. It is useful for defining where functionality in communication protocols should occur.

The OSI reference model consists of seven layers. Each layer of the OSI provides a service, or capability, to the next higher level in the model. The highest four levels—Application, Presentation, Session, and Transport—are commonly host layers, while Network, Data Link, and Physical are considered network layers. Not every layer of the reference model is used in all communication protocols, nor are the layers always explicitly unique. For example, message and message transmission security are not isolated to any particular layer of the OSI reference model and can be applied at all layers.

Layer 7 – Application

The Application Layer is responsible for interacting with the Operating System and the applications that are executed by that operating system. The Application Layer is not software programs, although some programs may perform application layer functions, but rather protocols that ensure applications can interact with the lower layers of the communication stack. JREAP is an example of an application layer protocol, the JREAP standard defines the message structure of the data that is created by a Joint Range Extension (JRE) Processor.

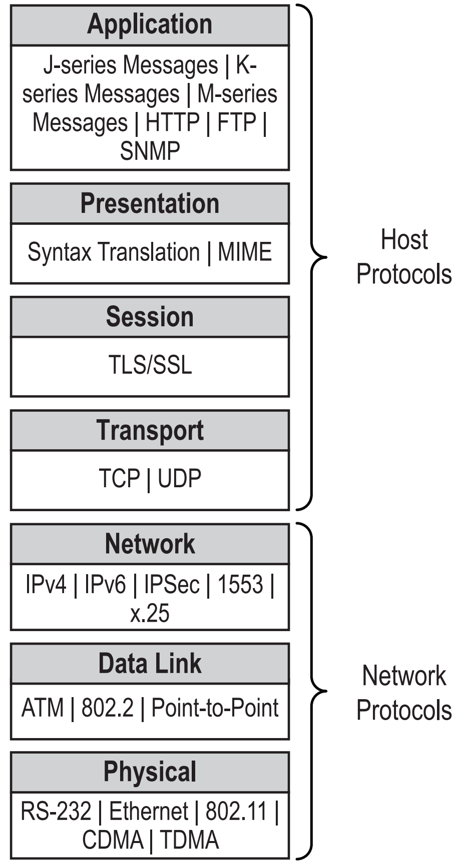


Figure 1-2. OSI Reference Model.

Layer 6 – Presentation

The Presentation Layer is responsible for ensuring that the data presented to the Application Layer is properly formatted and can be understood. An example of Layer 6 is the translation of little-endian to big-endian. Endian is a term used to describe how data is stored in a computer's memory. The little-endian format stores the least significant bit (LSB) in the lowest memory address, and the big-endian stores the most significant bit (MSB) in the lowest memory address. If two computer systems, Computer A and Computer B, need to talk and Computer A uses little-endian and Computer B uses big-endian, the Presentation Layer will handle the translation between the two different formats.

Layer 5 – Session

The Session Layer is responsible for establishing and managing connections between computers.

■ Layer 4 - Transport

The Transport Layer is responsible for ensuring that packets of data are reliably sent and received between computers. The Transport Layer commonly includes methods of error detection and correction, flow control, message segmentation, and message re-assembly. Common protocols found at this layer are Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP).

■ Layer 3 – Network

The Network Layer is responsible for handling addressed messages and in some protocols, separating messages into smaller packets that can be reliably transmitted on the network. A very common protocol that operates at this layer is Internet Protocol (IP).

■ Layer 2 – Data Link

The Data Link Layer is responsible for ensuring that a connection between hosts on a network is established and reliable. Layer 2 often provides services to Layer 1 to detect and correct errors that occur in physical transmission.

■ Layer 1 – Physical

The Physical Layer is responsible for the electrical transmission of data. This is often implemented as a cabling standard or a radio wave form. Common cable standards include Ethernet, RS-232, and RS-422. Some radio wave forms that many are familiar with that are defined here are 802.11a/b/g/n, TDMA, and Code Demand Multiple Access (CDMA).

While not all tactical data links fit neatly into the OSI Reference Model, the OSI can be used to visualize how functionality within each Data Link stacks to ensure that reliable communications are managed.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Introduction

Link 16 employs the Joint Tactical Information Distribution System (JTIDS) and Multifunctional Information Distribution System (MIDS) data link terminals. Link 16 is a frequency-hopping, jam-resistant, high-capacity data link. Operating on the principle of Time Division Multiple Access (TDMA), wherein 128 time slots per second are allocated among participating JTIDS Units (JUs), time slots are organized into multiple functional Network Participation Groups (NPGs). This chapter provides an overview of the Link 16 Tactical Data Link (TDL).

Part 1 Introduction to Link 16

Link 16 is the designation of a TDL that is being fully integrated into operations of the Joint Services, the forces of the North Atlantic Treaty Organization (NATO), and other allies. It is anticipated that the number of Link 16-equipped platforms will approach 5000 by the year 2015.

This section summarizes the Link 16 TDL capabilities. You will learn what is provided by the Link 16 message structure and waveform.

Section A

Overview

The general purpose of Link 16 is the exchange of near-real-time tactical data among joined units. Link 16 does not significantly change the basic concepts of tactical data link information exchange supported for many years by Link 4A, Link 11, and Link 11B. Rather, Link 16 enhances tactical employment of all equipped platforms and provides certain technical and operational improvements to existing tactical data link capabilities, which include:

- Nodelessness
- Jam resistance
- Improved security
- Increased data rate (throughput)
- Increased volume and granularity of information exchange
- Reduced data terminal size, allowing installation in fighter and attack aircraft
- Digitized, jam-resistant, secure voice capability
- Relative navigation
- Precise Participant Location and Identification (PPLI)

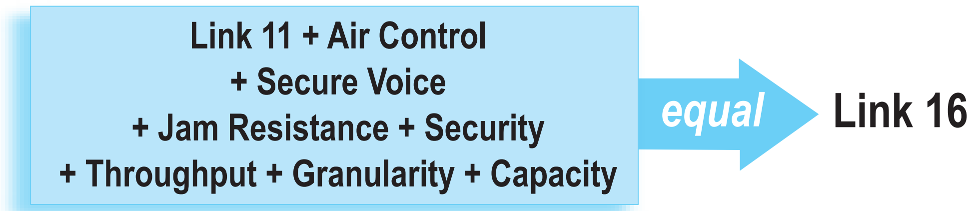


Figure 2-1. Whereas Link 16 is functionally similar to the capabilities of Link 11, it provides technology and capabilities not available in this legacy link.

Link 16 History

Link 16 Beginnings

The TDLs, formerly known as Tactical Digital Information Links (TADILs)[1], were developed in conjunction with digital computers to permit Joint and Coalition forces to exchange information across a digital interface. Link 11 (the former TADIL A) and Link 11B (the former TADIL B) were designed to enable eight-bit computers to share near-real-time surveillance and command data among functionally supporting units in the performance of their missions. Link 16, formerly known as TADIL J, was developed as a modernized, replacement upgrade to these links to reflect later 16-bit requirements.

Link 16 development began in the 1970s. Link 16 initially became operational in the United States Military during the mid-to-late 1980s, with the introduction of the Class 1 JTIDS terminal. Although these platforms processed only the Interim JTIDS Message Specification (IJMS), this was the beginning of the Link 16 evolution.

The JTIDS Class 2 terminal was designed to be installed in multiple types of platforms. Initially, the terminal was integrated into an aircraft platform as a test-only implementation to support a terminal developmental and operational evaluation, which took place during 1986 and 1987. After a successful test, an integration kit and software were developed for operational implementation of Link 16 into military aircraft. For a variety of reasons, however, in the late 1980s it was decided to limit the deployment of Link 16 to its Command and Control (C2) platforms.

---

1 DISA ICP TM00-019.

In early 1992, it was decided to look at the utility of data links in various aircraft and a data link Operational Special Project (OSP) was initiated. JTIDS Class 2 terminals[2] were installed in the military aircraft using the already developed integration kits and software. The success of this OSP led reevaluation plans regarding data links in nonC2 platforms for military aircraft.

In the late 1990s, the JTIDS Class 1 terminal was replaced with the JTIDS Class 2H terminal, and the JTIDS Class 1 terminal was replaced with the JTIDS Class 2 Modular Control Equipment (MCE) terminal. Additionally, Link 16 was implemented on other airborne platforms.

□ *Terminology*

■ Link 16

Throughout this guidebook, the term **"Link 16"** refers to the tactical data link that is specified in the Message Standard for Link 16, the MIL-STD-6016 series. All information about Link 16 contained therein applies equally to Joint Service and NATO operations. You may also have heard the term "TADIL J." This term, which is no longer in use, was synonymous with the term "Link 16."

■ Link 16 Host

A Tactical Data System (TDS) that incorporates Link 16 functionality can sometimes be referred to as a **"Link 16 Host"** platform.

■ Link 16 Network

A Link 16 Network is an accumulation of TDSs participating in a predefined exchange of tactical data via radio frequency (RF) signals operating within line-of-sight (LOS) of other participants in the network.

---

2 *Beginning in FY 2007, the JTIDS Class 2 terminals were replaced with MIDS LVT-3 terminals.*

■ Link 16 Terminal

The word **"terminal"** is used throughout this guidebook to refer generically to a number of radio sets that are used to transmit and receive tactical data to and from a Link 16 RF networ:

- The acronym **"JTIDS"** refers to the Joint Tactical Information Distribution System, the first-generation Link 16 terminal. It encompasses the Class 1 and Class 2 terminals' software, hardware, and RF equipment, as well as the high-capacity, secure, antijam waveform that they generate.
- The **Multifunctional Information Distribution System** (MIDS) **Low-Volume Terminal** (LVT) is the second generation of Link 16 terminals. Many variants of this terminal, designated LVT 1 through LVT 11, have been produced, each unique in its interface and programming.
- The next generation of Link 16-capable radios will be the **Joint Tactical Radio System** (JTRS) and **MIDS JTRS**.

JTIDS or MIDS is the software, hardware, RF equipment, and waveform of Link 16.

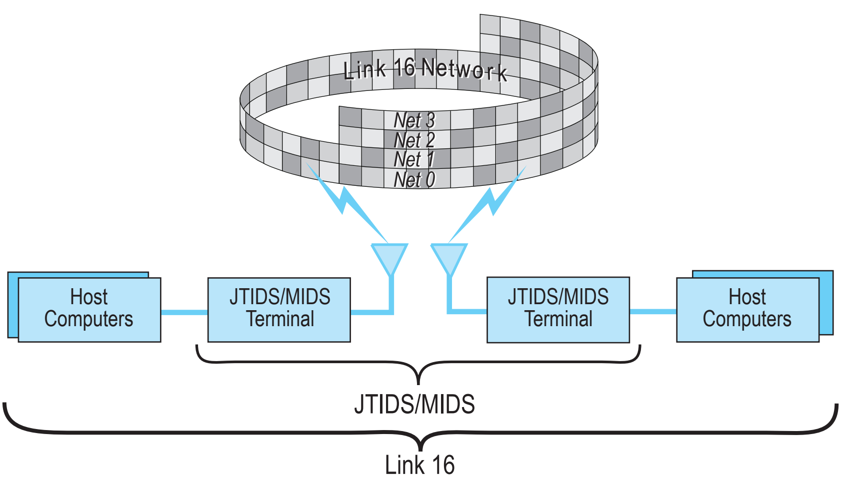


Figure 2-2. Tactical data is shared among friendly units equipped with Tactical Data Systems over Link 16 using JTIDS and MIDS terminals.

■ TDL Messages

Link 11 messages, designated the **M-series messages**, are preformatted messages used to convey tactical data on Link 11. Link 16 messages, or **J-series messages**, are preformatted messages used to convey tactical data on Link 16. **IJMS Messages** are formatted according to the early IJMS, which was implemented in the first JTIDS Class 1 terminals.

IJMS is not fully compatible with modern Link 16.

Section B

The Link 16 J-series Messages

Like other tactical data links, Link 16 conveys its information in specially formatted messages. These message formats are composed of sets of fields, each of which is composed, in turn, of prescribed numbers of bits that may be encoded into predetermined patterns to convey specific information. The messages exchanged over Link 16 between participating Link 16 units are called the J-series messages.

Link 16 is the exchange of tactical data using J-series message formats.

☐ Message Structure

Each J-series message format is identified by both a label and a sublabel. For a J12.6 Target Sorting message, for example, the "J" indicates Link 16, the "12" is the message label, and the ".6" is the message sublabel. Since the label field is five bits wide (for 32 labels) and the sublabel field is three bits wide (for eight subcategories), there are 256 possible message definitions (32 x 8 = 256). Not all 256 possible label and sublabel combinations, however, represent actual messages, as you will observe in *Figure 2-3*.

Up to 256 different J-series messages may be defined.

J-message Type		Message Sub-labels							
		x.0	1.1	x.2	x.3	x.4	x.5	x.6	x.7
Message Labels	J0.x	J0.0	J0.1	J0.2	J0.3	J0.4	J0.5	J0.6	J0.7
	J1.x	J1.0	J1.1	J1.2	J1.3	J1.4	J1.5	J1.6	J1.7
	J2.x	J2.0	J2.1	J2.2	J2.3	J2.4	J2.5	J2.6	J2.7
	J3.x	J3.0	J3.1	J3.2	J3.3	J3.4	J3.5	J3.6	J3.7
	J4.x	J4.0	J4.1	J4.2	J4.3	J4.4	J4.5	J4.6	J4.7
	J5.x	J5.0	J5.1	J5.2	J5.3	J5.4	J5.5	J5.6	J5.7
	J6.x	J6.0	J6.1	J6.2	J6.3	J6.4	J6.5	J6.6	J6.7
	J7.x	J7.0	J7.1	J7.2	J7.3	J7.4	J7.5	J7.6	J7.7
	J8.x	J8.0	J8.1	J8.2	J8.3	J8.4	J8.5	J8.6	J8.7
	J9.x	J9.0	J9.1	J9.2	J9.3	J9.4	J9.5	J9.6	J9.7
	J10.x	J10.0	J10.1	J10.2	J10.3	J10.4	J10.5	J10.6	J10.7
	J11.x	J11.0	J11.1	J11.2	J11.3	J11.4	J11.5	J11.6	J11.7
	J12.x	J12.0	J12.1	J12.2	J12.3	J12.4	J12.5	J12.6	J12.7
	J13.x	J13.0	J13.1	J13.2	J13.3	J13.4	J13.5	J13.6	J13.7
	J14.x	J14.0	J14.1	J14.2	J14.3	J14.4	J14.5	J14.6	J14.7
	J15.x	J15.0	J15.1	J15.2	J15.3	J15.4	J15.5	J15.6	J15.7
	J16.x	J16.0	J16.1	J16.2	J16.3	J16.4	J16.5	J16.6	J16.7
	J17.x	J17.0	J17.1	J17.2	J17.3	J17.4	J17.5	J17.6	J17.7
	J18.x	J18.0	J18.1	J18.2	J18.3	J18.4	J18.5	J18.6	J18.7
	J19.x	J19.0	J19.1	J19.2	J19.3	J19.4	J19.5	J19.6	J19.7
	J20.x	J20.0	J20.1	J20.2	J20.3	J20.4	J20.5	J20.6	J20.7
	J21.x	J21.0	J21.1	J21.2	J21.3	J21.4	J21.5	J21.6	J21.7
	J22.x	J22.0	J22.1	J22.2	J22.3	J22.4	J22.5	J22.6	J22.7
	J23.x	J23.0	J23.1	J23.2	J23.3	J23.4	J23.5	J23.6	J23.7
	J24.x	J24.0	J24.1	J24.2	J24.3	J24.4	J24.5	J24.6	J24.7
	J25.x	J25.0	J25.1	J25.2	J25.3	J25.4	J25.5	J25.6	J25.7
	J26.x	J26.0	J26.1	J26.2	J26.3	J26.4	J26.5	J26.6	J26.7
	J27.x	J27.0	J27.1	J27.2	J27.3	J27.4	J27.5	J27.6	J27.7
	J28.x	J28.0	J28.1	J28.2	J28.3	J28.4	J28.5	J28.6	J28.7
	J29.x	J29.0	J29.1	J29.2	J29.3	J29.4	J29.5	J29.6	J29.7
	J30.x	J30.0	J30.1	J30.2	J30.3	J30.4	J30.5	J30.6	J30.7
	J31.x	J31.0	J31.1	J31.2	J31.3	J31.4	J31.5	J31.6	J31.7

Figure 2-3. The possible J-series messages are shown. Light cells denote defined messages, and gray cells denote messages that have not yet been specifically defined.

Within the J-series message set are messages for network management, friendly status, surveillance, electronic warfare, weapons employment, imagery, and track management. The currently defined messages are described in *Figure 2-4*.

In both ground-based and airborne systems, the J-series messages are processed directly by the tactical or mission computer. Certain ground-based systems can also perform a second function: the forwarding of data in both directions between Link 16 and Link 11/11B.

MSG	Message Title	Purpose
J0.0	Initial Entry	Provides the data elements, in a known time slot, required for net entry.
J0.1	Test	Used for terminal test and performance evaluation.
J0.2	Network Time Update	Adjusts the system time to a standard time.
J0.3	Time Slot Assignment	Permits dynamic assignment of time slots.
J0.4	Radio Relay Control	Provides the means for the JU responsible for relay control to assign and deassign the paired slot radio relay function to a terminal and to control the relay function parameter.
J0.5	Repromulgation Relay	Requests that those messages in the same time slot containing the J0.5 message be relayed by all JUs receiving the message.
J0.6	Communications Control	Initiate or terminates specific transmissions to control communications, and requests network management actions.
J0.7	Time Slot Reallocation	Provides the capability for a JU to request a percentage of time slots from a shared pool and disseminate the requests of other JUs.
J1.0	Connectivity Interrogation	Solicits direct or indirect connectivity of the addressed JUs to support route establishment.
J1.1	Connectivity Status	Disseminates direct or multilevel connectivity of the source JUs.
J1.2	Route Establishment	Establishes a route for relay/destination control.
J1.3	Acknowledgment	Used by a JU involved in ground-to-ground communications to respond to messages that require machine receipt/compliance.
J1.4	Communicant Status	Used by JUs to report the connectivity quality of its direct communicants to Net Control Station (NCS) and other direct communicants.

Figure 2-4. The J-series messages (continued on next page)

MSG	Message Title	Purpose
J1.5	Net Control Initialization	Provides a number of initial terminal parameters required to allow a terminal to actively participate in an established net under the control of a dynamic net manager.
J1.6	Needline Participation Group Assignment	Used by the designated NCS to assign an addressed JU its associated destination Source Track Numbers (STNs) with Participation Group (PG) numbers to form Needline PGs.
J2.0	Indirect Interface Unit PPLI	Provides Participating Unit/Reporting Unit/Generic Unit information on the Link 16 network when network participation status, identification, and positional information is forwarded from Link 11/11B.
J2.2	Air PPLI	Provides all JUs information about airborne JUs on the Link 16 network. It is used by airborne JUs to provide network participation status, identification, positional information, and relative navigation information.
J2.3	Surface PPLI	Provides all JUs information about surface JUs on the Link 16 network. It is used by surface JUs to provide network participation and relative navigation information.
J2.4	Subsurface PPLI	Provides all JUs information about subsurface JUs on the Link 16 network. It is used by subsurface JUs to provide network participation status, identification, positional information, and relative navigation information.
J2.5	Land Point PPLI	Provides all JUs information about stationary ground JUs on the Link 16 network. It is used by stationary ground JUs to provide network participation status, identification, positional information, and relative navigation information.
J2.6	Land Track PPLI	Provides all JUs information about mobile ground JUs on the Link 16 network. It is used by mobile ground JUs to provide positional information, and relative navigation information.
J3.0	Reference Point	Used to exchange tactical information about geographic references.
J3.1	Emergency Point	Provides the location and type of an emergency that requires search and rescue.
J3.2	Air Track	Used to exchange information on air tracks.
J3.3	Surface Track	Used to exchange information on surface tracks.
J3.4	Subsurface Track	Used to exchange information on subsurface tracks and Datums.
J3.5	Land Point/Track	Used to exchange tactical surveillance information on land points and tracks.

Figure 2-4. The J-series messages (continued on next page)

MSG	Message Title	Purpose
J3.6	Space Track	Exchanges information on Space and Ballistic Missile tracks.
J3.7	Electronic Warfare Product Information	Provides the means to exchange tactically significant information that has been derived from electromagnetic sources.
J5.4	Acoustic Bearing/ Range	Used to report acoustic bearing and range of subsurface contacts.
J6.0	Amplification	Used to exchange amplifying information, including threat information, within the interface.
J7.0	Track Management	Used to transmit information necessary to effect management actions on tracks being reported within the interface. Management actions include dropping tracks, reporting environment/category and identity conflicts, changing environment/category and identity, changing alert status, and changing strength.
J7.1	Data Update Request	Used to request tactical information that has been locally generated by units participating within the interface.
J7.2	Correlation	Used to resolve a dual designation problem by identifying one track to be retained and another to be dropped.
J7.3	Pointer	Used to transmit a geographic position to an addressed unit within the interface.
J7.4	Track Identifier	Used to transmit special identification numbers associated with the reference track number (TN).
J7.5	IFF/SIF Management	Used to transmit Identification Friend or Foe/Selective Identification Feature (IFF/SIF) information or a special code on a referenced track. Provisions are available to obtain the most current information by exchanging, clearing, or updating IFF/SIF data between units within the interface.
J7.6	Filter Management	For foreign agency use
J7.7	Association	Used to transmit information, on two or more TNs, that has been automatically or manually associated when the information is deemed to pertain to the same contact. When a determination is made that the relationship above no longer exists, there is a provision for terminating this information association.
J8.0	Unit Designator	Used to transmit to a terminal (from its NCS) the unit designator associated with the TNs in the terminal's Participation Group assignments. The message will also be used to inform an NCS of a terminal's unit designator.

Figure 2-4. The J-series messages (continued on next page)

MSG	Message Title	Purpose
J8.1	Mission Correlator Change	Used to add, delete, or change Mission Correlators on a specific aircraft or flight of aircraft.
J9.0	Command	Provides the means to transmit threat warning conditions, alert states, and weapons condition orders, to direct weapon system engagement for air defense and air support, and to direct Anti-Submarine Warfare (ASW) operations.
J9.1	Engagement Coordination	Provides the means for two or more elements to coordinate engagement, to conduct more efficient engagement, and to reduce the probability of wasted resources.
J9.2	ECCM Coordination	Provides the means to coordinate and direct Electronic Counter-Countermeasures (ECCM) activities among C2 JUs.
J10.2	Engagement Status	Provides the status of an engagement between the Reference TN and the Target TN.
J10.3	Handover	Used to transfer control of aircraft and remotely piloted vehicles/ missiles between controlling units.
J10.5	Controlling Unit Report	Used to identify the JU that is controlling the track and to provide the Mission Correlator and/or voice call sign.
J10.6	Pairing	Provides a means to indicate a pairing (not engagement status) between a friendly track and another track or point.
J11.0	Weapon Response/ Status (1)	Provides weapon compliance responses to controller directives.
J11.1	Weapon Directives (1)	Provides controller directives to a weapon.
J11.2	Weapon Coordination (1)	Used to coordinate the transfer of control authority and the delegation of third party source.
J12.0	Mission Assignment	Used by C2 JUs and optionally by nonC2 JUs to assign missions, designate targets, and provide target information to nonC2 platforms. NonC2 JU acknowledgement of this message is through Receipt/ Compliance (R/C) action.
J12.1	Vector	Used by C2 JUs to send vector information and vector discretes specifically to air units operating on its net. Vectors are given for interception of air targets, navigation, and air traffic control.
J12.2	Precision Aircraft Directions	Used by controlling units for operations requiring precise control positioning of mission aircraft (for example, ground-directed release of ordinance, automatic carrier landing operations, etc.)

Figure 2-4. The J-series messages (continued on next page)

MSG	Message Title	Purpose
J12.3	Flight Path	Used by controlling units to provide air units with multiple-leg flight path information.
J12.4	Controlling Unit Change	Used to provide new control agency information to an aircraft prior to handoff to the new control agency. It is also used by a tactical aircraft to initiate control procedures with a new controlling unit or to effect a change of controlling unit in response to a Controlling Unit Change (CUC) Order or by a C2 JU to initiate control by own unit.
J12.5	Target/Track Correlation	Used by controlling C2 JUs to: • Correlate a target and a track, • Decorrelate a target and a track, and • Correlate multiple targets with a track.
J12.6	Target Sorting	Used to: • Enable nonC2 JUs to exchange targets and targeting information among themselves, • Pass sensor data to C2 JUs and among nonC2 JUs, • Pass nonC2 JU engagement status information between nonC2 JUs and from nonC2 JUs to C2 JUs, and; • Provide control among nonC2 JUs.
J12.7	Target Bearing	Used by nonC2 JUs to: • Exchange target reports using polar coordinates, and may include range, bearing, elevation, rate, and uncertainty data, and; • Pass sensor data to JUs.
J13.0	Airfield Status	Reports operational status of airfields, runways, airfield facilities, and aircraft carrier flight decks.
J13.2	Air Platform and System Status	Provides the current status of an air platform including ordnance load, fuel, operational status, and on-board systems' status.
J13.3	Surface Platform and System Status	Provides the current status of a surface platform including ordnance load, operational status and on-board systems' status.
J13.4	Subsurface Platform and System Status	Provides the current status of a subsurface platform to include operational status and on-board systems' status.
J13.5	Land Platform and System Status	Provides the current operational weapons and equipment status of a land platform.
J14.0	Parametric Information	Provides the means to exchange parametric information that has been derived from electromagnetic sources.

Figure 2-4. The J-series messages (continued on next page)

MSG	Message Title	Purpose
J14.2	EW Control/ Coordination	Provides the means for Electronic Warfare (EW) participants to coordinate EW activities among themselves.
J15.0	Threat Warning	Provides the capability for threat warning to targeted friendly platforms, including Threat Type, Threat Posture, Position/Relative Position, Altitude, and Speed.
J16.0	Image Transfer Message	Provides the capability to transmit and receive imagery.
J17.0	Weather Over Target	Provides the current weather conditions over a target area.
J28.x	Series	Purpose is defined by country and service of user.
J29.x	Series	Purpose is defined by country and service of user.
J30.x	Series	Purpose is defined by country and service of user.
J31.0	Over-the-Air Rekeying Management	Used to exchange cryptonet management information for rekeying the KGV-8.
J31.1	Over-the-Air Rekeying	Used to transmit the new cryptovariables.
J31.7	No Statement	Used to fill out the remainder of a transmission opportunity when the messages to be transmitted do not require the full number of Reed-Solomon code words.
Round-Trip Timing (RTT)		
RTT-A	Round-Trip Timing Interrogation – Addressed	Provides the means for a terminal to synchronize with system time using the active synchronization procedure. A specific terminal is interrogated and responds with the RTT Reply.
RTT-B	Round-Trip Timing Interrogation – Broadcast	Provides the means for a terminal to synchronize with system time using the active synchronization procedure. The RTT-B is not addressed to any particular terminal. Any terminal that meets the specified requirement for time quality level responds with the RTT Reply.
RTT-REP	Round-Trip Timing Reply	Provides the means for a terminal to support the active synchronization procedure of another JU by providing time-of-arrival data in response to either an RTT-A or RTT-B Interrogation.

Figure 2-4. The J-series messages convey tactical information in preformatted messages.

Section C

Overview of Link 16 Architecture

Link 16 uses the principle of **Time Division Multiple Access** (TDMA), an automatic function of the Link 16 terminal. The TDMA architecture uses time interlacing to provide multiple and apparently simultaneous communications nets. All JTIDS Units, or JUs, are pre-assigned sets of time slots in which to transmit their data and in which to receive data from other units. Each time slot is 1/128 second, or 7.8125 milliseconds (ms), in duration.

One second contains 128 times slots.

Fifty-one frequencies are available for JTIDS transmissions. The frequency is not held constant during the time slot but is changed rapidly (every 13 microseconds) according to a predetermined pseudorandom pattern. This technique is called **frequency hopping**.

Link 11 uses one frequency; Link 16 uses 51 frequencies.

☐ Networks and Nets

A Link 16 **network** is a collection of participants, all of which are in synchronization and share a common understanding of where the time slot boundaries occur. The set of all time slots held by all participants can also be considered a network.

A network is the superset of all time slots and all users in synchronization.

A **net**, on the other hand, is a subset of time slots belonging to a Link 16 network, as well as the participants that share this subset of time slots. Link 16 nets are differentiated by their frequency-hopping patterns. Multiple nets in a network can be "stacked" or "multinetted" by allowing time slots to be used redundantly, with the data transmitted in each net on different frequencies. Each net is assigned a number that designates a particular hopping pattern.[3]

A net is a subset of the network's time slots, and its particular users.

A Link 16 network may consist of one or more nets. The operable nets are numbered from 0 to 126, providing up to 127 operable nets in a Link 16 network, although typically, no more than three to six are ever utilized at one time during network execution. During any given time slot, therefore, a unit is either transmitting or receiving on one of a possible 127 nets.

Theoretically, a network can have up to 127 simultaneous nets.

The operable Link 16 net numbers are downloaded to the terminal automatically with the network design. Net number 127, however, is reserved for a special use. When a network design specifies "Net 127," this means that an operator using this net will find its actual specification elsewhere—normally in the Operational Tasking Data Links (OPTASK LINK) message—and will have to manually set the net number during terminal initialization to a net number between 0 and 126.

"Net 127" requires operator action. Find the actual net numbers for "Net 127" functions in the OPTASK LINK.

3 *Stacked nets are discussed in Section D.*

Figure 2-5. JTIDS units automatically transmit, receive, and relay data at pre-assigned times on pre-assigned nets based on instructions given to their terminals when they are initialized. These pre-assignments are determined in advance of operations to support the expected information exchange requirements of the force.

Data Exchange

Transmission Types

Link 16 transmits 3, 6, or 12 Link 16 data words during a 7.8125-ms time slot, depending on whether it uses the Standard, Packed-2, or Packed-4 data packing structure. A Link 16 data word is analogous to a Link 11 frame. Each Link 16 **data word** contains 70 bits of data.

Four types of transmissions are possible:

- Fixed Word Format (FWF)
- Free Text (FT)
- Variable Message Format (VMF)
- Round-Trip Timing (RTT)

J-series messages are always sent in fixed-format transmissions.

Section D

Features of the Link 16 Architecture

The features of the unique Link 16 architecture that result in improved communication are described in this section.

☐ Nodelessness

A node is a unit required to maintain communications. On a Link 11 net, for example, the NCS is a node. If the NCS goes down, the link goes down. In Link 16 there are no nodes. Time slots are pre-assigned to each participant, and the link will function regardless of the participation of any particular unit. The closest thing in Link 16 to a node is the Network Time Reference (NTR). An NTR is needed to start up a network and for a new unit to synchronize with and enter a network.

Link 16 was designed to operate without a single point of failure.

After a network has been established, a Link 16 participant can operate for hours when an NTR is lost, if its clock is sufficiently warmed up. Time quality declines rapidly, however, and with it, navigation quality also declines. If your application relies on Link 16 navigation, you are encouraged, with relative time-based networks, to maintain an NTR at all times so that time qualities remain sufficiently high to navigate, with transitions in the NTR role held to about 10 minutes or less.

☐ Security

Both the message and the transmission are encrypted. The message is encrypted by the encryption device for JTIDS, in accordance with a cryptovariable specified for **message security**, or **MSEC**. **Transmission security**, or **TSEC**, is provided by the same cryptovariable or by a second cryptovariable, which controls the specifics of the JTIDS/MIDS waveform. For MIDS, the MSEC and TSEC are provided by a circuit board embedded in the terminal.

One important feature of this waveform is its use of frequency hopping. The hopping pattern is determined by both the net number and the TSEC cryptovariable. The instantaneous relocation of the carrier frequency spreads the signal across the spectrum. The TSEC cryptovariable also determines the amount of jitter in the signal, as well as a predetermined, pseudorandom pattern of noise that is mixed with the signal prior to transmission.

Cryptovariable	Type of Security
MSEC	Encryption of message data
TSEC	Encryption of JTIDS waveform: • Jitter • Pseudorandom noise • Frequency-hopping pattern

Figure 2-6. Link 16 uses two types of security: both the message and the transmission are encrypted.

☐ Network Participation Groups

The time slots of a net can be parceled out to one or more Network Participation Groups (NPGs). An NPG is defined by its function, and thus also by the types of messages that will be transmitted on it. The currently existing NPGs are shown below.

NPG	Functional Group
1	Initial Entry
2 and 3	Round-Trip Timing
4	Network Management
5 and 6	Precise Participant Location and Identification; Platform and System Status
7	Surveillance
8	Mission Management/Weapons Coordination
9	Air Control
10	Electronic Warfare
11	Imagery
12	Voice Group A

Figure 2-7. Network capacity (continued on next page)

NPG	Functional Group
13	Voice Group B
14	Indirect PPLI
17	Unassigned
18	Network Enabled Weapons
19 and 20	Fighter-to-Fighter Communications
21	BMD Operations (1)
22	Composite A
23	Composite B
25	Reserved for Future Joint Uses
26	Unassigned
27	Joint PPLI
28	Distributed Network Management
29	Residual Message (Fixed-Format Text)
30	IJMS Position and Status
31	IJMS Messages
32 through 511	Needlines

Notes:
(1) Name changed from Engagement Coordination by ICP TM06-07 Ch1.

Figure 2-7. Network capacity is allocated into functional groups, called NPGs, which are dedicated to specific purposes.

This division of the network into functional groups allows JUs to participate on only the NPGs used for functions that they perform.

☐ Stacked Nets and Multinetting

Theoretically, Link 16 can support up to 127 possible nets (numbered 0 to 126), each operating in the same network at the same time. However, only between 20 and 30 can coexist without interfering with one another during actual operations. To achieve this multiple net capability, either of the two techniques described below may be employed.

Stacked Nets

Transmission in the same time slots, the same NPG, but on different operator-selectable net numbers, is known as **stacked nets**. The affected time slots will share the TSEC, and may also share the MSEC, cryptovariables. Stacked nets are always designated by their assignment to “Net 127” in network description documents. By convention, designating a net number “127” indicates that the operator will select the actual net number later, from specific instructions in the OPTASK LINK message. NPG 9 (Air Control) and NPGs 12 and 13 (Voice) are examples of stacked net applications where operators can perform the same function on different nets.

Stacked nets: data transmitted in the same time slots and NPG, but on different nets.

For each time slot, a JU is either transmitting or receiving on one net. To use the stacked net structure, the participants on each net must be mutually exclusive. Stacked nets are particularly useful for air control purposes with mutually exclusive sets of controlling units and controlled aircraft. They are also used for voice communications, providing a potential for 127 different, operator-selectable voice circuits for each of the two voice NPGs.

Multinetting

Transmission in the same time slots, but on different net numbers, is known as **multinetting**. *These transmissions may or may not be on different NPGs*. C2 platforms exchanging EW data at the same time fighters are exchanging fighter-to-fighter data is an example of multinetting.

The separation of data is accomplished by each different net number using a different, distinct frequency-hopping pattern, which is determined by the TSEC cryptovariable and the net number.

Multinetting: data transmitted in the same time slots, but on different NPGs and net numbers.

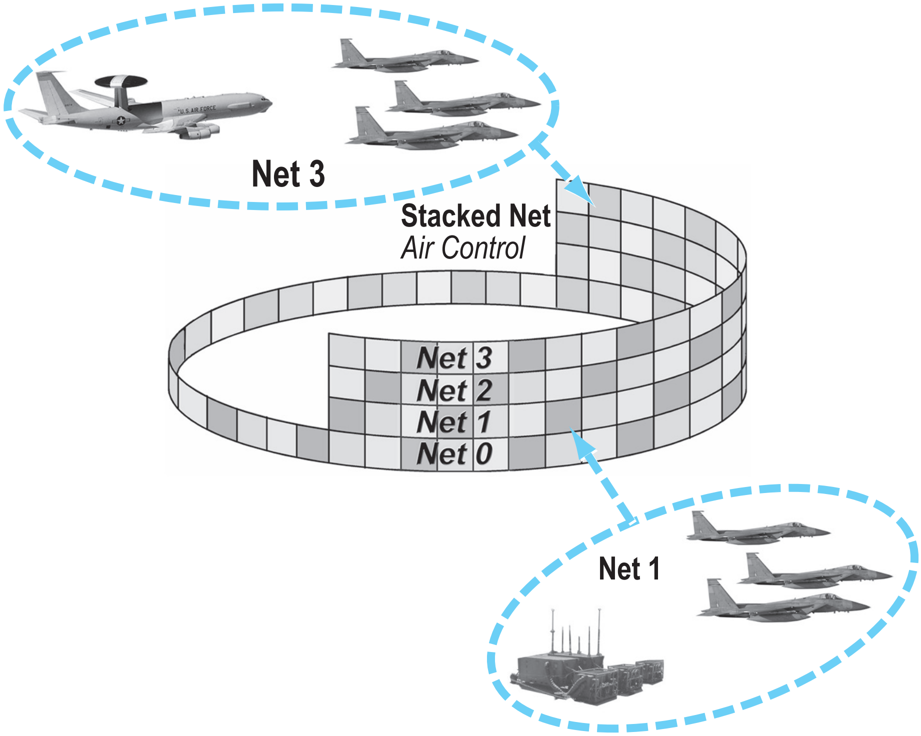


Figure 2-8. Simultaneous multiple nets are useful for separating out information that participants on the main net do not need to receive.

Section E

Summary of Additional Capabilities

The Link 16 J-series messages allow the reporting of two to three times as much exchangeable tactical information as the Link 11 and Link 11B M-series messages. Some of the field sizes have been increased to allow an improved degree of precision in the reporting of data. Some new functions are defined. Areas in which major improvements or changes have been made include:

- Unit Addresses
- Track Numbers
- Track Quality
- Track Identification
- Friendly Status
- Increased Granularity of Measurement
- Lines and Areas
- Geodetic Positioning
- Relative Navigation
- Electronic Warfare
- Land Points and Tracks

A Link 16 address may be 5 characters long.

Part 2 Terminals and Interfaces

The interface between a Link 16 terminal and its tactical host or mission computer is defined by input and output messages, which vary depending on the terminal in use. This chapter describes the Link 16 terminals currently developed—JTIDS and MIDS—and in use by tactical data systems participating in Link 16 worldwide. The flow of data between the terminals and the tactical host and the flow of data within the terminals are explained.

Section A

Link 16 Data Terminals

The JTIDS and the MIDS LVTs are part of a Joint, international, and interoperable family of Link 16 terminals. Although the JTIDS terminals are nearing the end of production, they are still being sustained and are currently fielded with a variety of US and allied platforms. The second generation of Link 16 terminals, the MIDS, is a multinational, multiservice cooperative program sponsored by five countries. These terminals are reduced in size and cost from the original JTIDS terminals and are interoperable with the secure JTIDS waveform. Development of the MIDS JTRS terminal will represent the next generation of Link 16-capable radios.

Section B

Voice Transmission and Reception

Most Link 16 terminals support two secure voice channels, or ports. JTIDS Class 2 terminals (except the Class 2M) support 2.4 kbps encoded and unencoded voice, and 16 kbps unencoded voice, for both ports. In general, the MIDS terminals (except for the LVT 2, LVT 3, and LVT-6) also support Link 16 voice communications.

Both Link 16 secure voice channels are push-to-talk (PTT).

Voice audio is Reed-Solomon encoded (for 2.4-kbps voice) and digitized. However, the JTIDS Class 2 terminals employed in the Control and Reporting Center (CRC) platforms use external voice encoders (vocoders) on both ports, rather than the voice encoding function in the Interface Unit (IU) of the terminal. Control of each voice channel is provided by a PTT protocol. Note that even though the digitized voice is not encoded for error correction, it is still encrypted, and is therefore secure.

When the operator presses the PTT button, two voice buffers are alternately filled with digitized voice data.

During voice reception, digitized data is converted back to audio.

In the JTIDS Class 2 terminals, digitized voice data is transferred between the Subscriber Interface Computer Program (SICP) and the two digital voice ports through several buffers located in Global Memory. The SICP supplies two transmit buffers and two receive buffers for each voice port. The voice buffers hold a maximum of 450 bits, as required for non-error-corrected digitized data. Upon a PTT command, the voice port obtains the transmit buffer address from Global Memory and starts loading the buffer with digitized voice. When the buffer is full, it sets a flag to notify the SICP and, if the PTT signal is still present, begins loading the second transmit buffer. The SICP unloads the data and transfers it in a data transfer block to the Network Interface Computer Program (NICP) for transmission. After the second buffer is full, the voice port signals the SICP and switches back to the first. Alternately switching back and forth between the two buffers continues until the PTT is removed. When the PTT is removed, the voice port switches to reception processing.

Unencoded JTIDS secure voice degrades more quickly than encoded JTIDS data.

When the SICP receives a voice message from the NICP, it stores the received digital data in the first voice receive buffer and sets a flag for the voice port. The voice port retrieves the digitized data as it becomes available. The SICP alternates between the first and second buffers until there is no more data, or until the PTT is issued locally.

Practical experience indicates that JTIDS voice remains understandable with up to a 10 percent bit error rate in the reception, compared to a 50 percent bit error rate for encoded data. Therefore, JTIDS voice will degrade and become unusable before JTIDS data.

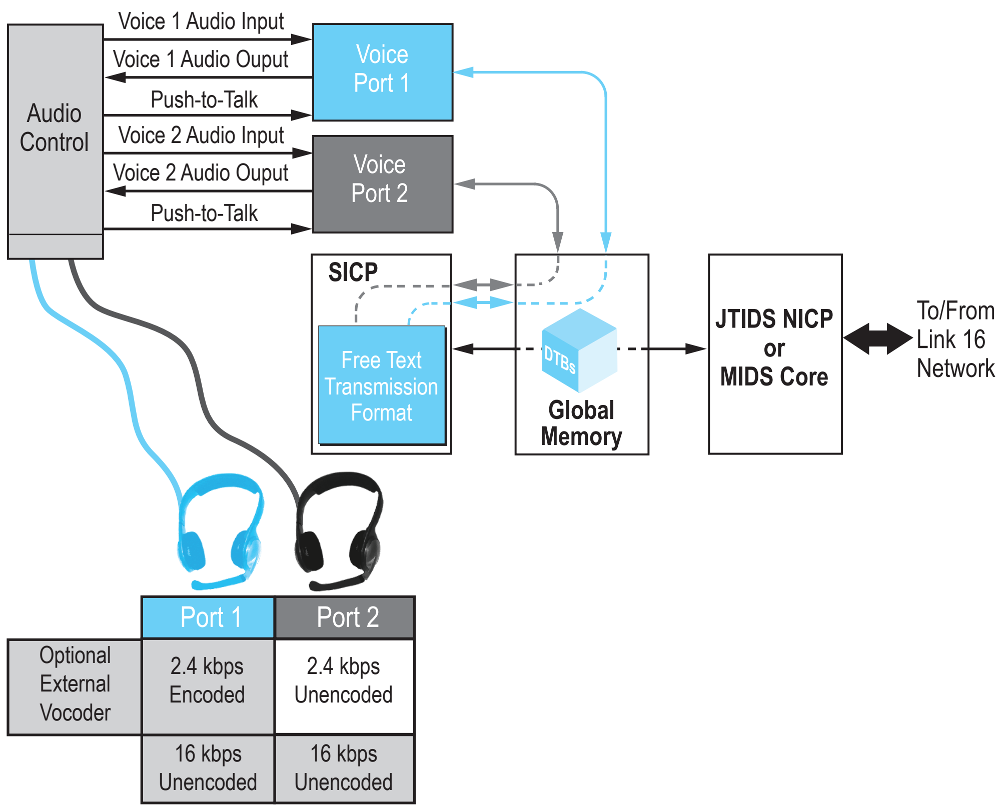


Figure 2-9. Voice audio is digitized and is passed through Global Memory to the SICP for output to the network as Free Text messages. Voice messages received on the network by the NICP are passed to the SICP. The SICP transfers the digitized voice through Global Memory to the voice port, where it is converted back to audio.

Section C

The JTIDS Tactical Air Navigation (TACAN) Port Interface

Used by the airborne platforms, TACAN is one of the functions supported by most JTIDS/MIDS terminals. The TACAN port of the terminal provides the interface between the host avionics systems and the terminal receive/transmit (R/T) and Digital Data Processor (DDP).

JTIDS TACAN operates even in Data Silent mode.

On these platforms, the TACAN function of the R/T normally employs a 500-kHz serial channel clock. Synchronized to this clock are serial input and output channels. R/T mode and channel tuning information, as well as zero-distance calibration information, are provided on the input channel. Bearing, range, and range rate are provided on the output channel. There is also an audio Morse code output signal providing the TACAN station identification. Some tactical aircraft have replaced their TACAN systems with the MIDS LVT-6 TACAN capability.

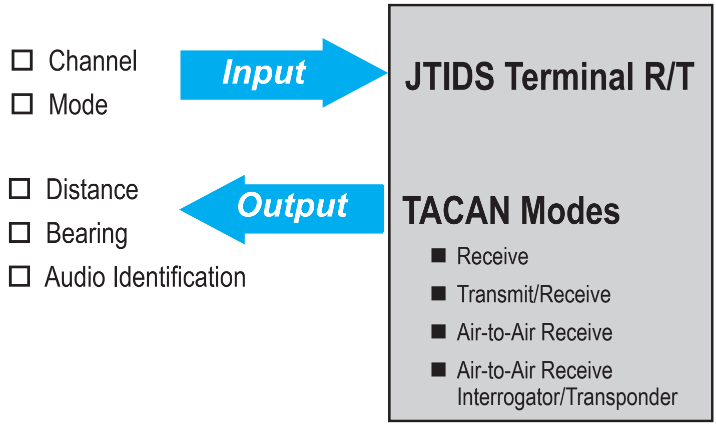


Figure 2-10. The R/T component of the JTIDS terminal provides an independent TACAN function.

Information received from the R/T by the TACAN port is written into Global Memory for the host avionics systems. This information can include range, bearing mode and channel, status, an odometer (distance) reading, range rate, bearing rate, and a built-in test (BIT) summary. Control of the TACAN function from the SICP consists of the TACAN mode and channel, as well as Distance Measuring Equipment (DME) calibration data. The DME calibration data includes delays for antennas A and B and identifies the information the operator desires. TACAN continues to operate when the terminal is set to Data Silent.

Part 3 Time Division Multiple Access Architecture

This section describes the Link 16 communications architecture known as Time Division Multiple Access, or TDMA. The Link 16 TDMA architecture includes time slots, sets, and recurrence rate numbers, or RRNs. It also describes the general data structures supported by the network architecture (Fixed Word Format data, Free Text data, header data, Reed-Solomon encoding, and Round-Trip Timing messages, or RTTs), and the modulation techniques employed for encoding this data onto a carrier for transmission during the time slots (cyclic code-shift keying (CCSK), continuous phase shift modulation (CPSM), pulses, and frequency hopping).

Section A

TDMA and the Link 16 Network

The Link 16 network employs a communications architecture known as Time Division Multiple Access, or TDMA. This architecture uses time interlacing to provide multiple and apparently simultaneous communications circuits. Each circuit, and each participant on the circuit, is assigned specific time periods during which to transmit and in which to receive. This TDMA architecture forms the framework of Link 16 communications.

☐ Epochs, Slots, and Sets

Every 24-hour day is divided by the JTIDS/MIDS terminal into 112.5 **epochs**. An epoch is 12.8 minutes in duration. An epoch is further divided into 98,304 **time slots**, each of which is 7.8125 ms in duration.

The time slot is the basic unit of access to the Link 16 network.

The time slot is the basic unit of access to the Link 16 network. These basic units, the time slots, are assigned to each participating **JTIDS Unit** (JU) for particular functions. A JU is assigned either to transmit or to receive during each time slot.

A JU is either transmitting or receiving in each time slot..

The time slots of an epoch, in turn, are grouped into three **sets**, named **set A**, **set B**, and **set C**. Each contains 32,768 time slots numbered from zero to 32,767. This number is called the **slot index**. (Three sets x 32,768 time slots = 98,304, the total number of time slots in an epoch.) The time slots belonging to set A, for example, are identified as A-0 through A-32767. By convention, the time slots of an epoch are named in an alternating pattern. The time slots of each set are interlaced, or **interleaved**, with those of the other sets in the following repetitive sequence:

A-0, B-0, C-0,
A-1, B-1, C-1,
A-2, B-2, C-2,
•
•
•
A-32767, B-32767, C-32767

This sequence, ending with slot C-32767, is repeated for each epoch.

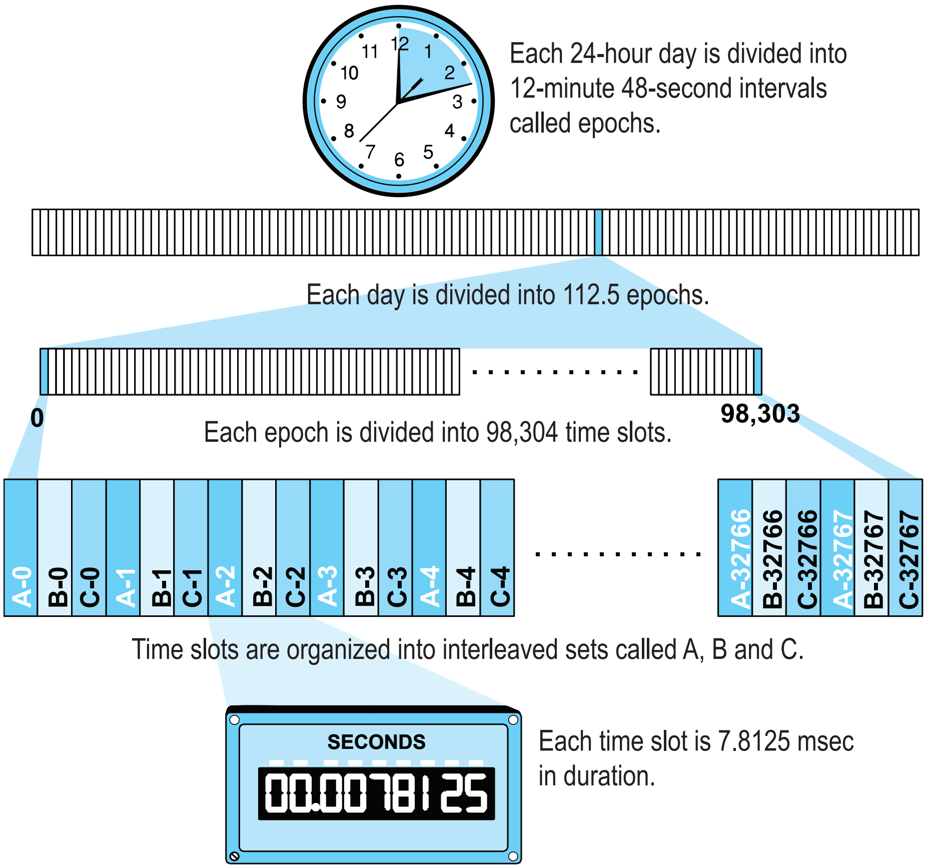


Figure 2-11. The Link 16 TDMA architecture divides a 24-hour day into epochs, sets, and time slots.

Frames

The 12.8-minute epoch is too unwieldy a time interval for describing the rapid communications required by Link 16, so a smaller, more manageable, time interval is defined. This basic recurring unit of time in the Link 16 network is called a **frame**. There are 64 frames per epoch. Each frame is 12 seconds in duration and is composed of 1,536 time slots: 512 belonging to set A, 512 belonging to set B, and 512 belonging to set C. The time slots of a frame are numbered from 0 to 511 and are interleaved in a repetitive cycle such that A-0, B-0, C-0 are followed by A-1, B-1, C-1 and are preceded by A-511, B-511, C-511. Frames occur repeatedly, with one following another, for as long as the link is operational. For this reason, a frame is often illustrated by a ring in which slot A-0 follows slot C-511.

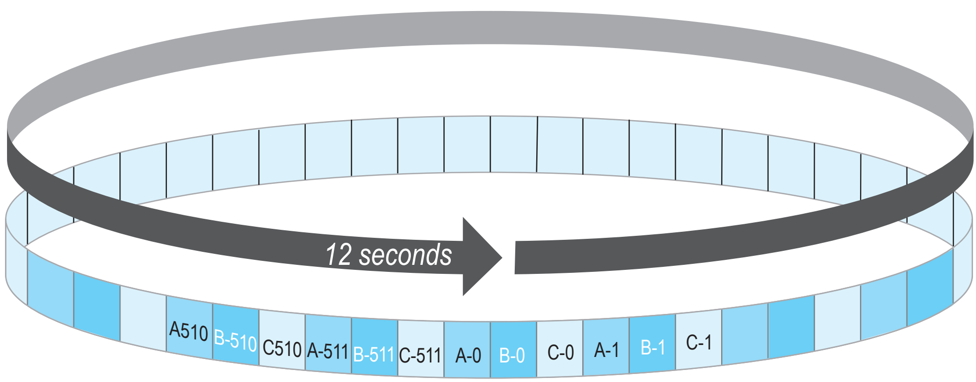


Figure 2-12. A frame consists of 1,536 time slots grouped into interleaved sets A, B, and C, with each set containing 512 time slots numbered from 0 to 511.

RRN	Number of Slots per Epoch	Slot Interval		
		Slots	Time	
15	32768	3	23.4375	Milliseconds
14	16384	6	46.8750	
13	8192	12	93.7500	
12	4096	24	187.5000	
11	2048	48	375.0000	
10	1024	96	750.0000	
9	512	192	1.50	Seconds
8	256	384	3.00	
7	128	768	6.00	
6	64	1536	12.00	
5	32	3072	24.00	
4	16	6144	48.00	
3	8	12288	1.6	Minutes
2	4	24576	3.2	
1	2	49152	6.4	
0	1	98304	12.8	

Figure 2-13. The Recurrence Rate Numbers (RRNs) relative to the frame are shown. Since one epoch consists of 64 frames, the number of slots per frame is found by dividing the number of slots per epoch by 64. An RRN of 15 represents every slot in a set: 32,768 in the epoch, 512 in the frame. Because the three sets are interleaved, the interval between slots in any one set is actually 3, not 1.

Time Slot Blocks

Time slots are assigned to each terminal in the network as blocks of slots. This block of slots, known as the time slot block (TSB), is defined by three variables: a set (A, B, or C), a starting number or index (0 to 32,767), and the recurrence rate. Up to 64 TSBs may be assigned. RRNs of 6, 7, and 8, which correspond to reporting intervals of 12 seconds, 6 seconds, and 3 seconds, are used most often in TSB assignments.

A terminal's time slot usage is specified by up to 64 TSB assignments.

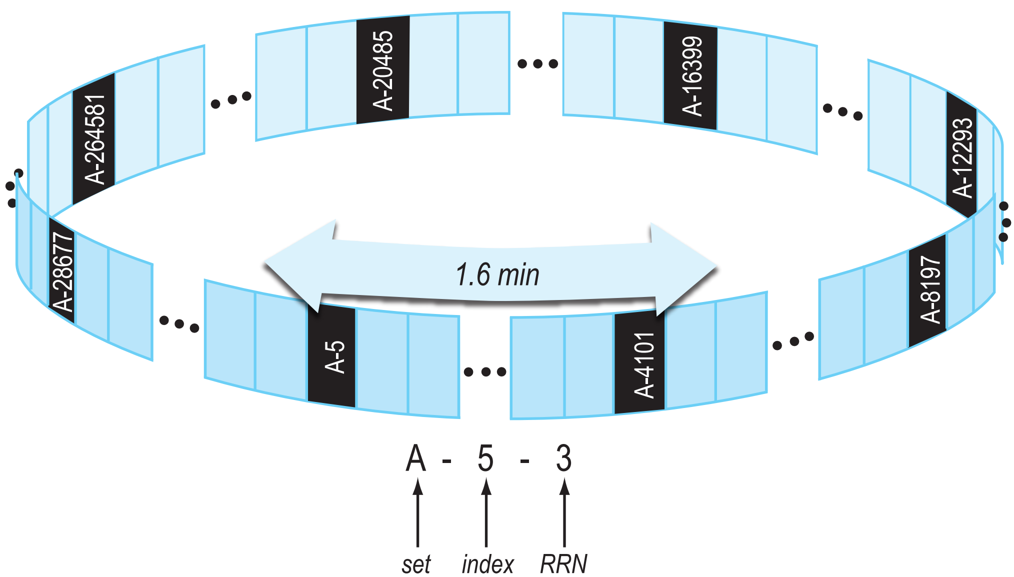


Figure 2-14. Time slots are assigned in blocks by specifying a set, index, and RRN.

Multiple Simultaneous Nets

Multiple nets can be constructed by "stacking" several single nets, as illustrated in *Figure 2-15*. The time slots of these nets are synchronized so that a time slot of one net coincides exactly with the corresponding time slot of every other net. Thus, the multinet architecture contains 98,304 time "slices" per epoch.

Link 16 supports multiple, simultaneous nets.

This multinet architecture allows several groups of participants to exchange messages independent of the other groups, during the same time slot. The 7-bit net number allows a network of up to 128 nets to be constructed. One of these numbers, **net number 127**, is reserved to indicate a stacked net configuration. The remaining nets are numbered from 0 to 126. In a stacked net configuration, the operator selects which net to use during operations. Each net is assigned a unique frequency-hopping pattern for its transmissions. Although it is theoretically possible to define a network containing 127 nets, statistical studies have shown that operating about 20 – 30 nets simultaneously in the same geographical area can cause some degradation in communications.

Each net has a unique pattern of frequency hops.

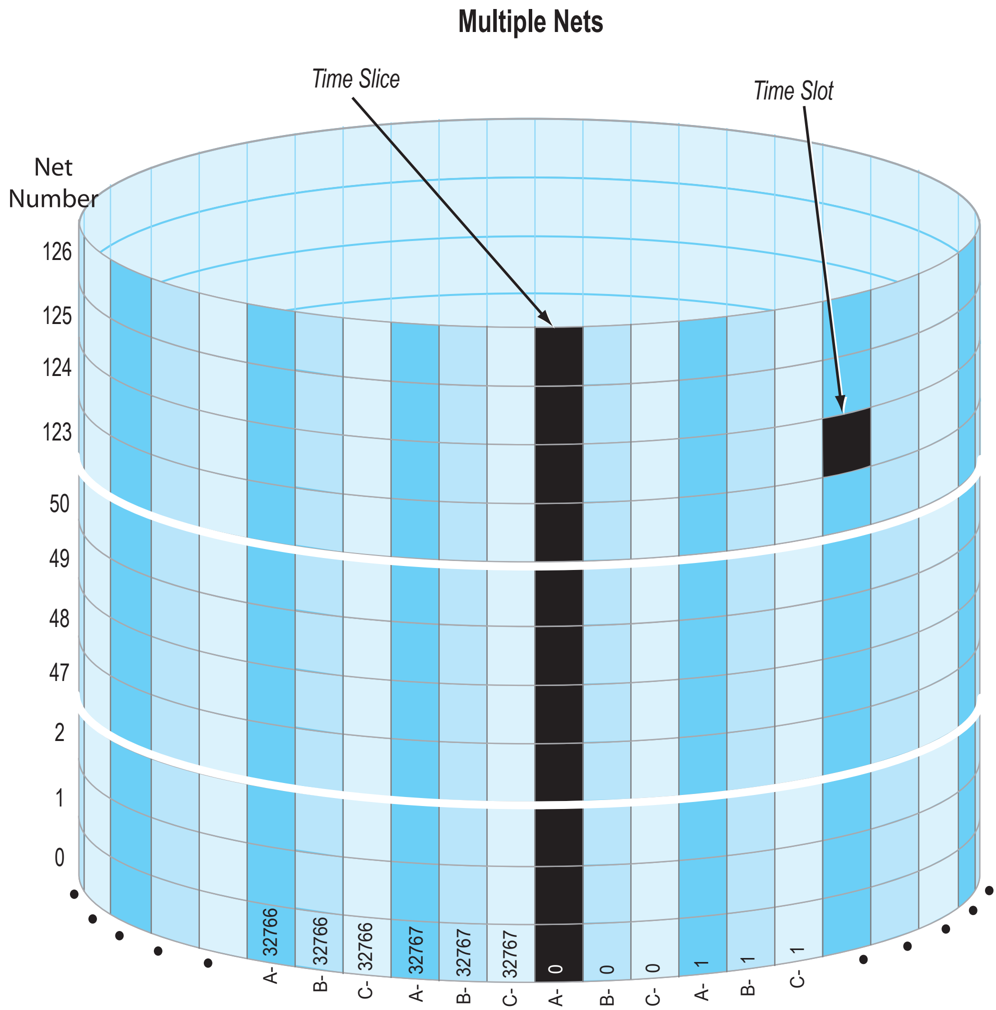


Figure 2-15. The Link 16 multinet architecture stacks 127 of these single net structures with their time slot boundaries aligned. This multinet architecture can be conceptualized by imagining a cylinder of 98,304 time slices.

Synchronization

Networks are currently being operated using a relative time base. With a relative time base, one terminal is designated to be **Network Time Reference** (NTR), and terminals synchronize their time with that of the NTR.[4] The time maintained by this designated terminal defines the **system time** of the Link 16 network. As the reference, this time defines the beginning and end of time slots and ensures the alignment of time slices in the multiple nets. Periodically, the NTR transmits a net entry message to assist other terminals in synchronizing with the network and thereby acquiring system time.

The JTIDS/MIDS terminal automatically synchronizes to the system time of the NTR.

Synchronization, an automatic function of the JTIDS/MIDS terminal, is achieved in two steps. **Coarse synchronization**, the first step, is achieved when a net entry message is successfully received. **Fine synchronization**, the second step, occurs when the terminal has successfully exchanged several RTT messages with the NTR to refine its clock error sufficiently so that it will not adversely affect the network when it begins to transmit data.[5]

Synchronization occurs in two steps: coarse and fine.

4 *Networks can also be operated with an absolute time base, using GPS Coordinated Universal Time (UTC) time as an external time reference (ETR). When an ETR is used, the nature of NTRs changes significantly.*

5 *The technique for synchronizing without RTT transmission, called passive synchronization, is described in Chapter 2, Part 5, Section D. Platforms that do this are designated Secondary Users; refer to Chapter 2, Part 5, Section E for details.*

Thereafter, each terminal maintains a measure of how accurately it knows system time, called its **Time Quality** (Q_t). The NTR has a Q_t of 15, the highest possible value. A terminal continuously refines its knowledge of system time by periodically transmitting RTT messages and by measuring the time of arrival (TOA) of all received messages.

The NTR's Qt is always 15 by definition.

☐ Components of the Time Slot

Recall that the basic unit of access to the Link 16 network is the time slot. Each time slot is 7.8125 ms in duration. Within every 12-second frame, 512 time slots are distributed uniformly among sets A, B, and C, totaling 1,536 time slots per frame. A platform is assigned to either transmit or receive in each time slot. Each time slot is, therefore, a transmission opportunity. Several components comprise a time slot. From beginning to end, these components are:

- Jitter
- Synchronization
- Time refinement
- Message header and data
- Propagation

Data is transmitted within the time slot as a series of information-carrying pulse symbol packets. A **pulse symbol packet** is a 13-microsecond (µs) period during which the carrier is modulated for 6.4 µs. This is followed by 6.6 µs of dead time.

There are 128 time slots per second.

Quick TDMA Summary

In summary, the Link 16 TDMA architecture divides network time into epochs, frames, and time slots. The time slot is the basic unit of access to the network. With a duration of 7.8125 ms each, there are 128 time slots in every second. A JU is assigned either to transmit or to receive in each time slot. Pulses encoded with information are transmitted during the time slot. Transmissions from multiple units during the same time slot are permitted.

TDMA Period	Equivalence
1 Day	= 24 hours
	= 112.5 Epochs
1 Epoch	= 12.8 minutes
	= 64 Frames
	= 98,304 Time Slots
	= 32,767 Time Slots/Set
1 Frame	= 12 seconds
	= 1,536 Time Slots
	= 512 Time Slots/Set
128 Time Slots	= 1 second
1 Time Slot	= 7.8125 milliseconds

Figure 2-16. The Link 16 network employs a communications architecture known as Time Division Multiple Access. Network time is divided into epochs, frames, and time slots.

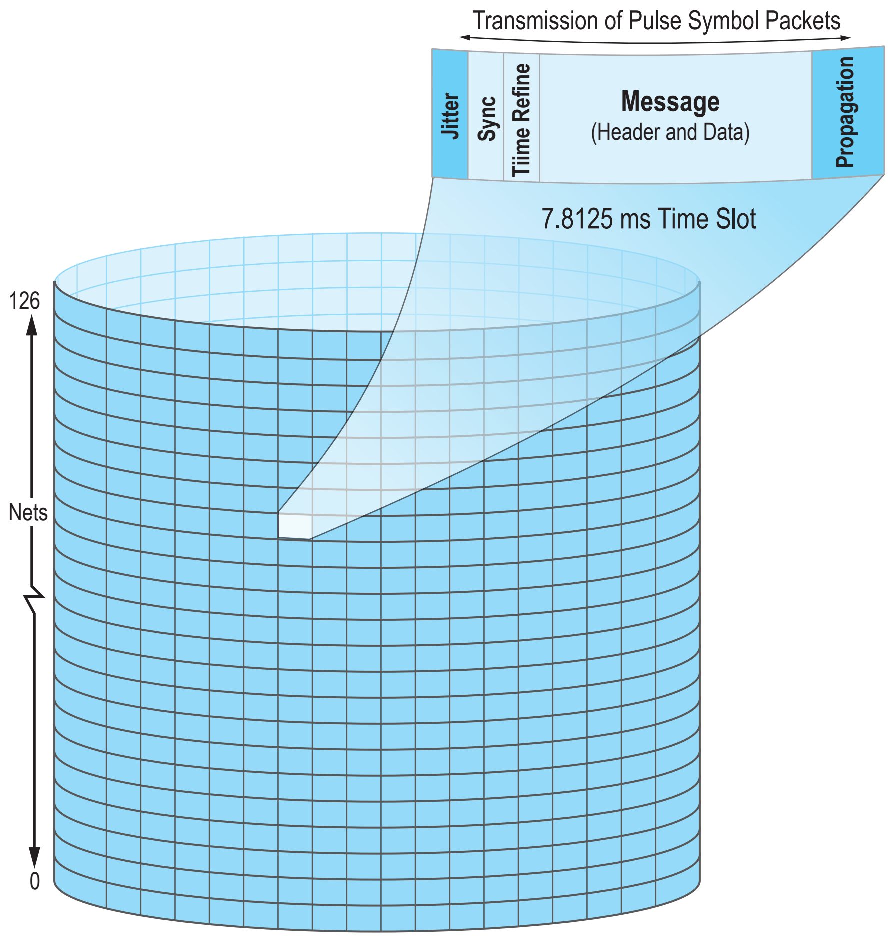


Figure 2-17. The Link 16 fixed word format messages may contain an initial word, one or more extension words, and one or more continuation words.

Section B

Link 16 Terminal Message Types

Link 16 messages are exchanged during the TDMA time slots of the Link 16 network. Each message consists of a **message header** and **message data words**. The message header, which is not considered part of the message structure, is identically formed for IJMS, JTIDS, and MIDS. The message header specifies the type of data being transmitted and identifies the source track number of the transmitting terminal.

Four types of terminal transmission types are defined:

- Fixed Word Format (FWF)
- Variable Message Format (VMF)
- Free Text (FT)
- Round-Trip Timing (RTT)

FWF messages are used to exchange the J-series messages. VMF messages provide a general way to exchange any type of user-defined messages. FT messages are used for digitized voice. RTT messages are used for synchronization with the network.

The data contained in these transmissions is always transmitted as fixed-length, three-word blocks of 225 bits each. These three-word blocks may be packed into a time slot at different densities: Standard (one three-word block), Packed-2 (two three-word blocks), and Packed-4 (four three-word blocks).

Fixed Word Format Messages

The FWF messages consist of one or more data words. Each word consists of 75 bits, of which 70 are data, four are used for parity checks, and one is reserved as a spare. Three types of data words are defined: the **initial word**, the **extension word**, and the **continuation word**. Every J-series message begins with an initial word. Depending on the intent of the message, one or more extension words may be required. Extension words must be sent in order (for example, I, E0, E1; not I, E1.) In addition, one or more continuation words may be required. Continuation words are labeled, and they may be sent out of order (for example, I, E0, C2). FWF messages may consist of an initial word, one or more extension words, and one or more continuation words. If there are an insufficient number of 75-bit words to fill a transmit block, the terminal "pads" the block with **No Statement** (NS) words. Message metering in the host computer helps to minimize the number of NS words inserted by the terminal.

The FWF messages are used to exchange tactical and command information over Link 16. These are the messages commonly referred to as the J-series messages. The United States (US) Services reference the MIL-STD-6016 series message standards documents for the Link 16 J-series message and data item definitions.

> ***The fixed word format messages are the J-series messages!***

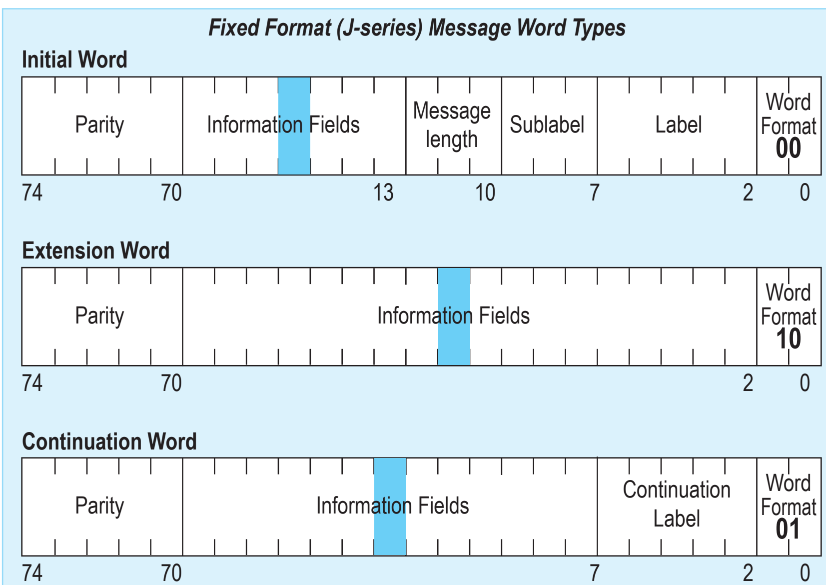


Figure 2-18. The Link 16 fixed-format messages may contain an initial word, one or more extension words, and one or more continuation words. Up to eight words may be used to create a single J-series message.

Variable Message Format Messages

Like FWF messages, VMF messages consist of 75-bit words. Link 16 VMF is not to be confused with the K-series messages defined in MIL-STD-6017. However, VMF messages may vary both in content and length, and fields within the message can cross word boundaries. Information within the message itself identifies the fields and their length.

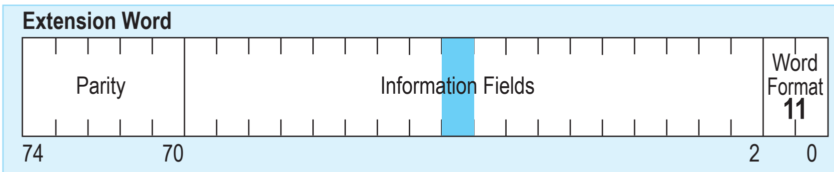


Figure 2-19. VMF messages vary in content and length.

Free Text Messages

FT messages are independent of any message standard. They are unformatted and utilize all 75 bits in the data word—all 225 data bits in the 3-word block.

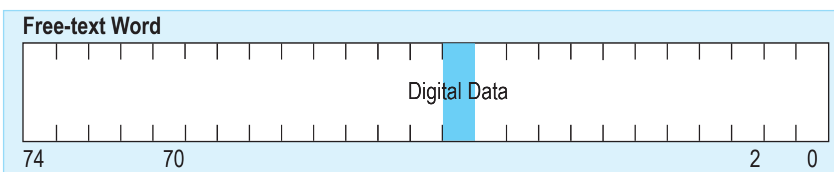


Figure 2-20. FT messages are independent of any message standard. All bits in the word are used for data.

No parity processing is associated with FT messages. They may or may not be Reed-Solomon encoded for error correction. When Reed-Solomon encoding is used, the 225 bits of data are mapped onto 465 bits for transmission. When Reed-Solomon encoding is not used, all 465 bits are available for generic, FT data, although only 450 of these bits are used for unencoded voice. This allows a single assignment of slots to be compatible with standard line rates (2400 bits per second (bps), 4800 bps, etc.). The FT format is used for transmitting Link 16 voice.

Message Packing

Message words may be taken in groups of three words, six words, or twelve words to form transmissions. If there are an insufficient number of words to complete a group, the terminal fills in with a “No Statement” word. The processing of a group of three words is called **Standard** (STD) format. The processing of a group of six words is called **Packed-2** (P2) format. The processing of twelve words is called **Packed-4** (P4) format.

Round-Trip Timing Messages

Recall that the network consists of time slices whose alignment is established by one Link 16 unit, the NTR. To receive and transmit on a Link 16 network, a terminal must be synchronized with the network.

The acquisition and maintenance of system time is called **synchronization**. Special sets of messages are defined to support this function. These are the RTT messages. They represent the only exception to the rule that a terminal can transmit or receive, but not both, in a given time slot. With the RTT messages, a terminal can transmit an interrogation and receive a reply within a single time slot.

RTTs enable the terminal to refine its system time.

The initial exchanges of RTT messages enable the terminal to synchronize with the network. Subsequent exchanges allow the terminal to refine its measurement of system time—that is, its Q_t. Each terminal reports its own Q_t over the network. It also maintains an internal table of the terminals that are within its LOS and which have the highest values of this parameter. Entries in this internal table help the terminal choose which participant to interrogate for its next RTT message.

RTTs are exchanged within a single time slot.

Section C

Inside the Time Slot

In order to communicate digital information over a radio, the RF carrier must be modulated with the digital data. The method used to encode digital data onto the JTIDS/MIDS carrier signal has two parts: Cyclic Code Shift Keying (CCSK) and Continuous Phase Shift Modulation (CPSM).

☐ Pulses: Single and Double

The **single-pulse symbol packet** consists of one 6.4-µs pulse of modulated carrier followed by a 6.6-µs dead time, for a total pulse symbol packet duration of 13 microseconds.

Each pulse of the double pulse symbol packet conveys the same information.

The **double-pulse symbol packet** consists of two single pulses, both modulated with the same transmission symbol. The double pulse has a duration of 26 microseconds. Although the two pulses contain identical information, the carrier frequencies for each are chosen independently.

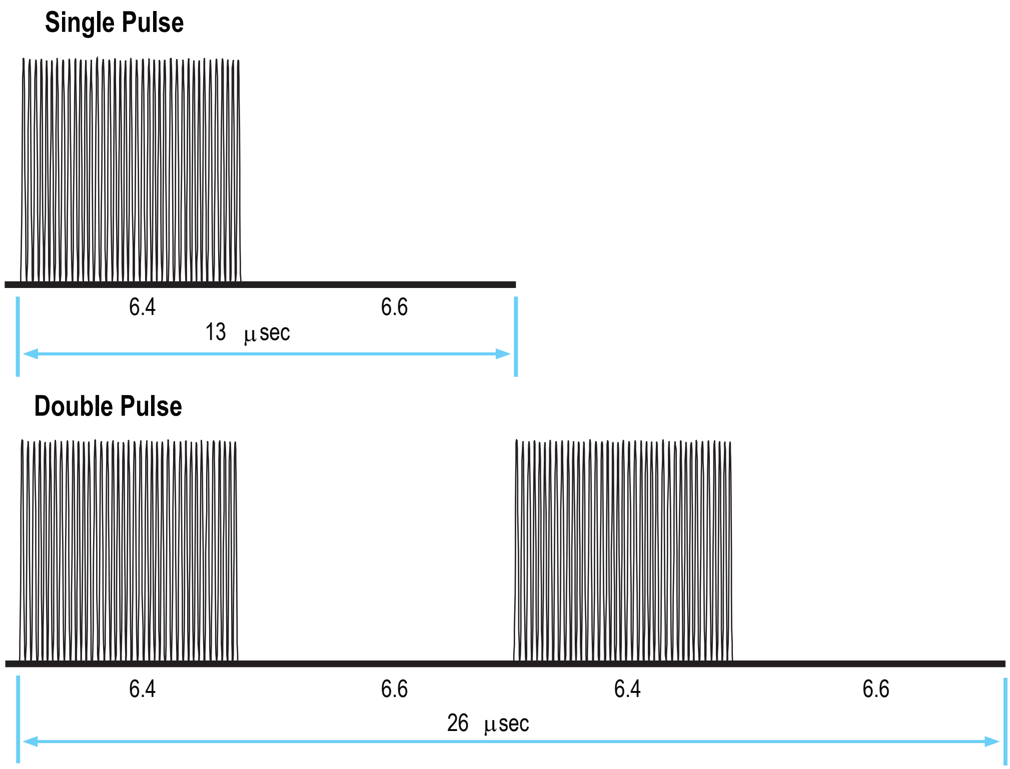


Figure 2-21. Either the single- or the double-pulse structure is used to transmit Link 16 data. The double-pulse structure provides redundancy and increases the antijam capability of the link.

The JTIDS/MIDS terminal uses 51 different carrier frequencies, hopping from one to another for every 6.4-µs pulse. This frequency-hopping technique makes the data very difficult to locate at any given instant, giving it a **low probability of intercept** (LPI) during any given pulse in the time slot. It also contributes to the reliability of the link. Data that is transmitted as double pulses is not only output twice, but on two different frequencies! This makes the signal doubly difficult to jam, and far less likely to be subject to multipath interference.

Part 4 Link 16 Spectrum Operations

The use of Link 16 is governed by frequency restrictions within the boundaries of participating nations. In addition, the use of aeronautical navigational equipment, both ground-based and airborne, places limitations on where and when Link 16 terminals are permitted to radiate. This section provides information on the Link 16 operating limitations and the procedures for the use of Link 16 terminals worldwide.

Section A

Link 16 Frequencies

Link 16 terminals operate within the frequency band 960 to 1215 Megahertz (MHz), which is designated worldwide for aeronautical radio-navigation purposes. Peacetime use of Link 16 in this band is strictly regulated to ensure compatibility with aeronautical radio-navigation systems operating in this band.

Use of Link 16 in the United States and Possessions

In the United States and its Possessions (US&P), the Link 16 frequency band is controlled by the National Telecommunications and Information Administration (NTIA) and administered by the Federal Aviation Administration (FAA). All Department of Defense-supported users of this frequency band are required to comply with the Chairman Joint Chiefs of Staff Instruction (CJCSI) 6232.01 for geographic area pulse deconfliction. This document contains the operational restrictions and limitations stated in the Link 16 spectrum certification,[6] as well as coordination procedures summarized in this chapter.

International Use of Link 16

Link 16 operations occur throughout the world, with an increasing number of countries allowing operations within their borders. Each country establishes Link 16 operating restrictions based on testing between their navigational aids (NAVAIDs) and Link 16. As a result, national Frequency Clearance Agreements (FCAs) differ from the US&P certification. Regardless of the restrictions placed on JTIDS/MIDS operations by a foreign government, visiting US forces must comply with the national frequency clearance and procedures established for that country's FCA.

The Aeronautical Radio-Navigation Band

The JTIDS/MIDS terminals operate in the portion of the frequency spectrum between 960 and 1215 MHz, which is called the Aeronautical Radionavigation Band. The primary users within this band are civilian and military air navigation systems, including civil Distance Measuring Equipment (DME) and military TACAN equipment. DME and TACAN channels occur **every 1 MHz** within this band.

---

6 The restrictions are described in the Interdepartment Radio Advisory Committee (IRAC) Document 33583 (2004), which supersedes the previous 21167 (1979), 27439 (1991), and 28843 (1994) IRAC documents.

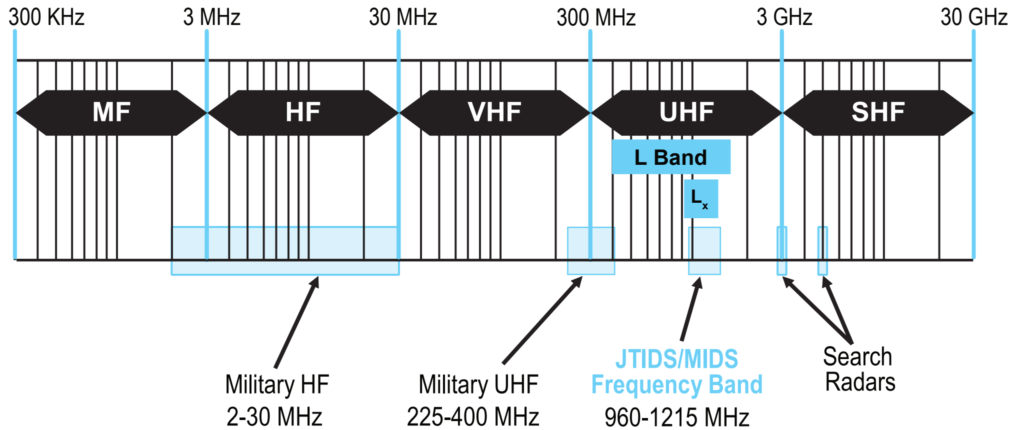


Figure 2-22. The portion of the spectrum used for Link 16 communications is in the ultra high frequency (UHF) band. UHF communications are line of sight. The portion of the frequency spectrum between 950 MHz and 1150 MHz is called the Lx band. The JTIDS/MIDS terminal operates partially, although not entirely, within this band—that is, the Lx band and the JTIDS/MIDS band do not completely overlap, as shown here.

Link 16 Frequencies

The 51 frequencies assigned to Link 16 for TDMA transmissions are those between 969 MHz and 1206 MHz, spaced 3 MHz apart. Two notches, which are centered on 1030 MHz and 1090 MHz, are excluded, because these frequencies are used by IFF and Traffic Collision Avoidance System (TCAS) equipment. The fact that Link 16 and TACAN pulse emissions tend to be uncorrelated in time tends to protect TACAN operation.

Link 16 operates in the 960 – 1215 MHz band, with JTIDS/MIDS frequencies occurring every 3 MHz between 969 and 1206 MHz.

JTIDS/MIDS Communication Modes

Three operator settings control the communication mode used by the JTIDS/MIDS terminal. Mode 1 is the normal operational mode. Modes 2 and 4 represent a reduction in capacity and capability. Mode 3 is an invalid mode; it is not implemented in the JTIDS Class 2 terminal, and it is not recognized by the NATO Standardization Agreement (STANAG) on MIDS:

- **Mode 1**: This is the normal JTIDS/MIDS mode of operation. It includes frequency-hopping with full MSEC and TSEC processing. Mode 1 operation is required by the current spectrum certification.
- **Mode 2**: No frequency-hopping. All pulses are transmitted on a single frequency. Peacetime constraints on slot usage are eliminated. Requires a frequency assignment waiver prior to use.
- **Mode 4**: No frequency-hopping. Some communications security processing is eliminated to allow the terminal to function as a fairly conventional data link. Requires a frequency assignment waiver prior to use.

Mode 1, the normal operational mode required by the current spectrum certification, allows full MSEC and TSEC processing and multinetting.

Section B

Interference Protection Features

Introduction

JTIDS and MIDS terminals must operate on Link 16 in the presence of interfering signals from the IFF interrogator, the ATCRBS IFF Mark XII System (AIMS) transponder, TACAN interrogators, and its own built-in TACAN function, as well as interfering signals from TACAN interrogators aboard adjacent platforms. An airborne TACAN interference environment might consist of as many as 60 interrogators in search mode and 540 interrogators in track mode. These interfering signals are distributed uniformly in frequency over the entire TACAN band. A ground beacon environment typically has a beacon on every ground-to-air channel, each transmitting 3600 pulse-pairs per second.

The Link 16 frequency band is flooded with low-level RF signals. Link 16 transmissions must not interfere with the operation of the systems relying on these signals.

Always consult the JTIDS Spectrum Users Guide for the latest separation requirements!

Terminal Emissions Requirements

To prevent the JTIDS/MIDS terminal's RF transmissions from interfering with the normal operations of other systems, its pulse power spectrum and out of band emission characteristics are strictly specified. The pulse power spectrum is unrestricted within 3 MHz of the center frequency, but it must be 10 decibels (dB) down at ±3 MHz, 25 dB down at ±6 MHz, and 60 dB down ±15 MHz. The out of-band emission characteristics, including broadband noise, sideband splatter, harmonics, and other spurious emissions, must be kept below –65 decibels referenced to one milliwatt (dBm) per kiloHertz (kHz).

Interference Protection Feature

Because Link 16 transmissions could potentially interfere with national air navigation and flight safety, all JTIDS and MIDS terminals are equipped with an **Interference Protection Feature** (IPF) to monitor their terminal transmissions. The IPF function monitors its transmitter output for:

- Out-of-band transmissions
- Transmissions in the IFF notches
- Improper frequency-hopping distribution
- Incorrect pulse lengths
- High R/T thermal level
- High Power Amplifier (HPA) operation
- Time Slot Duty Factor (TSDF)

Any one of these infringements constitutes an **IPF failure**. Normally, if authorized levels are exceeded, the IPF function will automatically disable the terminal's transmissions for up to one frame.

> ***An IPF failure is an FAA violation!***
> ***FAA violations are subject to fines.***

The Link 16 terminal implements two sets of protection features. The first feature imposes **peacetime constraints** on the terminal's operation in Mode 1. (These limitations are automatically overridden in the less capable Modes 2 and 4.) The second feature automatically monitors the terminal transmissions to ensure that it does not interfere with navigation systems.

Section C

Time Slot Duty Factor

TSDF was developed as a way of quantifying Link 16 transmissions as a measure of pulse density. The calculated TSDF values are used as part of the scheduling process to ensure that planned operations do not exceed frequency assignment restriction limits.

TSDF is normally a two-factor number written as a fraction: for example, 100/50. The first number represents the total percentage of potential pulses in a geographic area, and the second number represents the percentage of pulses that can be transmitted by the highest single user. Each TSDF number is based on the percentage of base value, which is represented by 396,288 pulses per 12 seconds. The example of 100/50, above, represents a geographic area where the total number of potential pulses is 396,288 (100 percent of 396,288), and the highest single user is 198,144 pulses (50 percent of 396,288).[7]

TSDF values are percentages.

If a third number is included in the TSDF fraction (for example, 100/50/(300)),[8] it represents the additional TSDF percentage allowed for all the platforms in an area defined within an annulus between a 100 nm circle and a 200 nm circle around each Link 16 terminal, for a total of 400 percent TSDF.

Managing TSDF enables compliance with IRAC restrictions that place various TSDF limitations on JTIDS/MIDS operations. The most obvious are the two geographic areas that establish the maximum number of pulses permitted within a geographic radius around each JTIDS/MIDS terminal (currently 100 and 200 nm). To determine the TSDF within the present 100-nm geographic area, select any terminal and add

7 The value 396,288 represents transmission of STD or P2SP packing in every one of the 1,536 time slots in the frame. STD and P2SP transmissions contain 258 pulses per frame: thus, 258 x 1536 = 396,288.

8 Approved geographic area limit in IRAC 33583.

the unit TSDF to the unit TSDF of all the JTIDS/MIDS terminals within this 100-nm radius. The sum TSDF becomes the first number, and the highest single user within the 100-nm radius becomes the second.

The remainder of this section describes the calculations needed for meeting US&P spectrum certification requirements. National FCAs also require the consideration of TSDF in coordinating Link 16 operations.

☐ Calculating TSDF

TSDF calculations are based on a standardized method included as part of the supporting documentation in Interdepartment Radio Advisory Committee (IRAC) Document 33583.[9] The TSDF values are derived from the assigned transmit time slots and represent all of the opportunities for a platform to transmit.

9 The IRAC document (33583) includes, as an attachment, SPS WG-1 TR 02-002, Description of Contention Transmissions. That document provides the agreed TSDF calculation method.

Part 5 Features and Functions of the Link 16 Network

The previous chapters focus on the physical structure of the Link 16 network. The focus of this chapter is on its logical structure. The logical structure is mission-oriented and is based on platform requirements. Many different logical structures are possible. These are currently designed by the US Armed Services' own **Network Design Facilities (NDFs)**.[10] To allow the operator to effectively utilize the network structure, an understanding of how it is designed and how it works is helpful in recognizing problems and diagnosing their probable cause. Knowledge of the logical structure of the network also enables an operator to distinguish between the limitations that are inherent in the Link 16 waveform and those that are part of the design of a particular network.

Section A

Participation Groups

Superimposed on the physical structure of the Link 16 network is a logical structure that allows it to be adapted to specific operational environments or needs. This adaptation is accomplished by apportioning the network capacity among multiple "virtual circuits" whose transmissions are dedicated to a single function. Participants are then assigned to these circuits, or functional groups, as required by their mission

---

10 *USAF Initialization Design Loads (IDLs) are maintained at the following Website: https://www.my.af.mil/gcss-af/afp40/USAF/ep/globalTab.do?command=org&pageId=681742&channelPageId=-1717014. Select Section A3YJ, then click on the link to the Air Force Link 16 Network Design Facility Knowledge Now Community of Practice (CoP). Individuals can also contact the Air Force Network Design Facility (NDF) at DSN 574-8328 or 574-8329 to request a desired IDL.*

and their capabilities. In addition to friendly force identification and position reporting, functional groups can include:

- Surveillance
- Fighter-to-fighter target sorting
- Air control
- Imagery
- Network Enabled Weapons
- Ballistic Missile Defense (BMD) Operations
- Electronic Warfare (EW) reporting and coordination
- Mission management and weapons coordination
- Two secure voice channels

There are also functional groups that support the operation of the network, including **Initial Entry** and **Round-Trip Timing** (RTT). All of these functional groups are known as network participation groups, or NPGs. The transmissions on each NPG consist of messages that support its particular function.

This functional structuring allows JTIDS Units to participate on only the NPGs necessary for the functions they actually perform. It is likely that all C2 platforms will operate on all applicable NPGs at all times. A maximum of 512 participation groups are possible. Of these, 30 have been allocated for subject-oriented functions, and 22 of these are currently defined. The Air Force employs between 11 and 15 NPGs. NPGs 30 and 31 are specifically dedicated to IJMS messages and are only used in NATO Networks.

The NPGs 32 through 511 are assigned for the Needline participation groups. Because no US Armed Services employ these groups, they are not discussed further in this guidebook. All further references to NPGs will refer to the subject-oriented Network Participation Groups.

NPG	Purpose
2	RTT-A
3	RTT-B
4	Network Management
5	PPLI and Status A
6	PPLI and Status B
7	Surveillance
8	Mission Management & Weapons Coordination
9	Air Control
10	Electronic Warfare
11	Imagery
12	Voice Group A
13	Voice Group B
14	Indirect PPLI
18	Network Enabled Weapons
19	Fighter-to-Fighter Net 1
20	Fighter-to-Fighter Net 2
21	BMD Operations
29	Residual Message
30	IJMS P Messages
31	IJMS T Messages

Figure 2-23. Each J-series message is mapped to a specific NPG.

Each J-series message is mapped to a specific NPG. The JTIDS Class 2 terminal permits the assignment of 64 time slot blocks to as many as 32 participation groups drawn from 512 possible selections. The chosen NPGs have an “external” number, which is the number (between 1 and 511) assigned, and an “internal” number, sequenced from 1 to 32. Each NPG is associated with a particular set of J-series messages. For example, the J3.x set of messages is transmitted on NPG 7.

The NPGs

NPGs support operational communications needs. They allow the network designer to separate the functions implemented in the J-series messages. Network capacity is first allocated to NPGs, and then to the users that participate in that NPG. The following paragraphs briefly describe each NPG that is currently defined. NPGs can be divided into two basic categories: those used for the exchange of tactical data, including voice, and those required for network maintenance and overhead.

Network capacity is assigned first to NPGs, and then to users participating in them.

In general, networks are designed to support particular operational goals. The NPGs described here may or may not be included in a given network, depending on the mission objectives and functional requirements that the network was designed to meet.

Section B

Time Slot Assignments

The amount of network capacity assigned to a given NPG depends on communications priorities and information exchange requirements. Examples are:

- The number and types of participants
- How often these participants need access to each NPG
- The expected volume of data
- The update rate of the information
- Relay requirements

The number of time slots that must be allocated within the NPG to each participant depends on the type of unit and its method of accessing the time slot.

Time Slot Access Modes

Within each NPG, the time slots assigned to each unit are evenly distributed over time and generally occur every three seconds, every six seconds, and so on. These slots are assigned using **time slot blocks,** which specify a set, index, and recurrence rate, as previously described, as well as a net number. Time slot block assignments are numbered from 1 to 64. The terminal is limited, therefore, to a maximum of 64 time slot block assignments.

A terminal may be assigned up to 64 time slot blocks.

While several different access modes for each time slot block have been proposed at one time or another, three are currently in use:

- Dedicated Access
- Contention Access
- Time Slot Reallocation

Section C

Network Roles

Network roles are functions assigned to a JU, either by initialization or by operator entry. A network role can support one or more of the following functions: synchronization, navigation, and data forwarding. Roles are assigned to C2 or nonC2 units and are made on the basis of platform capabilities and expected platform position. With the exception of Network Manager, all roles are terminal functions. They may be changed during operations and include:

- Network Time Reference
- Position Reference
- Initial Entry JU (Net Entry Transmit Enable) Terminal
- Navigation Controller
- Secondary Navigation Controller
- Primary User
- Secondary User
- Forwarding JU
- Network Manager

Network roles are assigned in the OPTASK LINK. A JU should hand off its assigned role(s) to another unit before it inhibits transmissions or goes data silent.

Hand off your assigned network role before going data silent!

Section D

Network Entry

Protocol for entering the Link 16 network is handled by the terminal. One unit is designated to be the system time reference. As we learned from the previous section, this unit is the NTR. It transmits the net entry message on NPG 1, Net 0, using the default TSEC and MSEC cryptovariables in the first time slot (A 0 6) of every frame.

Network Entry is performed by the terminal.

The net entry message for Link 16 is the Initial Entry message, J0.0. The time at which this message is transmitted defines the system time and the start of each Link 16 frame. The body of the net entry message includes the time quality, RTT radio silence status, and the current default net number. It may also contain voice, PPLI, and RTT time slot assignments on the default net for the next epoch. Depending on the transmitting terminal's antijam Communications Mode setting, the terminal may automatically append extension or continuation words to the message.

The Initial Entry message is J0.0.

The process of acquiring system time is called **synchronization**. It can be performed actively or passively. Each method requires several steps. Since the process starts with an estimate of the current time, network entry can be simplified for everyone if the NTR uses Coordinated Universal Time (UTC) from the Global Positioning System (GPS).

You cannot transmit data until you have synchronized with the network.

Simplify network entry by having the NTR use GPS for UTC.

Coarse Synchronization

Initializing the terminal requires several steps. Among them are obtaining a current time hack and making the time uncertainty setting, which tells the terminal how many seconds of uncertainty to use in listening for the NTR's initial entry message to achieve coarse synchronization.

The time and time uncertainty period are operator settings.

After making these settings, the operator's first step is to start network entry. The process of entering a network means acquiring synchronization. The JTIDS/MIDS terminal first uses an estimate of the current time and an estimate of its own clock error (time uncertainty) to choose a time slot from the A 0 6 time slot block that it is certain has not yet occurred. The terminal then begins listening for an Initial Entry message. It starts listening one time-uncertainty period before the expected time slot, and continues to listen through one time-uncertainty period afterward. If the uncertainty estimate is correct, it should receive the message. If the message is not received, the terminal automatically tries again. If the message is received, the time of receipt is used to correct the terminal's system time. This adjusted system time may still include an error due to propagation time.

After the Initial Entry message has been received, the terminal is declared to be in coarse synchronization. When a terminal has achieved coarse synchronization, it knows the system time to within one slot-time, and it can begin to transmit RTT interrogations.

The only transmission made by a terminal in coarse sync is the RTT interrogation.

Fine Synchronization

After achieving coarse synchronization, the terminal transmits an RTT interrogation to the NTR, or to the terminal with the highest time quality in its internal table. The receiver of the RTT-I responds during the same time slot with a reply. This reply contains the time of arrival of the interrogation at the receiving platform. Then, using both the measured time of arrival of the reply and the reported time of arrival of the interrogation, the terminal can further adjust its estimate of system time to remove the error due to propagation time. The terminal is then declared to be in **fine synchronization**. The terminal of a Primary User (PRU) must be in fine synchronization to fully participate in the network.

The terminal must be in fine sync to transmit data on the network.

The error in the clock maintaining system time is estimated continuously by the terminal. Even the temperature of the terminal components, as estimated by the length of time the terminal has been powered up, is considered. If the current clock frequency will keep the terminal's clock error to within 36 microseconds (µs) during the next 15 minutes, fine sync can be confirmed. If the clock error exceeds a threshold setting by as little as 54 µs, the terminal's status is downgraded from **fine sync confirmed** to **fine sync in process**. Terminals in fine sync can maintain time with sufficient accuracy to continue operating for up to three hours.

Active vs. Passive Synchronization

The process of transmitting RTTs to refine the terminal's estimate of system time is known as **active synchronization**. If a terminal is within LOS of the NTR or an Initial Entry JTIDS Unit (IEJU), and if their RTT time slot assignments are the same, it should take only seconds for this unit to become active on the network. Otherwise, the unit will not achieve fine synchronization.

Passive sync must be performed when the terminal is in radio silence.

It is also possible, however, to acquire system time passively—that is, without transmitting on the network. **Passive synchronization** must be used when the Long Term Transmit Inhibit (LTTI) mode is enabled and the terminal is in radio silence. Instead of transmitting RTTs after coarse synchronization has been established, the terminal listens for position messages on the PPLI NPGs. Using the position of the unit reported in the PPLI message and the knowledge of its own position from its navigation system, the terminal can estimate the propagation time required for the message. By comparing the expected time of arrival with the actual time of arrival, the terminal can then adjust its estimate of system time to remove the propagation error. Time-of-arrival measurements are made to the nearest 12.5 nanoseconds.

Section E

Precise Participant Location and Identification

JTIDS terminals employ relative navigation techniques to constantly fix their platform's position. This information is transmitted periodically, along with other identification and status information, in the PPLI message. The PPLI is the "friendly unit reporting message."

It can be used to determine link participants and data forwarding requirements, as well as to initiate air control.

Only friendly units transmit PPLIs.

It also supports passive synchronization. PPLIs are transmitted periodically by all JUs that are active on the network on NPG 5 and/or NPG 6. For most Services, including the US Air Force, Indirect PPLIs generated for Link 11 and Link 11B units by the Forwarding JTIDS Unit (FJU) are transmitted on NPG 7; however, the US Navy transmits them on NPG 14. Note, however, that in the near future the US Navy will also transmit Indirect PPLIs on NPG 7.

☐ PPLIs and Passive Synchronization

The PPLI message is essential to the process of passive synchronization. Using the position of a unit reported in the PPLI and knowledge of its own position, a unit operating passively can estimate the range, and therefore the propagation time, required for the message. Combining this information with the actual arrival time, and taking into consideration the time quality and position quality reported in the PPLI, the terminal in passive sync can make adjustments to its estimate of system time.

Secondary users are in passive synchronization.

Section F

Relays

Link 16 is strictly a UHF LOS communications system. For air-to-air, or ground-to-air, this is approximately 300 nautical miles. Between ground units, this is closer to 25 nautical miles. Because of this, relays are almost always required for large Op Areas. Relays are established during network design, and time slots are allocated specifically for this purpose. As many JUs as possible are preassigned as conditional, unconditional, or suspended relays. Time slots are allocated for the relay function as part of the network design and can be changed only by time slot reassignment.

Relays extend Link 16 connectivity beyond line-of-sight (BLOS).

☐ General Requirements

The JU designated to be a relay must be provided with the capacity to transmit the relayed message. Messages received in one time slot are relayed at a later time in a specified, preallocated slot. The original message and the retransmitted message are referred to as a relay pair. Paired **time slot blocks** (TSBs) are assigned as part of each NPG that requires relay support. The number of time slots required depends on the number of relay hops required to reach the destination.

> ***The network is designed with specific time slots designated as relay pairs, and specific JUs designated to perform the relay function.***

In addition, the relaying unit must be in fine sync and in the same range mode. Reed Solomon error correction is performed by the relaying terminal on messages prior to retransmission. Messages with uncorrectable errors are not retransmitted.

The most basic type of relay technique is called the paired slot relay. The originating terminal transmits a message. The relaying terminal receives it, stores it, and retransmits it. The transmit slot is paired with the receive slot by a fixed offset called the **relay delay**. The **relay delay** must be greater than five and less than 32 time slots. The net number on which the relay transmits does not have to be the same as that on which it received. For example, the JTIDS/MIDS terminal of the relaying unit can be initialized to relay-receive on Net 0 and relay-transmit six time slots later on Net 1. The assignment of a relay pair counts as one TSB assignment. By doubling the time slot requirements, therefore, relays reduce the potential capacity of an NPG by 50 percent.

The use of relays reduces the potential capacity of an NPG by 50 percent.

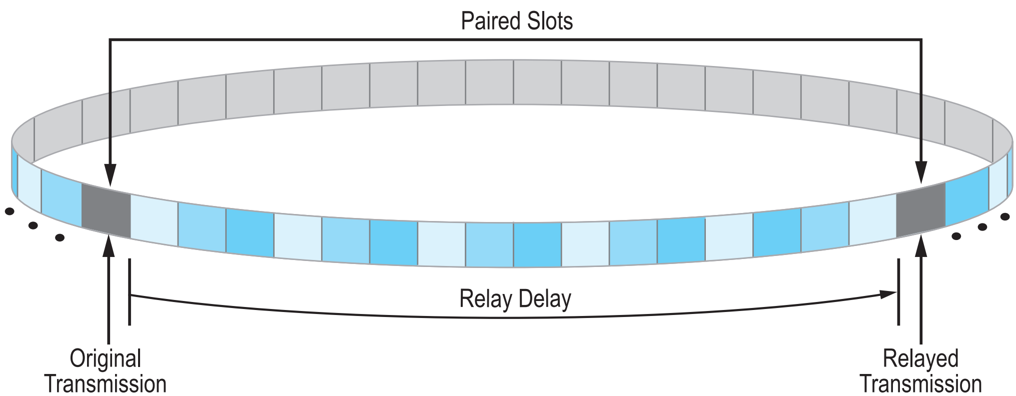


Figure 2-24. In the paired slot relay, the slot of the original message is paired with a slot for the relay retransmission of the message by specifying the original slot and a relay delay.

Relay Types

The type of paired-slot relay is specified in the message itself, and it provides additional information to the terminal about the information to be relayed. The following types are defined:

- Main Conditional/Unconditional
- Voice Conditional/Unconditional
- Control Conditional/Unconditional
- Zoom
- Directed
- Message Directed
- Participation Group

The **main net** is the net on which housekeeping and overhead functions are performed. These include the exchange of RTT and PPLI messages, and the main net is usually, but not always, on Net 0, depending on the network design. Voice and air control nets are usually defined as stacked nets. The **zoom relay** allows selected portions of the main net to be relayed on another net. The zoom net number must be specified with this relay type. The message-directed relay allows a particular message to be directed to a particular NPG. And, finally, messages from an entire NPG can be specified for relay.

All time slots assigned to a particular NPG can be specified for relay.

If the relay is defined to be an **unconditional relay**, the terminal relays messages in accordance with the receive and relay transmit time slot assignments provided at initialization time. The relay will always occur, unless the terminal is not in fine sync or has been set to data or radio silence.

The **conditional relay**, on the other hand, requires the terminal to selectively activate or deactivate the relay function based on which JU can provide the most efficient coverage. The conditional relay becomes active if its geographic coverage is greater than that of the current relay. Geographic coverage is determined from the height and range data provided in the relay unit's PPLI. In general, the unit with the greater altitude is assumed to be in a better relay position. For stacked nets such as the voice and control nets, the net numbers of the originator and the relay must match. For example, an F 15 on voice net 11 can relay only voice net 11, not all voice nets. Several units can be assigned to relay the same NPG in the conditional mode.

The conditional relay depends on geographic coverage.

A unit can be assigned to relay-receive on one net and relay-transmit on a different net. A relay can be **suspended** by placing the terminal in the suspend mode.

Section G

Communications Security

Communications security (COMSEC) entails several layers of encryption. Different pieces of hardware handle these on JTIDS and MIDS terminals.

MSEC and TSEC

Two layers of communications security are provided: **MSEC** and **TSEC**. The MSEC cryptovariable (CV) (pointed to by the MSEC Cryptovariable Logical Label (CVLL)) is used to encrypt the message data prior to the Reed-Solomon encoding, interleaving, and pulse generation.

MSEC encryption occurs before Reed-Solomon encoding.

The TSEC CV (pointed to by the TSEC CVLL) determines the amount of jitter in the time slot and the 32 chip pseudorandom noise variable. The TSEC CV, together with the net number and time slot number, also determines the frequency-hopping pattern of the carrier.

MSEC and TSEC can be either the same or different.

Each NPG is assigned two CVLLs, one to be used for MSEC and one to be used for TSEC. In addition, a default net number, a default MSEC, and a default TSEC are also assigned. When the terminal has nothing to transmit, it defaults to receive using these default parameters.

MSEC is message security; TSEC is transmission security. These are part of the network design load.

Section H

Multinetting

The JTIDS waveform allows for the definition of 127 different nets, numbered 0 to 126. The net number, along with the TSEC CV and time slot number, determines the carrier frequency-hopping pattern. These different hopping patterns are what keep the nets separate and distinct and allow multiple nets to operate concurrently. Multiple nets can be established simply by specifying different net numbers for a particular NPG, without changing the TSEC and MSEC CVs. If the MSEC and TSEC CVs are changed, several variations of multinetting are possible, including blind relays. Transmission in the same time slots, but on different NPGs and different net numbers from the main (default) net, is known as multinetting.

Section I

Range Extension Techniques

The most common method of extending JTIDS range BLOS is the employment of airborne relays. This is not always feasible, however, due to the lack of airborne assets or conflicting mission requirements. Several means of employing satellite communications to extend the range of Link 16 are under development as part of the Joint Range Extension Application Protocol (JREAP) program. Various connectivity devices using Ethernet or serial protocols have been developed as well to support testing and training over landlines.

☐ Satellite Methods

Satellite resources include Military Strategic and Tactical Relay Satellite (MILSTAR), the UHF Follow-On (UFO), the Defense Satellite Communications System (DSCS), and Fleet Satellite (FLTSAT). These satellites provide communications in three frequency bands: UHF, super high frequency (SHF), and extremely high frequency (EHF).

■ S TADIL J

Satellite TADIL J (S TADIL J) is a Navy design for extending the range of Link 16 using satellites. Aboard Navy ships, S TADIL J requires a modification to the tactical system to accommodate new cabling from the Command and Control Processor (C2P) or C2P Rehost to Demand Assigned Multiple Access (DAMA) equipment via a KG 84A encryption device. The Navy's C2P, in turn, requires new software for this implementation. The Marine Corps' Common Data Link System (CDLS) also implements S TADIL J, as will the new Common Aviation Command and Control System (CAC2S) when it is fielded.

S TADIL J is the US Navy's Link 16 satellite technique.

A platform may operate on both the Link 16 network and the satellite concurrently. Transmissions on the satellite are generally delayed with respect to the Link 16 network, and data received from the Link 16 network is given precedence by the platform over data received from the satellite. When a JU "drops out," as evidenced by no PPLI reception for 60 seconds, the platform automatically and seamlessly takes data for that JU from the satellite.

S TADIL J implements most of the J-series messages, although those required for time-critical functions—such as network management, air control, and national use—are not implemented. It uses a token-passing, round-robin network protocol. Data to be transmitted over the satellite is conveyed over a completely separate path out of the C2P that does not pass through the JTIDS/MIDS terminal. The KG 84A and compatible cryptos are used for most standard serial data protocols.

The net cycle time associated with S TADIL J depends on the number of satellite JUs (SJUs), as well as on track volume. Clearly, data rates over satellite links at 2400 baud or 4800 baud are much lower than conventional Link 16 rates, and data latency is a potential problem. For example, a four-unit network exchanging information on 180 tracks at 2400 baud is estimated to require 24 to 26 seconds, rather than the 20 seconds discussed in the S TADIL J specification and observed during real-world experience. There is also a token-passing switching delay estimated to be two seconds per unit. Higher data rates will become available, however, as the EHF median data rate (MDR) satellite communications provided by MILSTAR become operational.

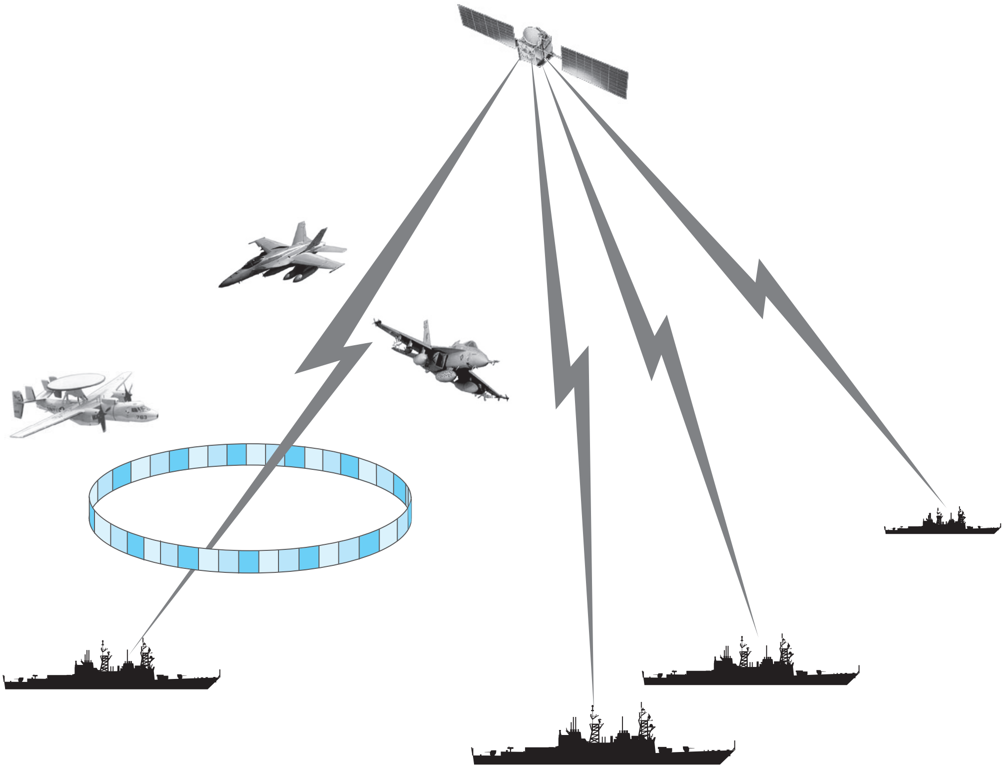


Figure 2-25. S TADIL J is a Navy technique for extending the range of Link 16 using a satellite and separate modulation techniques. The new Marine Corps CAC2S will also implement S TADIL J.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

NORTHROP GRUMMAN

Introduction

Link 11 employs netted communication techniques and standard message formats for the exchange of digital information among airborne, land-based, and shipboard tactical data systems. Providing mutual exchange of information among net participants using high-frequency (HF) or ultrahigh-frequency (UHF) radios, Link 11 is a half-duplex, netted, secure data link. Link 11 requires a Net Control Station (NCS) and Participating Units (PUs) to operate.

Link 11 Equipment

To understand the operation of the Link 11 system, it is important to be able to identify the hardware components that compose it and the functions they perform. In this section, you will learn the function of every component. You will trace the path of data all the way from the sending computer to the receiving computer. Understanding this pathway will help you to be able to isolate problems, when they occur, to the appropriate piece of equipment. Whenever a problem with Link 11 communications occurs, for example, you should no longer automatically assume "The data terminal set is bad."

While this section concentrates on shipboard equipment configurations, the general principles are the same for all configurations, whether they are located aboard a ship, or are shore-based or airborne platforms.

Overview of Link 11

Link 11, or Tactical Data Link (TDL) A, employs netted communication techniques and a standard message format — the M-series messages — for exchanging digital information among airborne, land-based, and shipboard tactical data system computers. Link 11 data communications must be capable of operation in either the HF or UHF bands. When operating in the HF band, Link 11 provides gapless, omnidirectional coverage of up to 300 nautical miles (nm) from the transmitting site. When operating in the UHF band, the link provides omnidirectional, gapless coverage to approximately 25 nm ship-to-ship, or 150 nm ship-to-air.

Link 11 allows tactical computers to exchange information.

■ Equipment Configuration

There are many different Link 11 configurations.

A representative Link 11 system configuration, which is illustrated in *Figure 3-1*, consists of a computer system, an encryption device, a data terminal set (DTS), an HF or UHF radio, a coupler, and an antenna. An external frequency standard may also be part of the system.

The computer system is called a Tactical Data System, or TDS. Airborne units are referred to as Airborne TDSs, or ATDSs, and shipboard units are referred to as Naval Tactical Data System, or NTDSs. The encryption device, or crypto, is a Key Generator-40 Alpha (KG-40A). Throughout this part of the guidebook, KG-40A will be used interchangeably with the terms encryption device and crypto.

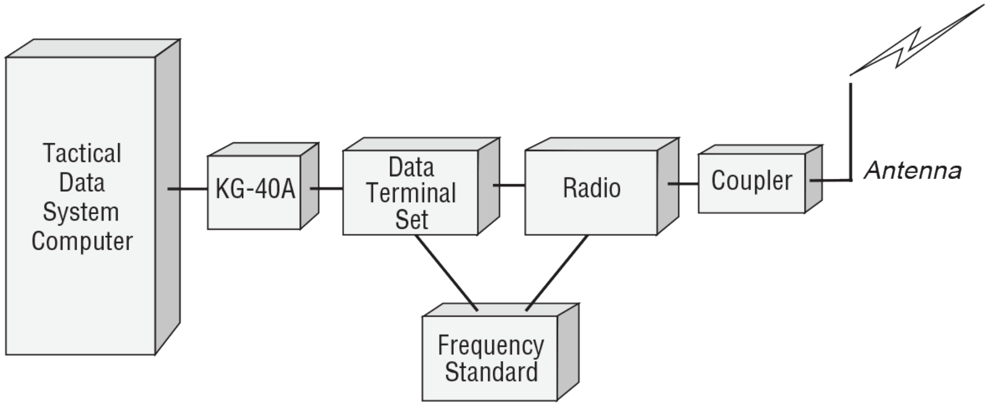


Figure 3-1. The Link 11 equipment configuration consists of a tactical computer system, an encryption device, a data terminal set, an HF or UHF radio, a coupler, and an antenna.

■ Data Flow on Transmission

Data flow on transmission is depicted in *Figure 3-2*. The tactical computer receives data from sensors, such as radar, navigation systems, and operators. It collects this information into a database. In order to share this database with other TDS computers, the information must be formatted into messages that have a specific, well-defined structure. Commands and other administrative information are also formatted into messages for distribution to other units.

These digital messages are placed into a **buffer**, an area within the computer memory reserved for input or output. When an output buffer is built, its contents are sent, one word at a time, to the KG-40A device to be encrypted.

On Link 11, all tactical data is encrypted before it is broadcast.

The encrypted data is then sent on to the DTS. The DTS converts this encrypted data from digital format to an analog audio signal. This signal is then directed to the Link 11 transmitter.

The transmitter modulates a radio frequency carrier with the audio signal and passes it through the antenna coupler to the antenna for broadcast to the other units participating in the link.

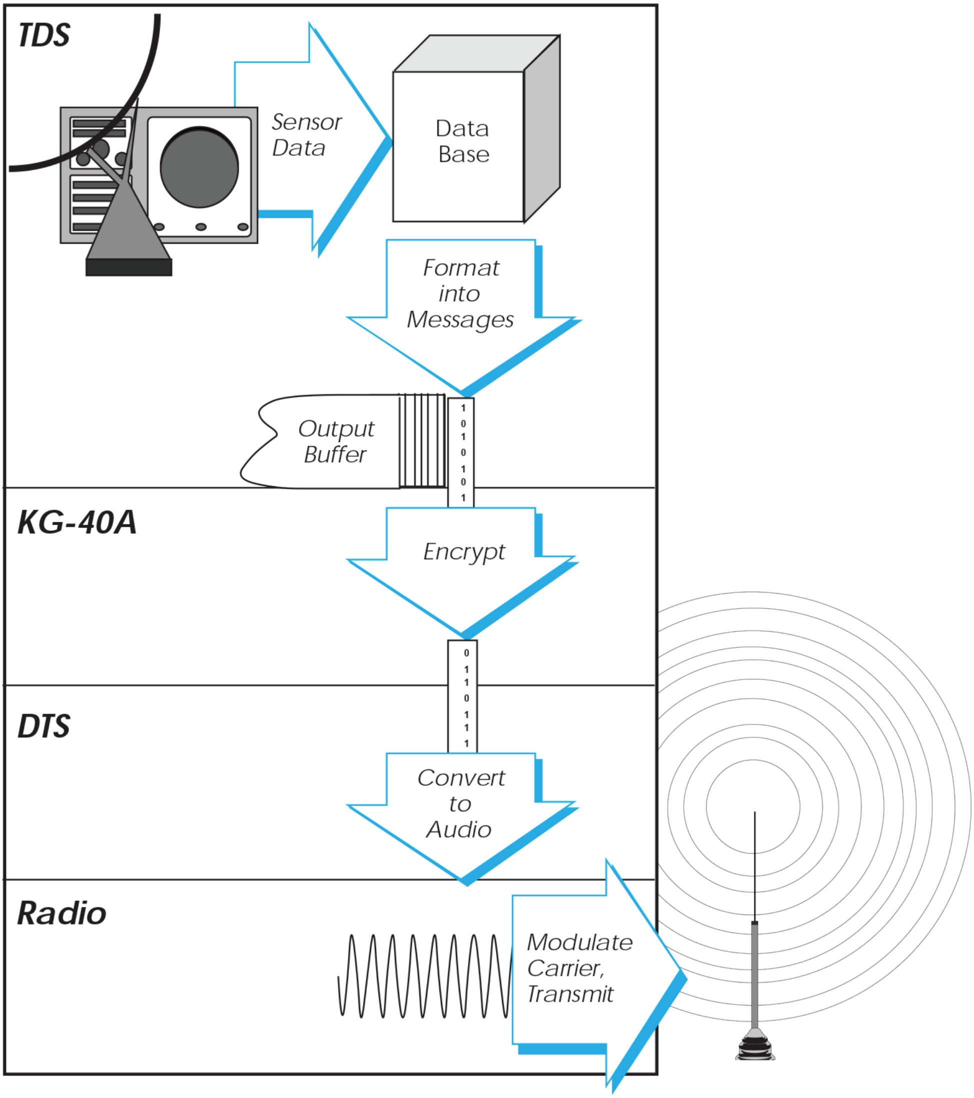


Figure 3-2. Sensor data and other input is formatted into messages, encrypted, converted to an audio signal, and broadcast to other net participants.

■ Data Flow on Reception

When a transmitted signal is received, the audio portion is demodulated from the radio frequency (RF) signal by the receiver. The resultant audio signal is sent to the DTS, where it is converted back into digital data. The digital data is then passed to the KG-40A one **frame** (parallel group of bits) at a time, where its information is decrypted. Finally, this decrypted data, once again in the format of the message originating at the transmitting unit, is sent on to the TDS computer, where it is collected in an input buffer for processing.

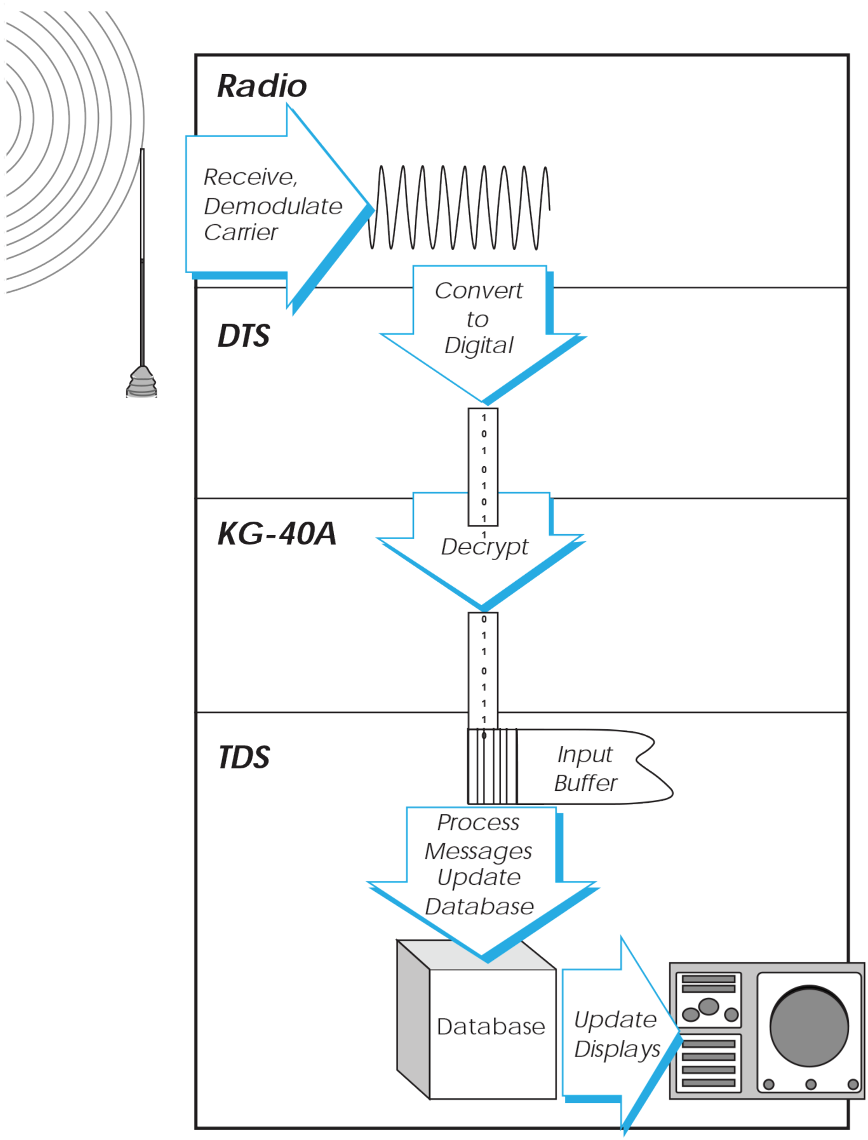


Figure 3-3. The received signal is demodulated to obtain the audio signal, which is converted back to digital data, decrypted, and passed to the TDS computer.

The Tactical Data System

Throughout the remainder of this Link 11 part of the guidebook, we will use NTDS to refer to the Tactical Data System to distinguish it more clearly from the DTS, or data terminal set.

Physically, these NTDS computers may appear quite different, but their Link 11 functions are identical:

- Supplying tactical digital information to net participants
- Retrieving and processing incoming tactical digital information received from net participants

The software executing in the tactical computer performs many other functions in addition to maintaining the tactical database. It manages the displays, performs interim updates of track locations, responds to operator entries and inquiries, and controls all peripheral input and output (I/O). All tactical system software is required to pass rigorous testing to be certified. This certification testing is performed by the Navy's SPAWAR Systems Center Pacific Code 59 (SSC Pac Code 59).

The Importance of Operator Entries

The NTDS computer accepts operator entries, such as the Data Link Reference Point (DLRP), PU addresses, track block data, and various filter select modes. It is very important that these selections be entered correctly. Improperly entering any one of these values will cause link communications either to degrade or to break down completely.

For example, a PU is transmitting good data with a strong signal. All of that data is input to the NTDS computer system for processing. However, the NTDS operator has failed to enter the number of that unit correctly into the NTDS system. So, as a result, none of the tracks originating from that PU will show on the NTDS display.

After information is received, it must be **correlated**, or matched, with information already existing in the database. Of particular importance is matching the positions of objects. An incorrect operator entry could prevent proper correlation, which may confuse the tactical picture with numerous uncorrelated tracks.

On Link 11, correctly matching the positions held by Own Unit with those of other units is known as gridlock. Failure to maintain gridlock may be the result of inaccurate positioning data from a ship's sensor, from the Ship's Inertial Navigation System (SINS), or from gyro data. It may also be the result of an inaccurate operator entry. Fortunately, external audio or visual alarms will usually alert the operator when navigation input failures occur. However, there are no such alerts for inaccurate operator entries.

■ DTS-to-NTDS Interface

The interface between the NTDS computer and the data terminal set, called the **NTDS interface**, is controlled by the DTS. Specifications for this interface are given in MIL-STD-1397. The KG-40A encryption device operates between the NTDS computer and the DTS. Although it encrypts the data, it does not otherwise affect this interface.

MIL-STD-1397 specifies both a parallel and serial NTDS interface. The parallel NTDS interface has 24 output data lines and 26 input data lines. The two extra input data lines correspond to the two bits added by the DTS to each incoming data word. These two bits, which are used to indicate the error status of the word, are summarized in *Figure 3-4*. The serial interface, used by the E-2, a Navy airborne unit, is described in Appendix G of the standard.

Value	Label	Correct
00	No errors detected.	No errors detected.
01	Not applicable.	Overall parity error detected.
10	Errors detected, no correction attempted.	Even errors detected, not corrected.
11	Not applicable.	Odd errors detected, correction attempted.

Figure 3-4. On reception, the DTS tags the 24 data bits with a 2-bit code that summarizes their bit error status.

Detected errors in the digital data will either be labeled or corrected, depending on the DTS switch setting.

Sometimes bit errors can be corrected by the DTS. However, whether or not the corrected data is used depends on the particular version of the Tactical Data System software. Errors in some messages can cause that message to be discarded, while errors in other messages can cause the entire transmission to be discarded. All NTDS systems discard the message containing the error, whether corrected or not. Other systems, such as the ATDS, may use data that has been corrected.

Shipboard NTDS systems do not process corrected data.

The Encryption Device

The KG-40A Encryption Device provides communications security (COMSEC) for each 24-bit word of tactical data that flows through the system. Each word is encrypted to prevent unauthorized interpretation.

The KG-40A encrypts and decrypts 24 bits of digital data.

Operator Entries

The KG-40A encryption device has four modes of operation: Cipher Al, Cipher A2, Cipher B, and Plain Text. When the KG-40A is properly loaded, COMSEC operation is fully automatic and requires no further operator intervention. This operation is so vital to data exchanges that the keylist should be loaded and cross-checked by two people.

Occasionally the KG-40A will become alarmed, usually when signals not meeting Link 11 protocol requirements are received. The alarm condition is indicated by a red light. When an alarm condition exists, no data will be passed in or out. Reset the KG-40A to restart the flow of data between the NTDS and the DTS.

The Data Terminal Set

The DTS is designed as a Modulator/Demodulator (MODEM). Normally, it operates in **half-duplex** mode, during which it can either send or receive data, but cannot do both simultaneously.

The single exception is during system test, when it operates in **full-duplex** mode and can send and receive data at the same time.

Additional functions performed by the DTS include the following:

- Error detection and correction
- Audio signal protocol generation
- Digital-to-analog conversion
- Analog-to-digital conversion
- Link protocol control
- NTDS interface control

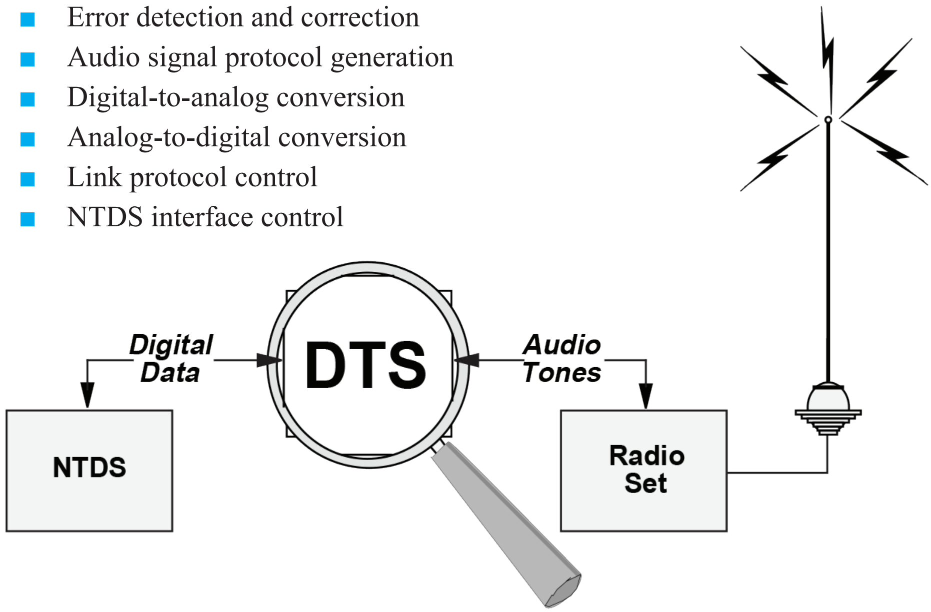


Figure 3-5. The DTS is the heart of the Link 11 system. In addition to encoding NTDS data into audio tones, it generates and recognizes protocol signals that control the operation of the net.

■ Error Detection and Correction (EDAC)

The DTS requests and accepts tactical data in the form of a 24-bit data word from the NTDS computer. To these 24 bits, it adds a 6-bit EDAC code. These 6 bits are also referred to as the Link 11 **Hamming bits**. The value of these bits is based on a parity check of specific combinations of the original 24 bits. These EDAC, or Hamming, bits allow error checking to be performed on received data words. If a single bit error occurs, it can be located and corrected. A selection on the DTS determines whether a detected error is to be labeled or corrected.

The DTS recognizes bit errors in the received signal. One bit in error can be corrected.

■ Audio Signal Generation

The newly formed 30-bit word is used to phase-modulate 15 internally generated audio tones. The 15 phase-modulated audio tones, together with a Doppler correction tone, are then combined into a composite audio signal that is applied to either the HF or UHF radio equipment for transmission.

The DTS converts the digital data to phase-shifted audio tones.

■ Link Protocol Control

In addition to encoding data from the NTDS computer, the DTS both generates and recognizes protocol data words that control the type and number of link transmissions. These protocol words include codes indicating the start of a transmission, the end of a transmission, and the PU address of the next unit to transmit.

■ NTDS Interface Control

The interface with the NTDS is under the control of the DTS. The DTS signals when it has input data and when it wants output data. The operation of this interface is controlled by an external interrupt from the DTS, with a code designating the purpose of the interrupt. The DTS-to-NTDS interrupt codes are summarized in

Figure 3-6. Interrupt codes 4 and 7 currently are not supported by most NTDS software.

Interrupt Code	Function
2	Reset
3	End of Receive
4	Prepare to Transmit, roll call with PU addresses supplied by the computer
5	Prepare to Transmit, roll call with PU addresses supplied by the controller
6	Prepare to Receive
7	Prepare to Broadcast *Source: MIL-STD-188-203-1A*

Figure 3-6. The DTS controls the input and output of data from the NTDS using interrupts. The interrupt code identifies the function to be performed by the NTDS.

Essentially, the NTDS computer is slaved to the DTS. When the DTS recognizes an output requirement, such as when its own PU number is received, it generates a Prepare-to-Transmit interrupt. The NTDS then provides the requested channel activity. When the DTS recognizes an input requirement, such as when a start code is recognized, it generates a Prepare-to-Receive interrupt. When the DTS recognizes the end of a data report, it generates an End-of-Receive interrupt.

The NTDS computer supplies and receives digital information only after being notified to do so by the DTS. The path from the DTS to the NTDS computer is completed through the KG-40A, which is required to be transparent to the flow of information between the DTS and the NTDS.

■ Modes of DTS Operation

There are six modes of DTS operation:

- Net Synchronization
- Net Test
- Roll Call
- Short Broadcast
- Broadcast
- Radio Silence

Net Synchronization (NS), also called "Net Sync," is used to establish communications initially. Net Test (NT) is used for connectivity checks and for checking or setting line levels. Roll Call (RC) is the normal mode of operating the Link 11 net. Short Broadcast (SBC) and Broadcast (BC) may be required for certain tactical situations. Not all data terminal sets support the Broadcast and Short Broadcast modes. Radio Silence disables all DTS output transmissions while continuing to allow for data reception. *Figure 3-7* summarizes the DTS system capabilities.

Characteristic	Description
NTDS Interface	In accordance with MIL-STD-1397 Type A (NTDS Slow)
Communications Interface	All DTSs can interface with the AN/SRC-16, AN/SRC-23, AN/URC-75, AN/WSC-3, AN/URC-93, AN/GRC-171, URC-81/83, R-1903, T-1322/SRC, AN/URT-23C/D, R-1051F/G/H link-capable radios.
Operator Interface	AN/USQ-74/83: Cathode Ray Tube (CRT) display/keyboard AN/USQ-36/59/79/76/92: Thumbwheel and/or manual switches/keypad
Tone Library	605-Hz Doppler tone and 15 phase-modulated tones: 935, 1045, 1155, 1265, 1375, 1485, 1595, 1705, 1815, 1925, 2035, 2145, 2255, 2365, and 2915 Hertz
Doppler Correction	Varies
Data Rates	1364 bits per second (slow) 2250 bits per second (fast)

Figure 3-7. DTS system capabilities (continued on next page)

Characteristic	Description
Controls	**Operate:** Transmit/receive or receive only (Radio Silent (RadSil)) **Net Modes:** Roll Call, Broadcast*, Short Broadcast*, Net Sync, Net Test **Sideband Select:** Automatic, Lower Sideband, Upper Sideband, Diversity **Timing:** Corrected or Stored **Error Correction:** Label or Correct **Station Mode:** Net Control Station or Picket **Doppler Correction:** On or Off Data Rate: Fast or Slow **Range:** Range to Net Control Station in nautical miles **NTDS Communications:** On or Off **C&D Control:** On or Off **XMT Chan:** Primary or Secondary
Status Indicators	**Normal Operation:** Communication Indicator, Receive Mode, Net Busy, Transmit Mode and Synchronization **Error Indication:** Receive Code Error, Transmit Data Error, Receive Data Error and Signal Quality*

** Not applicable to AN/USQ-36*

Figure 3-7. The DTS provides interfaces to the NTDS, the radio, and the operator.

■ Operator Entries and Selections

Many parameters affecting the operation of the DTS are under the operator's control. You must select the net mode of operation, whether your ship is acting as a picket (PKT) or the NCS, which sideband is to be processed, what type of timing is to be used, whether errors are to be labeled or corrected, whether or not frequency correction is enabled, which data rate to use, and so on. You must always enter your own PU address. As the NCS, you must also enter the addresses of PUs to poll. An explanation of configuration control settings is presented in *Figure 3-8*.

Unfortunately, not all DTSs have default settings for these entries and selections. On DTSs without default settings, the operator must explicitly check all settings on every occasion. The usual mode of operation is Fast data rate, Automatic sideband selection, Roll Call net mode, Fast and Continuous synchronization.

Control Name	Meaning
Net Mode	Selects the Net Mode in which to operate.
Roll Call (RC)	The NCS will automatically interrogate each picket in turn as determined by operator's PU number address setting in Address Array. ***NOTE*: Own Ship's PU number address (Own Address) has to be entered in NCS terminals; otherwise no own ship track data will be transmitted by NCS.**
Broadcast (BC)	Station will broadcast a continuous series of short broadcasts to all net participants. ***NOTE*: Broadcast initialization has to be coordinated with acting NCS to prevent net jamming (except AN/USQ-79 users).**
Short Broadcast (SBC)	Station will send a single data transmission to all net participants.
Net Sync (NS)	Enables the NCS to transmit continuous preamble frames (net synchronization). Enables the picket to receive a net synchronization transmission.
Net Test (NT)	Enables the NCS to transmit a known data pattern. At the picket station, the received pattern is compared with the known (stored) test pattern. Used for connectivity checks.
Radio Silence (RadSil)	Disables all DTS output transmissions, but does not prevent processing of received data.
Sideband Select	Selects which sideband (channel) or sideband combination will be used for receive signal processing.
Auto	The DTS will select the first error-free data from Upper Sideband, Lower Sideband or Diversity channel.
Lower Sideband (LSB)	The frequency band 3000 Hz below the assigned carrier frequency. The DTS is restricted to receiving on LSB only.
Upper Sideband (USB)	The frequency band 3000 Hz above the assigned carrier frequency. The DTS is restricted to receiving on USB only. ***NOTE*: The UHF band is restricted to a single audio channel only (USB).**
Diversity (DIV)	A combination formed from USB and LSB.

Figure 3-8. The configuration of the DTS (continued on next page)

Control Name	Meaning
Timing	Used to select the transmit time base mode.
Corrected (COR)	Enables correction of the time base each time own station address is recognized by a picket in Roll Call mode.
Stored (STR)	Enables use of the stored time base obtained during Net Sync mode. ***NOTE*: Can be used only by a picket station that has established sync during Net Sync operation.**
Error Correction	
L C	Selects whether an error in data reception is to be Labeled only or Corrected and Labeled.
NTDS Comm	
On Off	Inhibits or connects communications between DTS and NTDS computer. All other DTS functions remain unaffected.
Station Mode	
NCS	Indicates Net Control Station operation.
PKT	Indicates picket station operation.
Sync	
F/C	Fast and continuous frame sync is enabled.
F	Only fast sync is enabled. Sync only on five frame preamble period.
C	Only continuous sync is enabled. Sync occurs only during reception of Net Sync signal in the Net Sync mode.
Doppler Correction	
On	Doppler correction logic enabled.
Off	Doppler correction logic disabled.
Data Rate	
Fast	Fast data rate of 2250 bps.
Slow	Slow data rate of 1364 bps.
Range	
XXX	Picket enters 25-nm range increment to NCS to compensate for signal propagation delay.

Figure 3-8. The configuration of the DTS (continued on next page)

Control Name	Meaning
C&D Control* Address Control*	
On/Off	TDS computer-generated addressing is enabled/disabled.
XMT Chan*	
Pri/Sec	Selects UYK-20 transmit data channel to Converter Interface Unit. PRI=USB, SEC=LSB

* USQ-74 only

Figure 3-8. The configuration of the DTS is set by the operator.

■ Status and Error Indicators

The DTS reports current status and error conditions using indicator lights. While the specific set of indicators and their names may vary by DTS model, the following basic conditions are usually monitored and indicated:

- Transmit
- Receive
- Net Busy
- Transmit Data Error
- Receive Data Error
- Code Error
- Sync Complete

These indicators provide operators with useful information about the condition of the Link 11 signal input to, and output from, their DTSs.

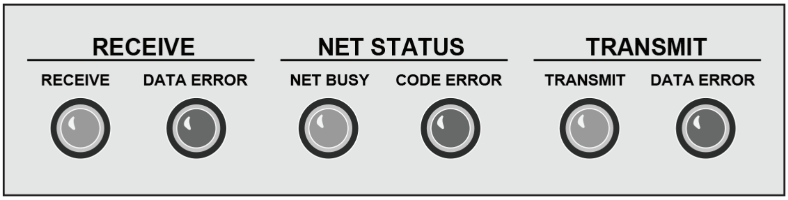


Figure 3-9. The DTS indicator lights show status and error conditions during link operations.

☐ Radios for Link 11 Data Communications

The Link 11 transmitters and receivers provide point-to-point connectivity between widely separated units in the net. The radios can be transmitter/receiver combinations in which the transmitter and receiver have independent functions. The other alternative is a radio with interdependent functions called a **transceiver**.

Two types of radio are used in Link 11. One type provides spectrum coverage from 2 - 30 megahertz in the HF band. The other provides coverage from 225 - 400 megahertz in the UHF band. HF is used to establish a net when the range between units in the net is from 25 to 300 nm. UHF is used when the range between units is less than 25 nm.

■ General Link 11 Radio Requirements

Link 11 radios must meet requirements that are different from radios designed for voice-only operation. The primary differences include the transmit-to-receive switching time, the keyline interface, the audio band-pass characteristics, the automatic gain control, the attack and release timing, and the audio input and output level conditioning. Because of the speed at which the link operates, all link communication equipment must be able to keep up with the repetitive cycles of transmission and reception. Sharing dedicated link transceivers for general service applications is to be discouraged.

Link 11 Radio Requirements
■ Switches quickly between Transmit and Receive
■ Audio bandpass is wider than voice bandpass
■ Transmitter must be keyed before data arrives
■ Fast Automatic Gain Control (AGC) attack and release times
■ Input at 0 dBm
■ Restricted phase jitter and envelope delay tolerances

Figure 3-10. The radio requirements for Link 11 are different from those of voice communications.

HF Radios

HF radios use a modulation technique called **Amplitude Modulation** (AM), in which the Link 11 audio signal is used to modulate, or vary, the amplitude of the carrier. These radios have several modes of operation, including Single Sideband Suppressed Carrier (SSBSC), Double Sideband Suppressed Carrier (DSBSC), Independent Sideband Suppressed Carrier (ISBSC), AM, and Continuous Wave (CW). In SSBSC, either USB or LSB is output, depending on the operator's selection. In DSBSC, both USB and LSB are output. In ISBSC, both the USB and LSB are output, but they are generated independently from separate LSB and USB audio input signals. The AM mode consists of the carrier and USB. In the CW mode, the carrier can be turned on and off, like Morse code.

Sum and difference frequencies are produced by HF radios when the carrier is amplitude-modulated with the audio signal.

For Link 11, the Independent Sideband Suppressed Carrier mode is used. In this mode, the Link 11 audio signals generated by the DTS are applied to both the upper and lower sidebands for transmission.

The carrier contains no information and is normally suppressed.

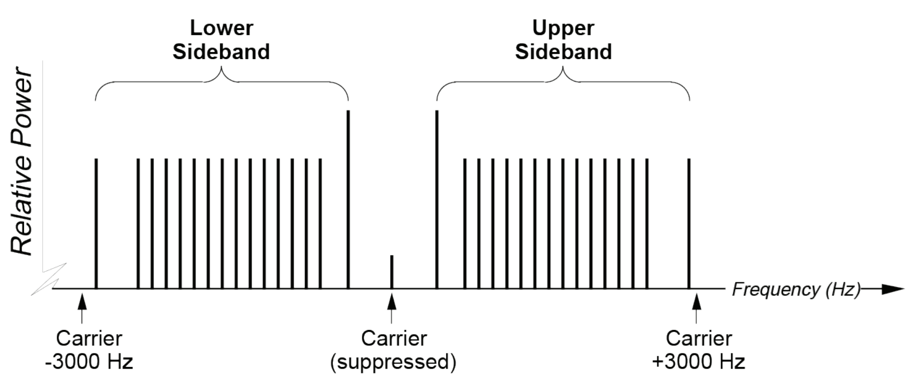


Figure 3-11. Upper and lower sidebands carry the information.

A sideband can be thought of as a channel. In HF Link 11 transmissions, both channels carry the same audio signal. The RF carrier frequency is not transmitted because it conveys no information. To extend the effective signal range, all signal power goes into the information-carrying sidebands. One advantage of using both sidebands with the same audio signal is that it affords a degree of diversity, so that signal fading and ambient noise can be overcome at the receiver. Whenever one sideband degrades, the other sideband does not degrade at the same time. The receiving unit can automatically select the best data from the upper sideband, the lower sideband, or the diversity.

A Single Side Band (SSB) transmitter that transmits the carrier frequency is in need of alignment. A good rule of thumb to remember is that an SSB transmitter with no modulation applied to its input should produce output at the antenna of no more than 0.8 Volts, measured as the root mean square (RMS). If the RMS output is greater than this, RF power is being wasted in the non-information portion of the spectrum, and the information portion may possibly be distorted as well.

The output from an unmodulated SSB transmitter should be less than 0.8 V RMS!

■ UHF Radios

UHF radios use a modulation technique called **Frequency Modulation** (FM). The Link 11 audio signal is used to modulate or shift the radio frequency about a center frequency. This technique of modulation is more resistant to interference than the technique of amplitude modulation. During the demodulation process, FM receivers limit the number of amplitude deviations. Only frequency deviation is used to extract the information from the signal. However, UHF is limited in range to line-of-sight.

UHF radios, although quieter than HF, are limited to line-of-sight.

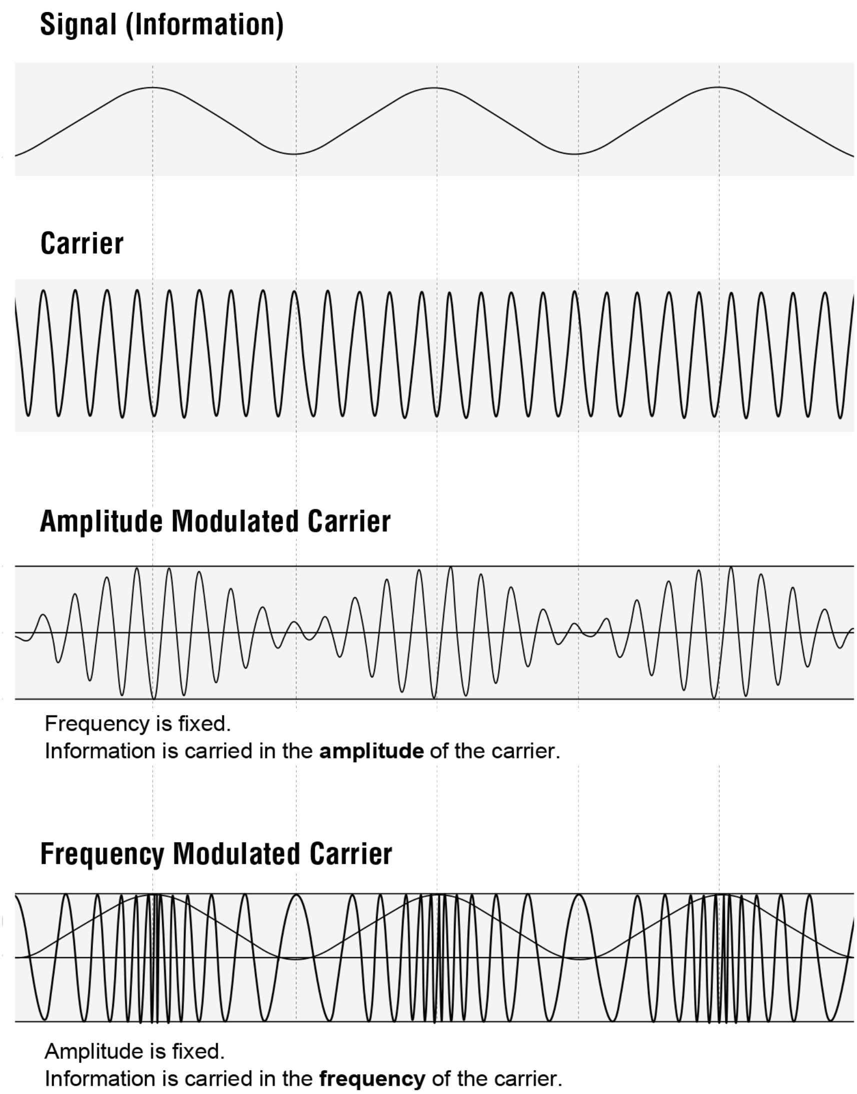


Figure 3-12. The information signal to be transmitted is modulated with a carrier of a much higher frequency. An HF transmission conveys information in the changing amplitude of the carrier. A UHF transmission conveys information in the changing frequency of the carrier.

Antenna Couplers

The transmitter/receiver is connected to the antenna through an antenna coupler.

HF Couplers

For every frequency, there is an ideal antenna of a specific electrical length. The lower the frequency, the longer is its ideal antenna; conversely, the higher the frequency, the shorter is its ideal antenna. A full-wavelength antenna designed to resonate at 4 MHz would ideally be about 250 feet long, an unsuitable length for shipboard installations. Instead, antennas are designed in submultiple lengths that are physically more suitable for installation aboard ship.

An antenna's impedance changes as the frequency changes. Because link HF communications cover a bandwidth of 28 MHz (from 2 to 30 MHz), a device is required for adapting a fixed-length antenna (usually 35 feet long) to a transmitter operating in that range. This device, called an antenna coupler, matches the transmitter's 50-ohm output impedance to the antenna's varying impedance.

A coupler matches the radio's output impedance to that of the antenna.

Some couplers provide the added advantage of allowing many transmitters to be fed into a single antenna. The resulting configuration is called a **multicoupler group**.

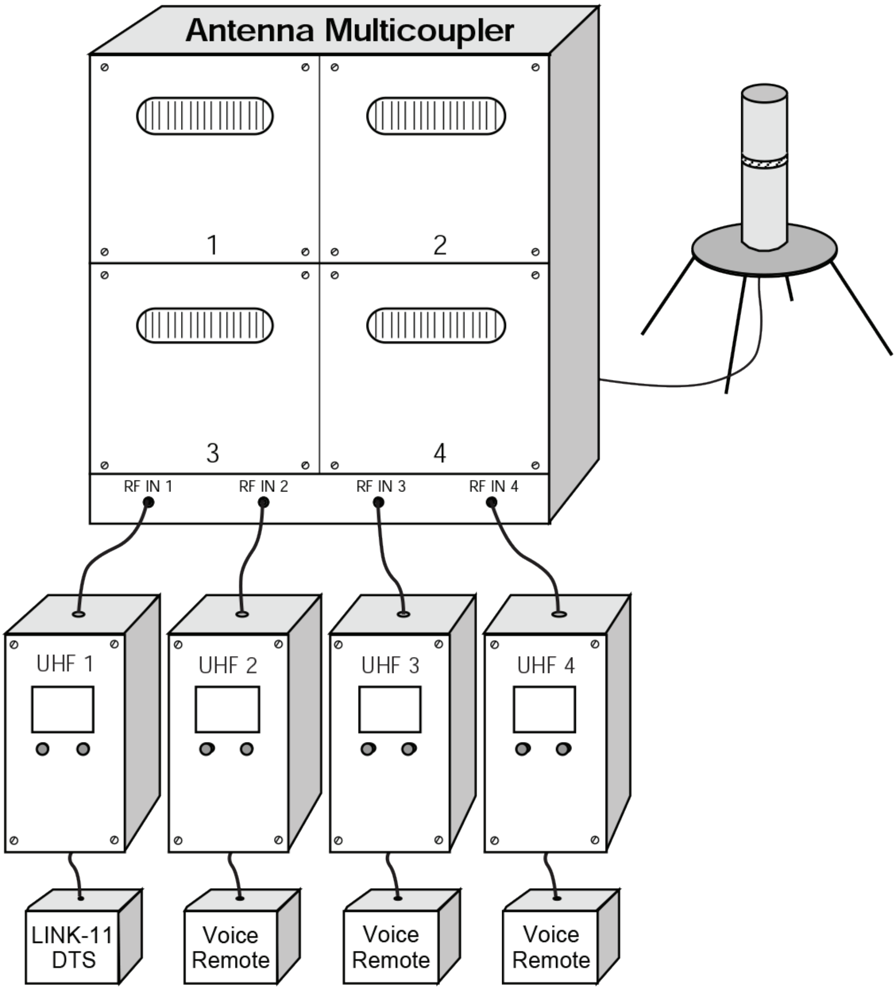


Figure 3-13. The antenna multicoupler allows multiple transmitters to feed a single antenna.

Multicouplers require frequency management to prevent influence across adjacent channels. Typically, a 15 percent frequency separation between adjacent channels should be maintained. Failure to maintain sufficient frequency separation between adjacent channels will allow adjacent couplers to leak energy between units. Serious signal distortion, as well as costly equipment failure, may then occur.

Maintain 15% frequency separation between adjacent HF multicoupler channels!

■ UHF Couplers

In general, UHF antenna couplers are combined within the system group or are part of the UHF transceiver. Because they have smaller components and lower power requirements, UHF couplers typically perform quite well.

Most UHF antenna couplers contain preset channels, a feature which permits faster tuning and remote selection of predesignated channels. On the surface, remote selection may appear to be a tactical advantage. The problem with having the user remotely select tactical channels is that he may create a frequency management nightmare. The user cannot effectively maintain the proper frequency separation between adjacent predesignated channels; the result may cause a voice channel to appear on another TDL's channel, or vice versa. The frequency separation required for UHF is 5 megahertz.

To prevent frequency separation problems, most installations provide designated radios, frequencies, and multicouplers. The user then selects the audio path connection to the desired channel. In this way, potential frequency management problems and hardware configuration problems can be circumvented in advance.

Maintain a 5-MHz frequency separation between adjacent UHF multicoupler channels!

Antennas

An antenna performs two functions: radiating electro-magnetic energy from a transmitting device to the atmosphere, and converting the atmospheric electromagnetic radiation to radio frequency current for the receiver.

HF Antennas

The simplest type of antenna is a single tall pole, or monopole. Shipboard HF antennas are variations of the monopole type. Most commonly, they are single 35-foot whips, constructed either of aluminum sections or of tubular or rectangular fiberglass. Whip antennas are rugged and offer minimal wind resistance. They may be mounted in either stationary or movable positions. Some units have a twin-whip design to increase directivity and gain characteristics. Other types of HF antennas include the fan and twin fan antenna, and for higher frequencies, the conical monopole and the trussed whip.

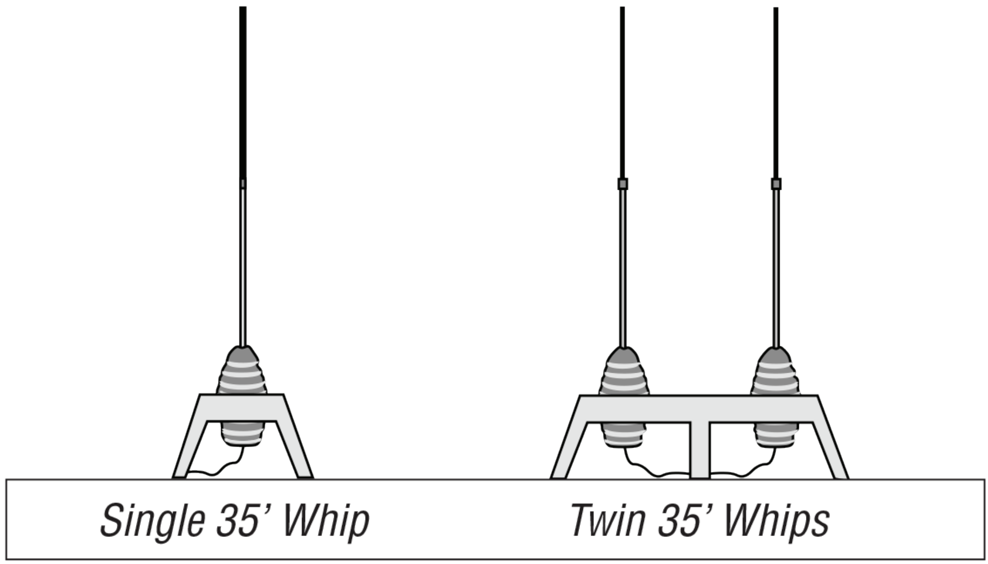


Figure 3-14. Antennas transmit and receive radio waves. Whip antennas are rugged and offer minimal wind resistance.

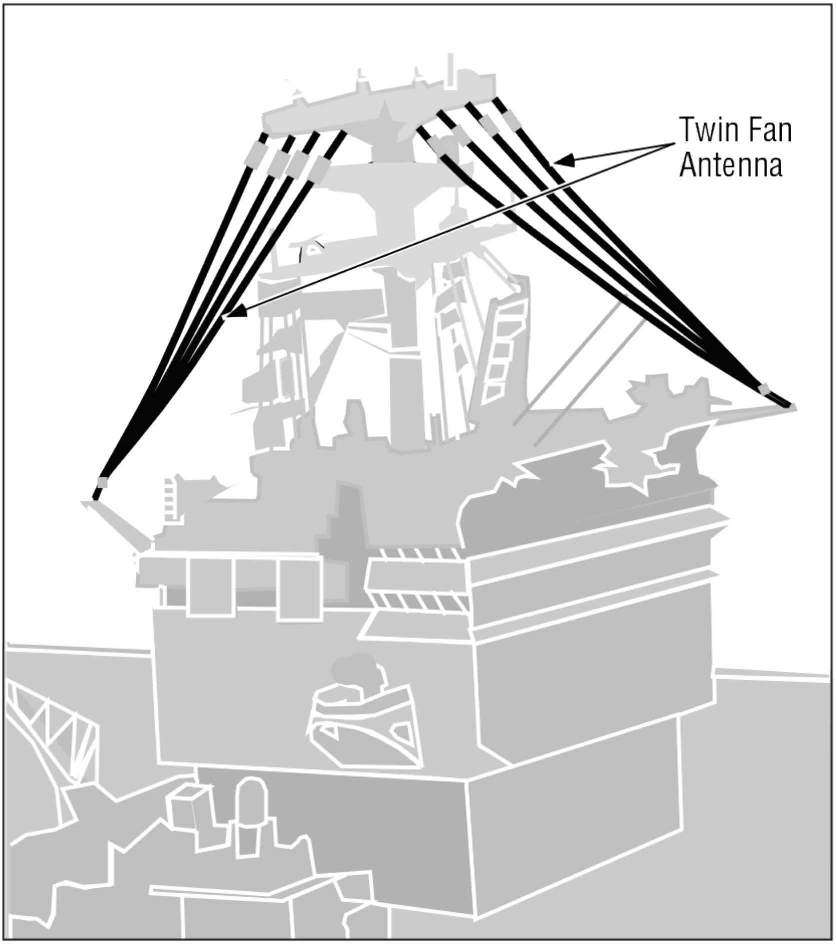


Figure 3-15. Another long wire type of antenna found on ships is the fan or twin fan antenna. Normally, it is positioned close to the horizontal or at a 45-degree angle.

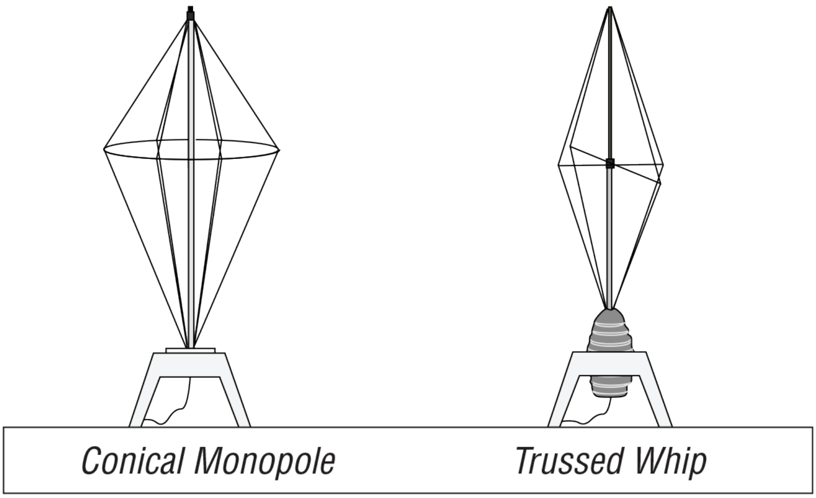


Figure 3-16. At higher frequencies, HF antennas can be made smaller in size. The conical monopole and the shorter trussed whip are antennas of this type.

Because they are often out of sight and inaccessible, antennas are often neglected. The degradation that results from neglect is not manifested in predictable ways. Some results of poor receive characteristics, such as high net cycle time arising from double-polling most net participants, or NCS interrogations superimposed on responding PUs, go largely unnoticed, or are not attributed to antenna problems. You may become accustomed to operating the net with degraded antennas, until eventually your unit is never again assigned the role of NCS because the net simply does not function well when your unit has it.

■ UHF Antennas

UHF antennas do not present the same problems as HF antennas. Because they are small, they can be mounted nearly anywhere on the mast, the higher the better. Because less hardware is exposed to the elements, UHF antennas generally require less maintenance than HF antennas.

Instead, UHF, which is a line-of-sight signal, is subject to other phenomena, such as shadowing, quadrant blockage, and ducting. Shadowing and blockage of the UHF antenna effectively limit omnidirectional coverage. Null points, or dead areas, in the antenna radiation pattern may prevent the user from establishing full-period omnidirectional coverage.

Antenna radiation pattern null points result when the antenna becomes obstructed by metal objects, such as a mast or a radar antenna platform. RF energy strikes these metal objects and is reflected around them. An analogy is the shadow (or “null point”) created when you stand in front of the beam (UHF antenna radiation) of your car headlights.

Ducting in the UHF band, while rare, does occur and allows us to communicate over hundreds of miles. Communications may continue for several hours and then suddenly drop out completely.

Patch Panels and Switchboards

A means of interconnecting the Link 11 system’s components is required. The ability to isolate and test a simple component must be considered. Redundancy in some components must also be considered. For example, all ships have more than one radio. This redundancy helps to ensure link capability even when a particular component has failed or is undergoing preventive maintenance. Flexibility in the way components are connected is essential. By using patch panels and switchboards, we can accomplish the connectivity requirements while also providing maximum component flexibility.

Patch panels and switchboards allow components of the Link 11 system to be connected in different configurations.

The four major equipment areas (NTDS computers, encryption devices, DTSs, and RF systems) are connected to one another through various types of patches. This allows the operator to detour around inoperative equipment. Patching configurations are unique to each class of ship. One configuration uses both patch cables and manual switches, while another configuration may contain only manual switches, or even a mix of computer-controlled input/ output selectors.

A patching system may appear to be basic and uncomplicated. However, in actuality, the parallel I/O switching to an NTDS computer is both complicated and failure prone. Each of the 26 receive and 24 transmit bits, as well as the five control signals (three for receive and two for transmit), requires a pair of conductors to connect the NTDS computer to the encryption unit and the encryption unit to the DTS. To achieve both transmit and receive connectivity, 110 conductors are required. To accomplish the necessary switching between units, mechanical switches must have a section or wafer dedicated to each pair of conductors.

Switches that have an open-faced construction have the greatest number of problems. Ambient dust and dirt can corrode the multiple switch contact surfaces. The loss of a single bit of data along this pathway is very difficult to detect.

Include the patch panels in your maintenance checks.

☐ The Link 11 Data Path

The successful exchange of Link 11 tactical information requires that the data pathway extend completely from the transmitting NTDS computer to the receiving NTDS computer.

The flow of data during transmission is illustrated in *Figure 3-17*. The 24 bits of message data are encrypted in the Key Generator (KG), and the encrypted bits are passed to the DTS. In the DTS, six Hamming bits are added for EDAC purposes. The resulting 30 bits are encoded into the phase shifts of the 15 Link 11 audio tones. These are then summed with the unshifted 605-Hz Doppler tone to form a composite signal. Two signals are generated from this: USB and LSB. In HF communications, both are input to the radio for transmission as independent sidebands of an amplitude-modulated carrier. In UHF communications, the USB signal is input to the radio for transmission on a frequency-modulated carrier.

For this data transfer to occur, several operator entries and switch positions must be correct. The operator entries in the NTDS must be correct. The TDS, KG, and DTS must be properly cabled, and the KG cannot be in the alarmed state. Your own ship's address must be entered correctly in the DTS. The audio signal must be correctly cabled to the radio. The radio must be set both for data and to the correct frequency. Proper frequency separation must be maintained between coupler channels.

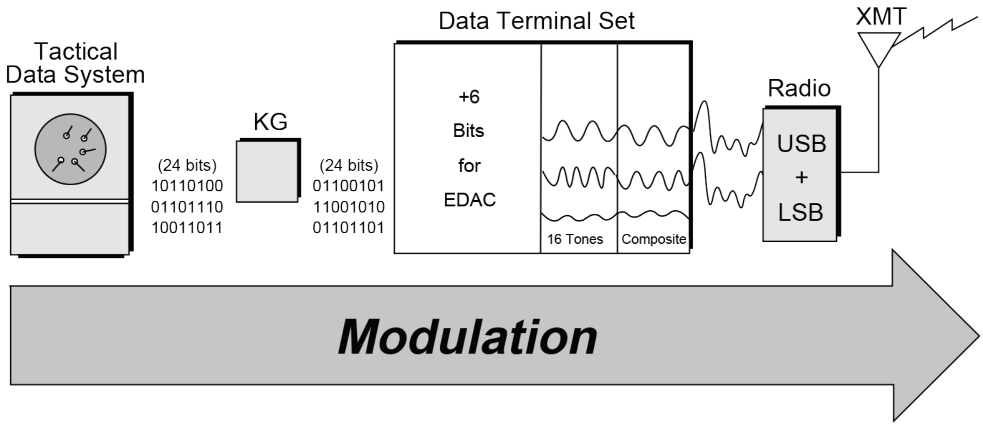


Figure 3-17. Twenty-four bits of encrypted digital data flow from the NTDS to the DTS, where six bits are added for EDAC. Finally, the entire 30 bits are encoded into an audio signal, which is then directed to the radio for transmission.

Once the signal has been transmitted, it can be received by another unit. The flow of data during reception is illustrated in *Figure 3-18*. The transmitted signal is received by the antenna and passed to the radio receiver. On HF, two sidebands are demodulated from the carrier, the USB and the LSB. On UHF, a single signal is demodulated from the carrier and appears on the USB channel. The demodulated audio signals, input to the DTS, are decoded into 30 bits of digital data based on the phase of each of the 15 data tones. The 30-bit value from the specified sideband (USB, LSB, DIV, AUTO) is selected for further processing. The 6 EDAC bits are examined to determine whether there are any errors in the 24 data bits. A 2-bit error status summary is added to the 24 data bits. Finally, the 24 data bits are decrypted within the KG and passed, with their two error status bits, to the NTDS computer.

For this reception data transfer to occur, several operator entries and switch positions must be correct. Proper frequency separation must be maintained between coupler channels, and the radio must be set for data and on the correct frequency. The transmitting ship must be within range and the signal not blocked, jammed, or otherwise degraded. The audio signal(s) must be correctly cabled to the DTS, and input at 0 decibels with respect to one milliwatt (dBm). Doppler correction should be enabled at the DTS, and the correct sideband selected. The DTS, KG-40A, and NTDS must be properly cabled, and the KG-40A cannot be in the alarmed state. The PU number must be entered correctly in the PU list at the NTDS.

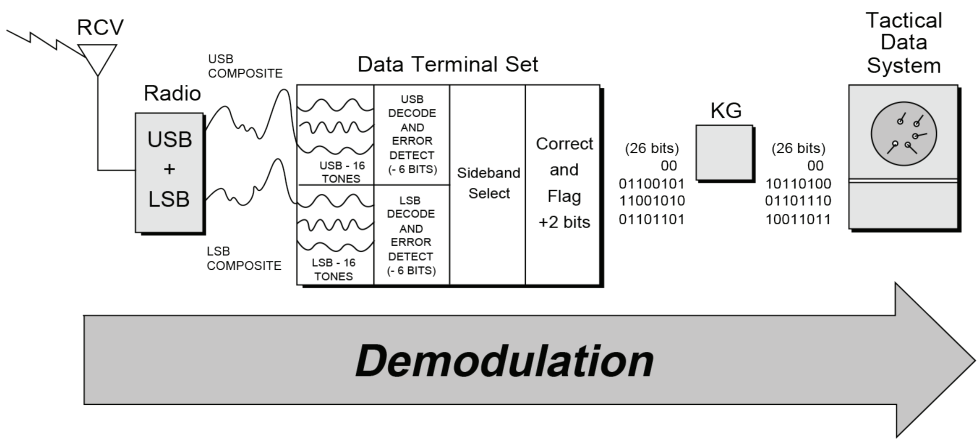


Figure 3-18. Audio signals are demodulated from the carrier by the radio and are passed as USB and LSB to the DTS. These audio signals are decoded into 30 bits of data. Six of these bits, the EDAC bits, are processed and replaced by two bits that report the error status. The 24 bits for the selected sideband are decrypted in the crypto and are then passed with the two error status bits to the NTDS computer.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Chapter 4 Understanding Link 22

Introduction

Link 22 is a North Atlantic Treaty Organization (NATO) secure radio system that provides Beyond Line-of-Sight (BLOS) communications. It interconnects air, surface, subsurface and ground-based tactical data systems, and is used for the exchange of tactical data among the military units of the participating nations.

Section A

History and Background

During the late 1980s, the North Atlantic Treaty Organization (NATO), agreeing on the need to improve the performance of Link 11, produced a mission need statement that became the basis for the establishment of the NATO Improved Link Eleven (NILE) Program. The program specified a new tactical message standard in the NATO STANdardization AGreement [STANAG 5522] to enhance data exchange and provide a new, layered communications architecture. This new data link was designated Link 22.

Requirements

The operational requirements are defined in the NATO Staff Requirement of 9 March 1990. The system, functional and performance requirements are defined in the NATO Elementary Requirements Document dated 12 December 1994.

Goals

The Link 22 goals are to replace Link 11, thereby removing the inherent limitations of Link 11; to improve Allied interoperability; to complement Link 16; and to enhance the commanders' war fighting capability.

Memorandum of Understanding

The Link 22 Program was initially conducted collaboratively by seven nations under the aegis of a Memorandum of Understanding (MOU). The original seven nations were Canada, France, Germany, Italy, the Netherlands, the United Kingdom (UK), and the United States (US), with the US acting as the host nation. Spain has replaced the Netherlands as a NILE Nation.

The NILE Project began in 1987 and was originally governed by MOUs that successfully covered the Project Definition Phase and the Design and Development Phases. Since 2002, the Project has been governed by an MOU and its amendments that cover the In-Service Support phase.

A steering committee guides the complete program. The program is managed by the Project Management Office (PMO), located at the Space and Naval Warfare Command (SPAWAR)'s Program Management Warfare (PMW) 150 in San Diego, California.

The PMO consists of a representative from each participating nation and a Project Manager from the US.

Development Approach

The design of Link 22 was performed using a "layered" approach, similar to the layers of a standard International Organization for Standardization (ISO) communications stack, which isolates specific functions within specific layers.

The layered development approach attempted to maximize the following:

- Reuse of existing Link 11 radios and equipment
- Use of Commercial Off-The-Shelf (COTS) computers
- Automated operation, thereby minimizing human-machine interaction

In addition, the goal of the message standard for Link 22 was to use as much of the Link 16 message standard as possible.

Phased Development

Link 22 employed a phased development, as shown below:

- 1989 – 1992: Project Definition Phase
- 1992 – 1996: Design and Development Phase One
    - Develop the prototype **Link Level Communications Security (COMSEC) (LLC)**
- 1996 – 2002: Design and Development Phase Two
    - Develop the production LLC
    - Develop the System Network Controller (SNC) software
    - Develop the High-Frequency (HF) fixed frequency Signal Processing Controller (SPC)
    - Develop the NILE Reference System (NRS) (Compatibility Tester)
    - Integrate Link 22 into the Multiple Link System Test and Training Tool (MLST3) (Interoperability Tester)
- 2002 – 2013: In-Service Support (ISS) Phase

SNC Standardization

To ensure compatibility across implementations, all participants must use the standard SNC software. Each implementing nation will acquire this software and will implement it in a hardware environment suitable for its own application.

Test Tools and Testbeds

The test tools consist of a compatibility tester called the NRS and an interoperability tester, the MLST3. These test tools are complete systems, consisting of both hardware and software. The NRS can be used to test whether a nation's implementation of the SNC is compatible with the standard SNC. The MLST3 tests the interoperability of the new systems in a multilink environment, in which Link 22 may operate concurrently with Link 11 and Link 16.

Purpose

The intent of this version of the Link 22 chapter is to provide a reference document on the Link 22 System that is releasable to any Nation or National contractors that are interested in learning about Link 22. It is used to provide general information about the functioning and operation of the Link 22 system, including a description of the NILE products.

Section B

Link 22 Overview

Link 22 is a NATO secure radio system that provides BLOS communications. It interconnects air, surface, subsurface, and ground-based tactical data systems, and it is used for the exchange of tactical data among the military units of the participating nations. Link 22 will be deployed in peacetime, crisis, and war to support NATO and Allied warfare taskings.

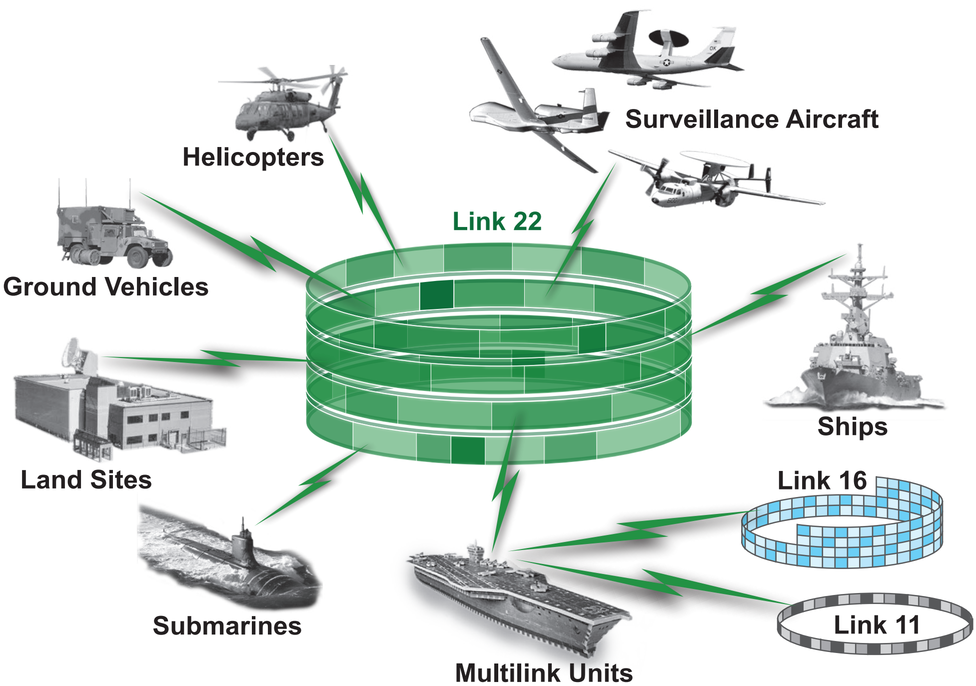


Figure 4-1. Link 22 Network Overview.

The Link 22 Program was initially conducted collaboratively by seven nations under the aegis of a **Memorandum of Understanding**. The original seven nations were Canada, France, Germany, Italy, the Netherlands, the United Kingdom, and the United States, with the United States acting as the host nation. Spain has replaced the Netherlands as a NILE Nation.

Link 22 was developed to replace and overcome the known deficiencies of Link 11. Link 22 was also designed to complement and interoperate easily with Link 16. It was designed with automated and simple management to ensure that it is easier to manage than both Link 11 and Link 16. This program is called "**NATO Improved Link Eleven**," which is abbreviated to "**NILE**." The tactical data link provided by the NILE system has been officially designated Link 22.

Communications Security

Link 22 employs a strong COMSEC system, which is provided by the inclusion of an integral encryption/decryption device inside the Link 22 system. This cryptographic device (crypto) at the data link level is called the LLC. It uses the same electronic chip used by Link 16. The LLC also provides detection of attempts to disrupt the network. A new Modernized LLC (MLLC) is planned for the future, to comply with the US National Security Agency (NSA) Crypto Modernization Roadmap. Link 22 transmission security is also available by the optional use of frequency hopping radios.

Tactical Messages

Tactical data is transmitted on Link 22 in fixed format messages, which are part of the **J-series** family of messages. It uses the same field definitions as Link 16 to provide standardization between the two tactical data links. Many of the Link 16 tactical messages are transmitted without modification within Link 22 tactical messages. Link 22 specific messages are more efficient versions of Link 16 messages and therefore use less bandwidth. Link 22 provides a number of **Quality of Service (QoS)** features, which are specified with each transmission request. Among other features, the selection of messages for transmission is based on the priority and the QoS of each message, which provides better use of available resources based on the operational situation.

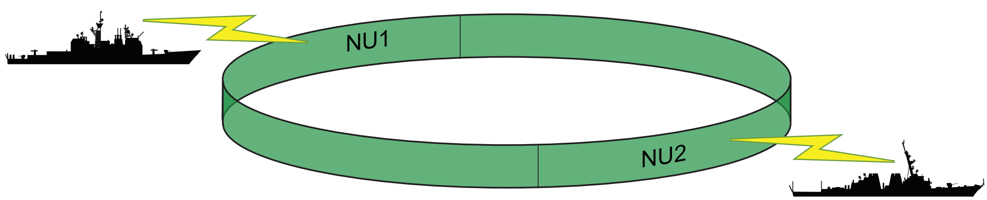


Figure 4-2. A simple Link 22 network between two tactical data links.

Link 22 Super Network

An operational Link 22 system is called a Link 22 **Super Network**. In its simplest form, a Link 22 Super Network consists of just two units communicating with each other in a single NILE Network. The most complex Link 22 Super Network would consist of the maximum number of units (125) with eight NILE Networks. A unit participating within the Link 22 Super Network can be a member of up to four of the NILE Networks. A more complex Super Network is shown in *Figure 4-3*.

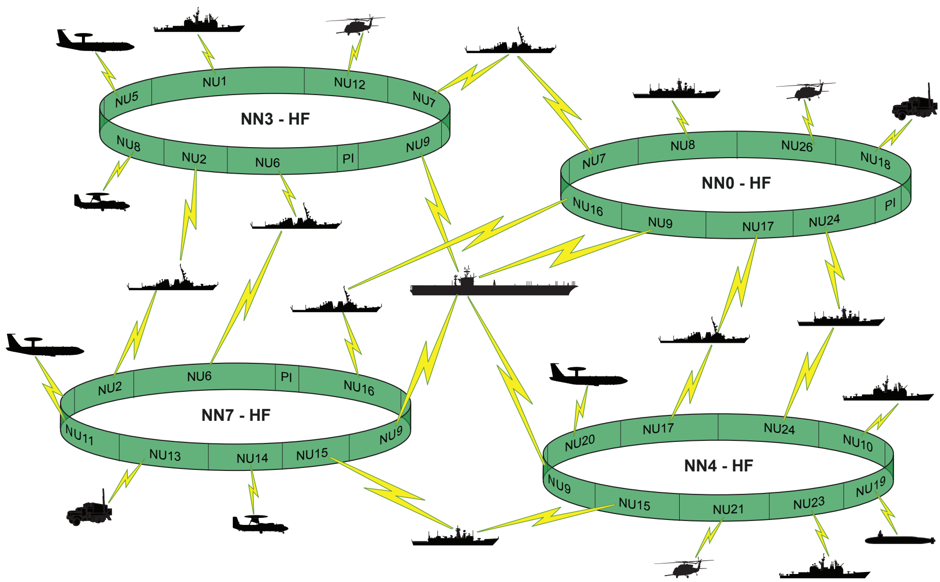


Figure 4-3. The Link 22 Super Network.

A Super Network enables seamless communication between units using different media to satisfy operational requirements within prevailing media propagation conditions. In a Super Network, any NILE unit can communicate with all other NILE units without regard to the NILE Network in which they are participating, thereby extending the operational theater. When a unit retransmits a message to extend coverage this is called relay, which is an automatic function of Link 22.

□ Automatic Relay

Coverage beyond what the media itself is capable of is provided by the automatic relay of messages and the ability to adapt to changes automatically, without operator intervention. This removes the need for dedicated air relay platforms and relay slot planning and management. A unit will automatically retransmit a received message when necessary to ensure that the message is received by its addressees. The SNC calculates whether the relay is necessary, based on its knowledge of the connectivity among units. The ability of a unit to relay can be affected by its relay setting. This setting's default is automatic relay, but the unit can be disabled from performing relay or designated as a preferred relayer. Relay is performed on a per message basis. Because messages are retransmitted only when necessary, this reduces the use of bandwidth.

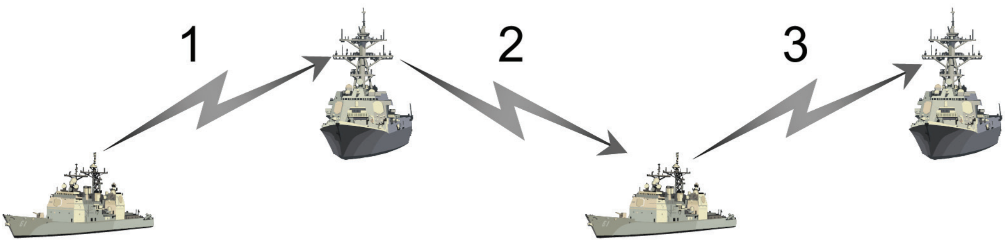


Figure 4-4. Automatic Relay Function of Link 22.

□ Beyond Line-Of-Sight Communication

Each NILE Network can employ either HF or Ultra High Frequency (UHF) communications.

HF communications are in the 2-30 MHz band, which provides BLOS communication (HF Sky Wave or HF Ground Wave) optimized for (but not limited to) transmission up to 300 nautical miles. HF also provides direct Line-Of-Sight (LOS) communications.

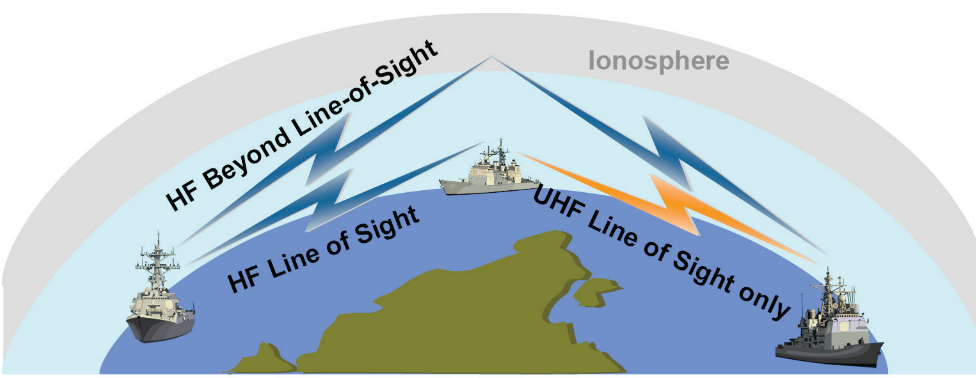


Figure 4-5. BLOS Communication on NILE Network.

UHF communications are in the 225-400 MHz band, which provides only LOS communication.

Within each band, either fixed frequency or frequency hopping radios can be used. Greater coverage is provided by the automatic relay of messages within the Link 22 system as previously mentioned.

Strong Waveforms and Error Correction

Link 22 has better tactical data throughput than Link 11, and it can even work in conditions where Link 11 will not. When conditions are bad, Link 22 can use more robust media parameters and maintain communication, although at a lower data rate than usual. When conditions are good, Link 22 can optimize the media parameters to maximize its data throughput. For example, specific media parameters were designed to operate in high latitudes, which present some of the worst-case conditions, and where Link 11 rarely operates.

Figure 4-6. Comparison of Link 11 and Link 22 Tactical Data Throughput.

Distributed Protocols – No Single Point of Failure

Link 22 uses distributed protocols, so it has no single point of failure (that is, the loss of a single unit does not cause the loss of an entire network). Some units perform specific management roles, but the system will continue operating without them. Each unit that performs a special role is required to designate a Standby unit, which can automatically take over the role in case of failure.

Link 22 has automated Network Management functions that require a minimum of operator interaction, if any. These functions are controlled by the transmission of Network Management messages. Each unit can define whether or not to automatically respond to, and whether or not to automatically perform, each of the Network Management functions.

Time Division Multiple Access

Time Division Multiple Access (TDMA) is the method by which the transmission capacity available to the entire network is distributed among its members. A cyclical period of time is divided up into timeslots, which can be of different durations. Most timeslots are allocated to specific units in the network. A unit transmits during its own timeslots. All other units listen during this period, and they may or may not receive the transmission. Priority Injection timeslots may be available, which can reduce the length of time a unit has to wait before it is able to transmit high-priority messages. If multiple units transmit in a Priority Injection timeslot at the same time, the transmission may not be received. Because of this, the transmission is also repeated in the units' own timeslot.

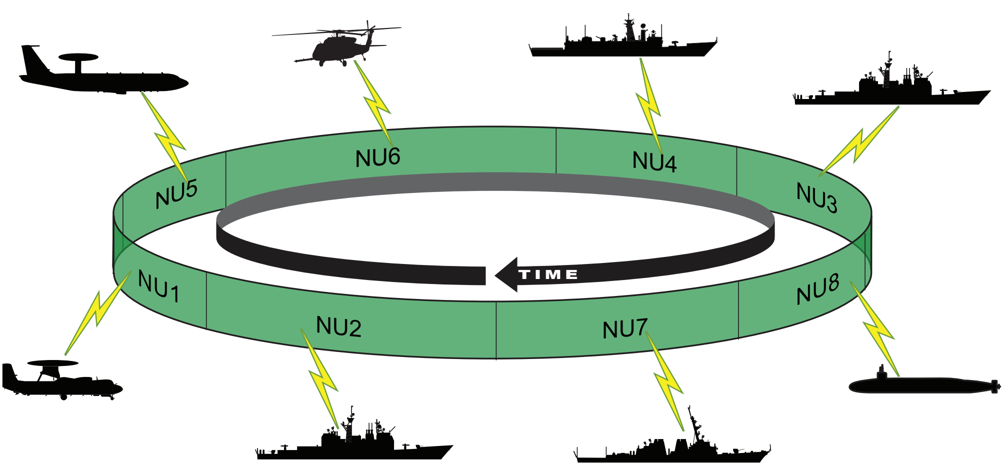


Figure 4-7. TDMA Architecture.

Automated Congestion Management

At the tactical level, when a unit is congested, it can reduce the local traffic that it generates based on the provided congestion information. In addition, Link 22 automates Congestion Management in a number of different ways. The routing of messages takes congestion into account and will route messages using alternative paths to reduce congestion. Link 22 has a Dynamic TDMA (DTDMA) protocol which, when enabled on a NILE Network, allow congested units to automatically request and receive additional capacity on a permanent or temporary basis (thereby modifying the TDMA structure). If DTDMA does not achieve the desired result, the unit managing a NILE Network can change the configuration of the network to redistribute the available capacity, or change the parameters of the media in use in an attempt to increase the network's capacity. As a last resort, a unit can interact with the operator to decide which, if any, of the tactical messages received and queued for relay may be deleted.

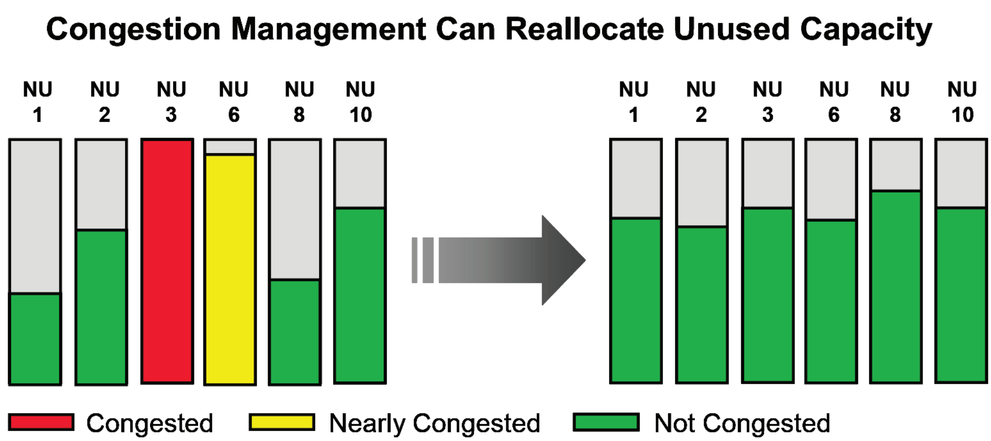


Figure 4-8. Automated Congestion Management on NILE Network.

Late Network Entry

After the Super Network has been started, units that arrive late can join the tactical data link by initiating a protocol called **Late Network Entry (LNE)**. The system also supports units that just want to listen to a network, called receive-only units, which have the capability to request access to the network, but are not allocated any transmission capacity. In addition, the system also supports units that only want to listen to a network without performing any transmissions at all (silent join units).

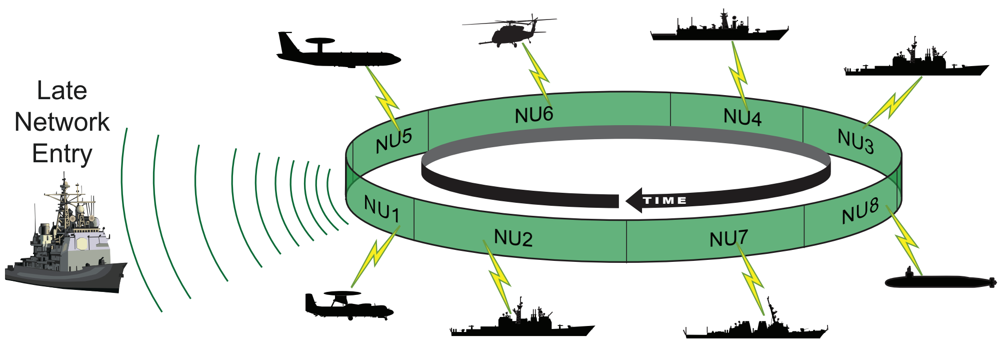


Figure 4-9. Late Network Entry on Link 22 Super Network.

Test Facilities

The NILE Project has funded the development of extensive Link 22 test facilities that are available for both compatibility and interoperability testing. Only these test systems are covered by this Link 22 chapter. Nations may develop their own Link 22 test systems, but they are not included in this Link 22 chapter.

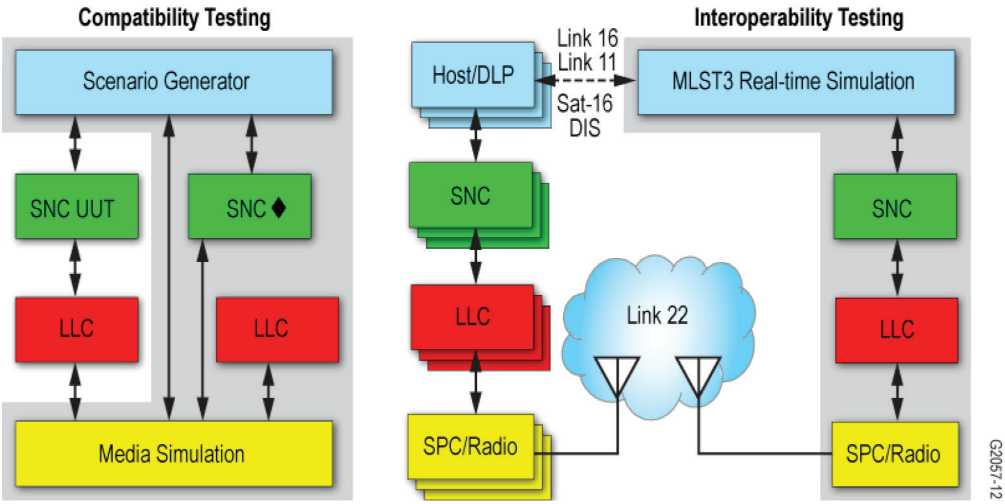


Figure 4-10. Link 22 Test Facilities.

The compatibility test system is called the NRS, which was developed to test the SNC and ensure that all modifications to the SNC meet and continue to meet the Link 22 requirements. It can also be used to test the other components of the Link 22 system, such as the LLC and SPCs/Radios.

The interoperability test system is called the MLST3. This was an existing system that was extended to incorporate the Link 22 Data Link Processor (DLP) simulation/ functionality providing a tactical interface as defined in STANAG 5522. This also required the implementation of the DLP-SNC interface. MLST3 has multiple configurations available for testing; most test configurations require the approved use of SNC and NRS components, the distribution of which is managed by the NILE PMO.

Section C

Features

This section covers the following Link 22 main features:

- System Architecture
- Secure Communications
- Tactical Message Transmission
- Quality of Service
- Fundamental Parameters
- Media
- Network Cycle Structure
- Initialization
- Network Management
- Joining a Network
- Resilience
- Congestion Management

System Architecture

The design of Link 22 uses a layered communications stack approach to produce an open-system architecture, with well-defined interfaces between the subcomponents. The approach maximizes extensions and enables contributions from multiple providers.

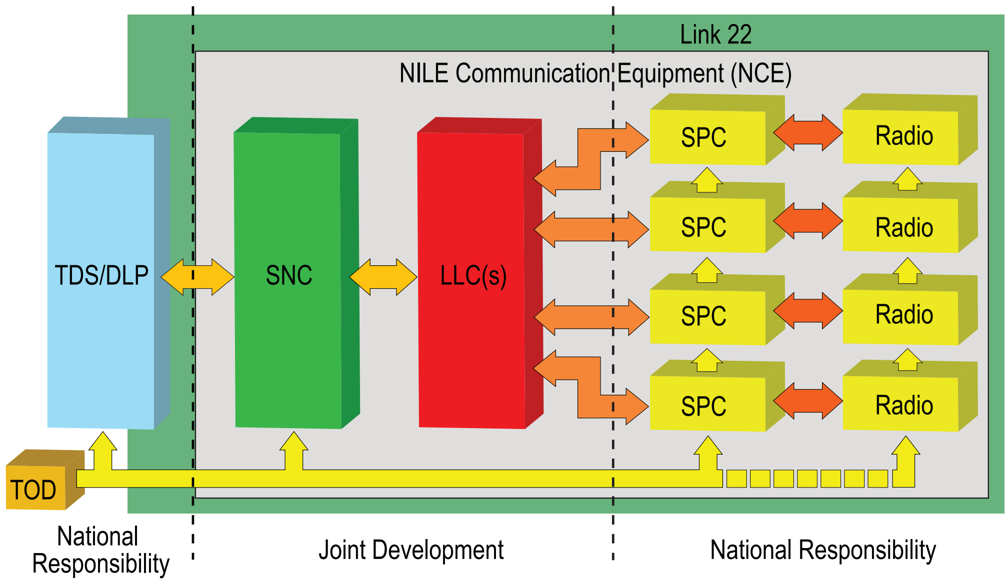


Figure 4-11. Link 22 System Architecture.

The inner grey box in the figure indicates the **NILE Communications Equipment (NCE)** components. These components are the following:

- System Network Controller (SNC)
- Link-Level COMSEC (LLC)
- Signal Processing Controllers (SPCs)
- Radios

The Link 22 system, shown by the outer green box in the figure, consists of the NCE and the Link 22 portion of the DLP. Within the DLP, this consists of the interface to the SNC and the handling of the tactical messages that it transmits and receives on the data link. The tactical messages are defined in the **NATO STANdardization AGreement** [STANAG 5522]. The DLP is connected to, or is part of, the Tactical Data System (TDS), also known as Host System of the NILE unit, which processes the received tactical messages and generates tactical messages for transmission in accordance with the unit's national requirements.

All NILE system components have been jointly defined and designed. The SNC and LLC subsystems have been commonly developed. The development of all other Link 22 subsystems is a national or manufacturer's responsibility.

Secure Communications

The LLC provides the system COMSEC. Its current configuration is a 19-inch rack-mounted hardware unit, as shown in the picture.

The LLC uses a weekly key to encrypt and decrypt the data traffic that passes through it. Two sets of keys can be loaded into the device, enabling it to operate up to 14 days without any operator intervention. The next week's key can be loaded at any time during the current week. Detailed information on the crypto key management is contained in the Crypto Key Management Plan document.

Transmission security is provided when frequency-hopping radios are used. The system is capable of using frequency hopping radios in both the HF and UHF bands.

Tactical Messages within Link 22 are handled as sealed envelopes and the system works without access to the tactical data contents. This provides the possibility to encrypt the tactical data at the top level and still be able to transmit it. This additional level of security cannot be provided by Link 16 as the terminal must retain access to the tactical data being transmitted.

Tactical Message Transmission

Link 22 transmits tactical data in fixed format messages, and uses the same data element definitions as Link 16. This provides standardization between the two tactical data links. Tactical messages are composed of from one to eight **Tactical Message Words (TMWs)**. Each TMW is 72 bits in length.

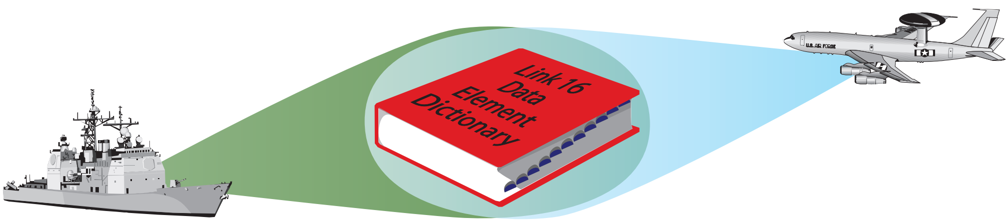


Figure 4-12. Link 22 Tactical Message Transmission.

Link 22 messages are called F-series messages and are part of the J-Family of messages. The F-series consists of two types of messages: the Unique F messages and the FJ messages. The Unique F-series messages are more compact versions of Link 16's messages, or messages that do not exist in Link 16. The FJ messages encapsulate Link 16 J-series messages within Link 22 messages, enabling Link 16 tactical messages to be transmitted without modification within Link 22.

The DLP requests transmission of a Link 22 tactical message with a **Transmission Service Request (TSR)**. Each request for transmission utilizes a unique identifier and defines the required QoS.

The DLP creates the Link 22 tactical messages from tactical data and the defined transmission requirements of [STANAG 5522]. Alternatively, the tactical messages may be created by the TDS and then passed to the DLP. The DLP, however, is the component responsible for passing all Link 22 tactical messages to be transmitted to the NCE. Likewise, the DLP is the destination for all tactical messages received by the NCE. The DLP may perform limited processing of the received tactical messages or may simply pass them on to the TDS for processing. Each message, as mentioned above, can be defined with different QoS.

The DLP performs other tactical functions, such as track management, correlation, reporting responsibility, conflict resolution, data filtering, and data forwarding [STANAG 5616 Volume II] and [STANAG 5616 Volume III]. These functions are a national responsibility, and they may be performed either by the DLP or the TDS. The DLP can perform minimal tactical message processing, or it can be a complete multilink Command and Control (C2) system.

Quality of Service

Link 22 provides a number of QoS features that are specified in the TSR. These features enable the efficient use of available resources. QoS features include the following:

- Priority
- Reliability
- Data Originator Identification
- Perishability
- Indicator Flags
- Addressing

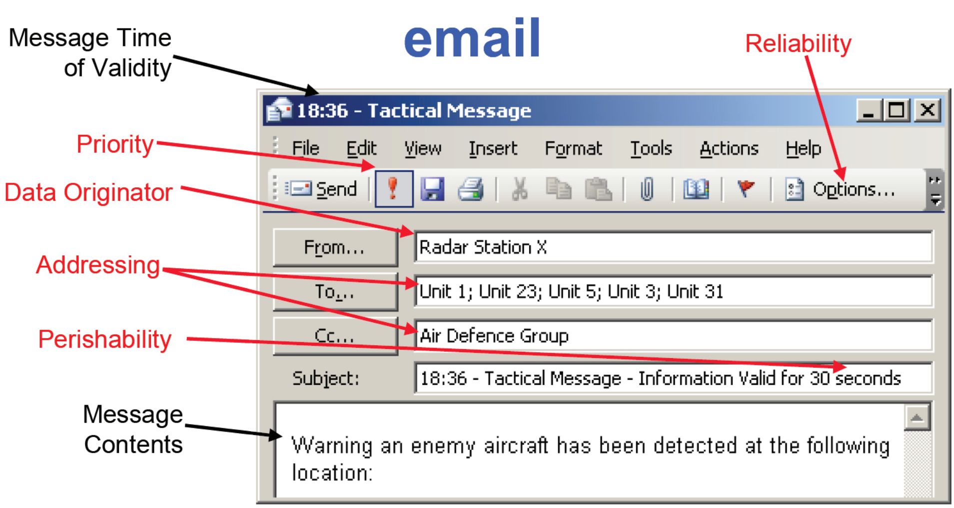


Figure 4-13. Link 22 Tactical Message QoS Features.

■ Priority

Link 22 provides four levels of priority (1-4), where Priority 1 is the highest and 4 is the lowest. Priority 1 requests can also utilize the Priority Injection (PI) Indicator Flag, which has the effect of increasing the priority by moving the request to the top of the Priority 1 queue and eligible for early additional transmission in a Priority Injection timeslot, if available. TSRs are considered during packing for transmission in a timeslot in highest priority, oldest TSR order.

■ Reliability

The required reliability of the destination unit receiving the message is included with each tactical message to be transmitted. Three levels of reliability are provided: **Standard Reliability** has an 80 percent probability of reception, **High Reliability** has a 90 percent probability of reception, and there is also a **Guaranteed Delivery** protocol. The probability of reception requested is used to calculate how many repeat transmissions are made. Reliability Protocols remove the need for redundant transmissions by the DLP. The Guaranteed Delivery protocol minimizes the repetition of transmission based on the acknowledgements received.

■ Data Originator Identification

The originator of the data to be transmitted is provided in the TSR. The Link 22 system ensures that this Data Originator Identification is delivered along with the data, so that any unit receiving it knows which unit originated the data regardless of its route through the system.

■ Perishability

Four levels of message perishability are provided by the system, and the TSR specifies which level applies to the data to be transmitted. Perishability allows the definition of how old the data can be before it is no longer relevant, and the Link 22 system ensures that data that has perished is not transmitted.

Indicator Flags

There are two indicator flags:

- The PI Indicator flag is used to enable Priority 1 messages to be injected in PI timeslots, which are timeslots that are not allocated to any specific unit
- The **Radio Silence Override Indicator** flag enables the message to be transmitted when the unit is in radio silence

Addressing

Two different Addressing services are provided, with and without Acknowledgement, which can usually be used at the same time. For both of these services, there are five types of addressing available:

- **Totalcast**: All Link 22 units
- **Neighborcast**: All radio frequency (RF) neighbors on each NILE Network on which the NILE unit operates
- **Mission Area Sub Network (MASN)**: A logical group of units that has been previously defined
- **Dynamic List**: A list of two to five units that are specified in the request
- **Point-to-Point**: A single unit that is specified in the request

Fundamental Parameters

Link 22 requires each unit to initialize with the same fundamental parameters as all other units. This is fundamental to the operation of the system. It significantly reduces the amount of configuration data to be distributed by the system. These fundamental parameters are supplied to each unit in the Operational Tasking (OPTASK) Link Message (OLM), which is provided to the TDS. The fundamental parameters must be supplied to the SNC by the DLP during SNC initialization. This data is maintained within the SNC and is referred to as the Super Network (SN) Directory.

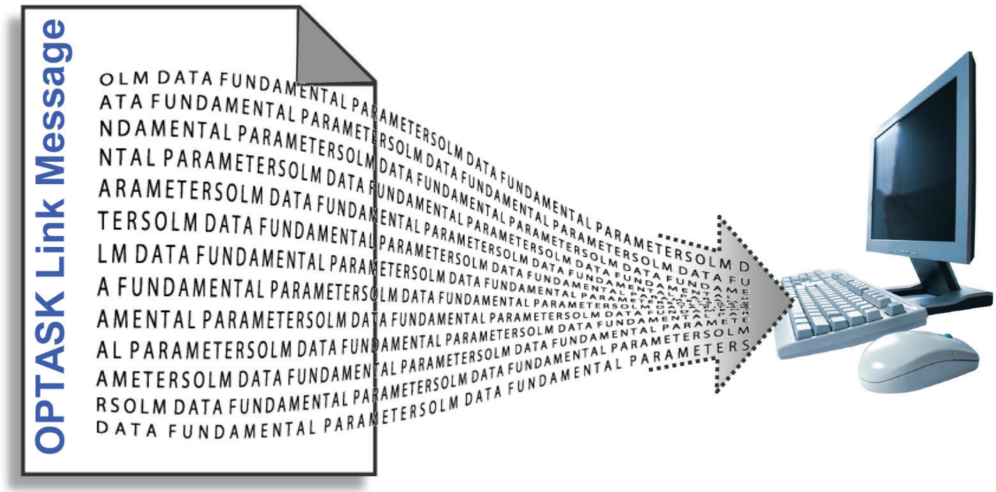


Figure 4-14. OPTASK Link Message Parameters for Link 22.

The generation of the OLM is performed by network planners, who take into account many pieces of information, such as the location of the operations, how many units are expected to participate, the expected tactical message throughput of each unit, and so on. The planners also consider which other tactical data links will be involved. They understand the complete communications infrastructure and define where and how Link 22 is to be used.

Media

Media using HF in the 2-30 MHz band provides BLOS communications, optimized for (but not limited to) transmission up to 300 nautical miles. Media using UHF in the 225-400 MHz band provides Line-of-Sight communications only. Within both bands, either fixed frequency or frequency hopping radios may be employed, for a total of four different media types:

- HF Fixed Frequency
- UHF Fixed Frequency
- HF Frequency Hopping
- UHF Frequency Hopping

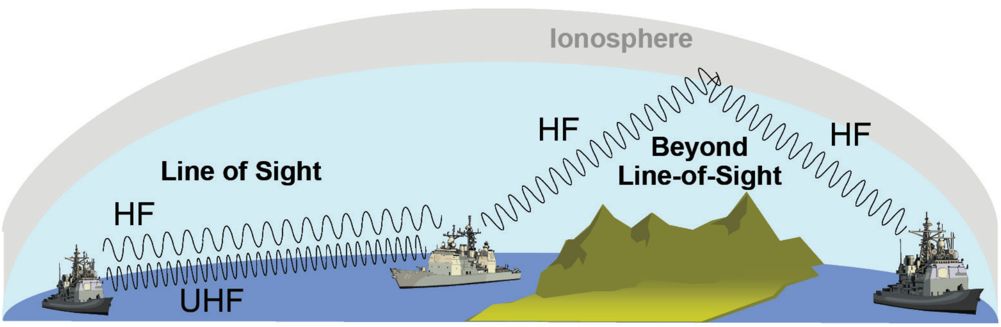


Figure 4-15. Link 22 Transmission Media.

Each media has one or more different settings, which use different modulation and encoding schemes. Along with the fragmentation rate, these factors determine the number of bits per network packet that are available for transmission, which ranges between 96 and 1824 bits, as can be seen in the following table. The duration of a UHF Frequency Hopping Media Coding Frame is a classified number, and is shown by the notation “<CN>” in the table.

Media Type	Media Coding Frame (ms)	Media Settings	Fragmentation Rate	Network Packet Size (bits)
HF Fixed Frequency	112.5	1-6	1-3	168 - 1368
UHF Fixed Frequency	48	1	1-3	608 - 1824
HF Frequency Hopping	112.5	1-4	1	96 - 240
UHF Frequency Hopping	<CN>	1-4	1	464

Figure 4-16. Link 22 Transmission Media Types.

Network Cycle Structure

The Network Cycle Structure (NCS) defines the TDMA protocol for each NILE Network. Time is divided into fixed length periods called minislots, the duration of which varies according to the media type. Periods of time called timeslots are an integer number of minislots, which may be of different size within specific limits. A timeslot is either allocated to a specific NILE unit, or is a Priority Injection timeslot. A unit may only transmit in its allocated timeslot(s), or for certain high-priority messages it may also transmit them in a PI timeslot. This ensures that each unit has an opportunity to transmit at least once within a given period of time, called the Network Cycle Time (NCT).

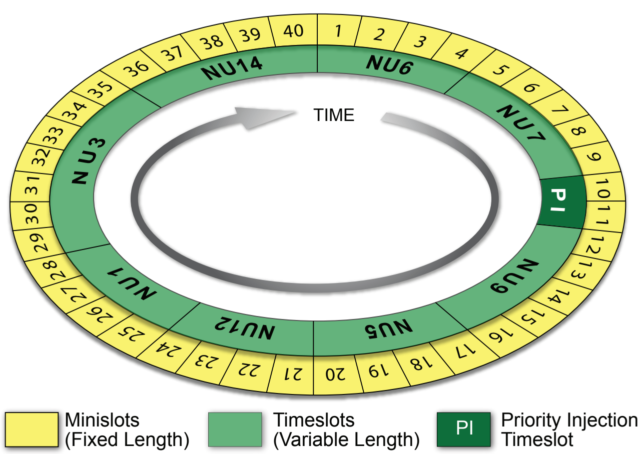


Figure 4-17. Network Cycle Structure for NILE Network.

The NCT is the number of minislots that form the network cycle (sum of the length of all timeslots). The NCT in the above figure is 40 minislots; however, this can vary up to a maximum of 1024.

When a network is operational the NCS is referred to as the Operational NCS (ONCS). Link 22 has the ability to modify the ONCS. This capability is called Dynamic TDMA (DTDMA). The SNC can also modify the ONCS by supplying a new one.

An NCS can be defined by the planners in the OLM. The planners take into account how many tactical messages per second a unit will need to transmit (Capacity Need), including relay traffic, and how long it can wait between transmissions (Access Delay). When the NCS is defined in the OLM, the DLP will initialize the network with the supplied NCS, which will then become the Operational NCS.

The SNC can also compute an NCS, in which case the Capacity Need and Access Delay of each unit in the network must be supplied. The SNC also uses two other parameters (Tolerance and Efficiency) in its computation, which enables the generation of an optimized NCS that does not meet all the input Capacity Need and Access Delay when it is physically impossible to do so.

Media types, media setting, and fragmentation rates all affect the size of timeslots in an NCS.

☐ *Initialization*

Every unit in the Link 22 Super Network uses the same Fundamental Link 22 Parameters to perform initialization. These parameters are specified in the OLM. This significantly reduces the volume of configuration data that needs to be distributed by the system. In fact, Link 22 can be initialized and can transmit tactical messages on a NILE Network at the instant the network is to start, with no prior communications on the network required.

Initialization consists of the following two parts:

- NILE Unit Initialization
- Network Initialization

The Link 22 unit's subsystems must be initialized first, before it can initialize any networks. Hardware configuration information must be supplied to the SNC by the DLP. The DLP also must supply the Fundamental Link 22 Parameters so that the SNC can initialize its internal data.

When SNC Initialization is complete, the DLP can begin to initialize the individual NILE Networks. The OLM can specify one of the two types of initialization; either quick initialization (known as Short Network Initialization) or an initialization that requires probing of the environmental condition before allowing for tactical traffic to be generated (known as Initialization with Probing). Short Network Initialization can use an NCS defined in the OLM or let the SNC calculate the NCS based on the Capacity Need and Access Delay parameters described above.

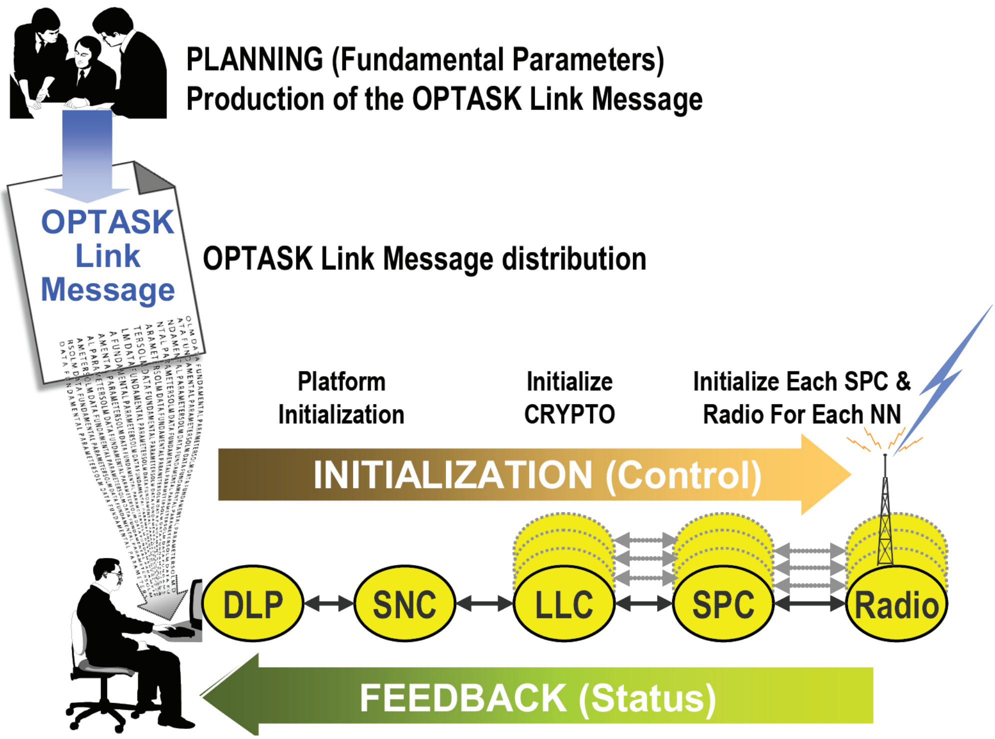


Figure 4-18. Link 22 Initialization.

If the unit has missed the start time for the network initialization, it should join the network by performing the LNE protocol. LNE provides the unit with the current parameters, which may have changed since the network was initialized.

Network Management

Link 22 was designed, using lessons learnt from Link 16 experience, to operate with automated and simple management. The result is that it is significantly easier to plan and operate than either Link 11 or Link 16.

Link 22 has automated Network Management functions that require a minimum of operator interaction, if any. These functions are controlled by the transmission of Network Management messages. Each unit can define whether or not to automatically respond to, and whether or not to automatically perform, each of the Network Management functions.

Link 22 specifies two network management roles. For each role, a standby unit automatically takes over the role, if the unit performing or assigned that role fails. The new management unit immediately nominates a new standby unit. The system will therefore continue operation without the presence of units originally nominated to perform these management roles, and will operate even if no units are performing the roles. After the Link 22 system has started, the Super Network Management Unit (SNMU) has overall management responsibility for the entire Super Network. The Network Management Units (NMUs) have management responsibility only for their particular NILE Network. The SNMU can order the NMUs to perform their network management functions. The SNMU can be the NMU for the networks that it is active on. A NMU may be the NMU of more than one network.

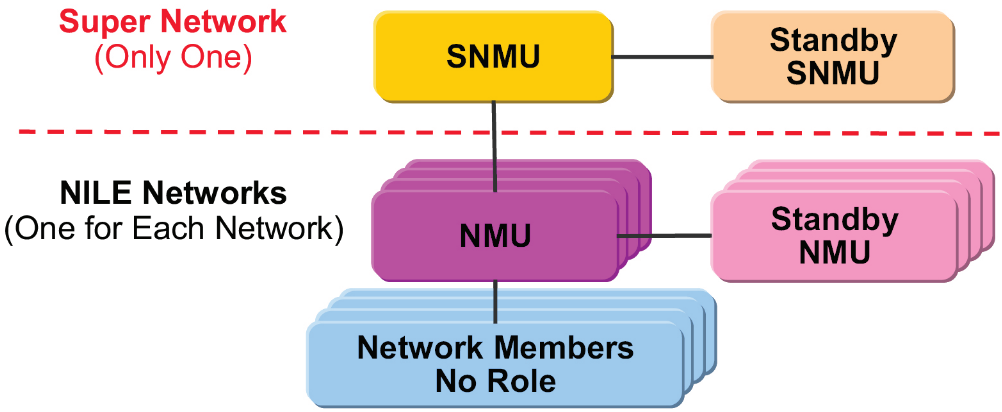


Figure 4-19. Link 22 Network Management.

The SNMU and, in some cases the NMU, can order certain management changes to the Link 22 system, including the following:

- Starting a new NILE Network
- Shutdown of a NILE Unit
- Shutdown of a NILE Network
- Shutdown of the entire Super Network
- Optimization of network performance
- Controlling Management Roles
- Joining a network
- Managing Radio Silence Status
- Managing Crypto Key Status

Other management functions do not require the use of an order, but do require transmission of a message to initiate the change:

- Managing Radio Power
- Managing the Super Network Directory
- Reporting monitoring data
- Reporting statistical data

Joining a Network

A unit that arrives after the Super Network has been started can still join by initiating the LNE protocol. This protocol provides the unit with the most current parameters necessary to join the network. The protocol is initiated by the operator and is usually fully automatic, with the protocol's progress available to the operator. A NILE unit may join a network in one of the following three ways:

- **Inactive Join**: the unit wants to join a network when it is not an active member of any NILE Network
- **Active Join**: the unit wants to join a network when it is already an active member of at least one other NILE Network
- **Silent Join**: a unit that is not an active member of any NILE Network and wants to listen to the network without making any transmissions

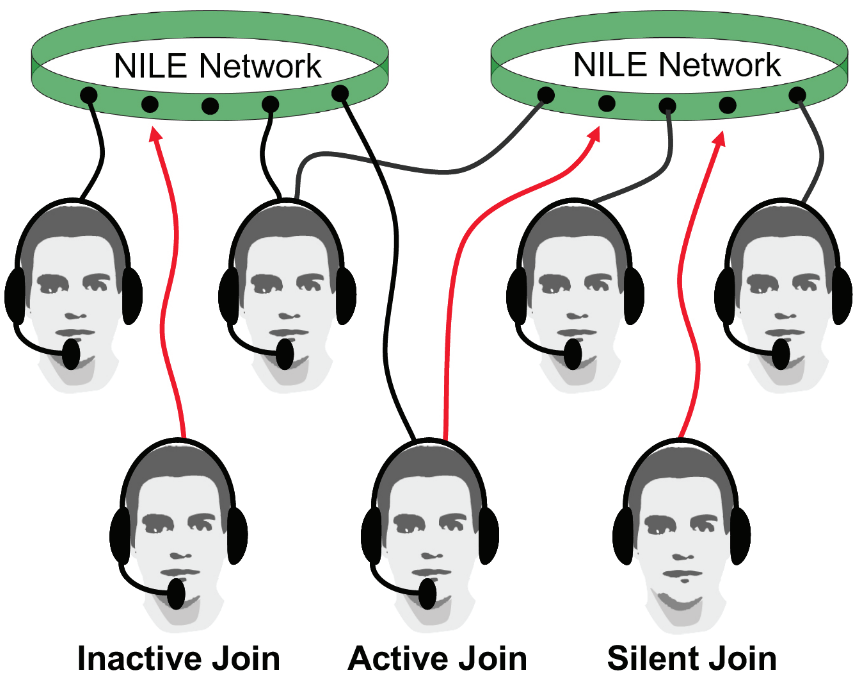


Figure 4-20. Methods to Join a NILE Network.

Resilience

The Link 22 system is designed to be resilient. If faults occur, it manages them and attempts to continue operating. A unit participating on multiple NILE Networks can have a failure on one network while continuing to operate on the other networks. A unit is able to handle the closure or shutdown of a network and the restart of the network after the hardware has been reset, without affecting the other networks.

When the connectivity changes, possibly due to the loss of a unit or the failure of equipment, the relay automatically takes this into account and modifies message routing in an attempt to maintain the probability that messages get to their addressees.

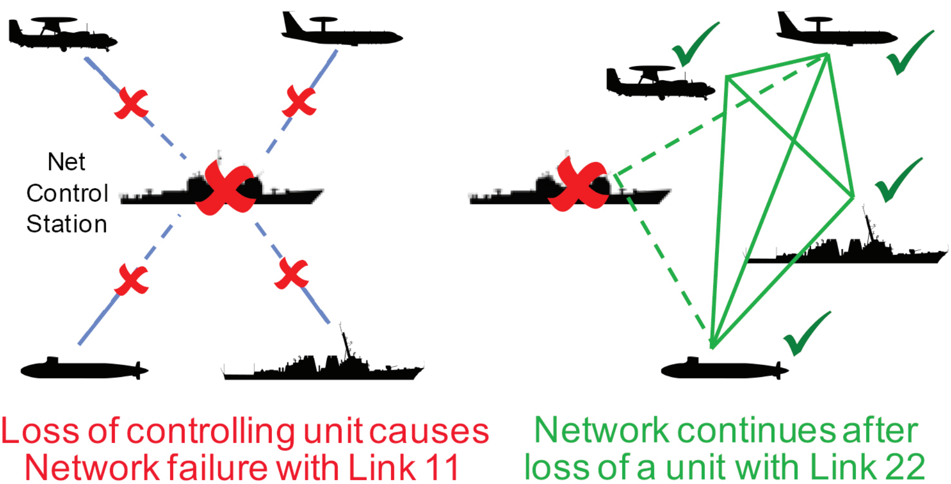


Figure 4-21. Comparison of Link 11 and Link 22 Resiliency.

Link 22 automatically retransmits messages to ensure that the requested quality of service (Reliability) is achieved whenever possible. This removes the need for the DLP to perform redundant transmissions and minimizes bandwidth utilization. Retransmissions are always placed in different packets on the network so that the loss of a single packet cannot cause the loss of all repeated transmissions.

The transmission on the NILE Networks is controlled by the TDMA structure, which is known to each unit, so the loss of any unit does not affect the ability of the remaining units to continue operation. Virtually all functions work in this manner (called distributed protocols), so there is no single point of failure.

Some units perform special roles, but the loss of these units is not disastrous to the operation of Link 22. Any unit that is performing one of the special roles must ensure that it always has a standby unit available to take over the role in case the unit is lost or its Link 22 system fails. A standby that takes over a role must ensure that a new standby is defined. Messages are exchanged between units, and the loss of reception from the role unit will cause its standby to activate the **Role Takeover** protocol. Similarly, if the role unit loses reception from its standby, it will give the standby role to another unit.

Troubleshooting at the unit, network, or Super Network level is enabled by the reporting of monitoring and statistical data. Each unit's SNC also validates all message data sent to it by the DLP before processing the message, and reports success or failure of each message back to the DLP. If the validation fails, the SNC also provides details of why the message failed validation.

☐ *Congestion Management*

Congestion Management is performed automatically in a number of ways. Message routing will use alternative paths to minimize congestion. When DTDMA is enabled, a unit that is not congested can donate spare transmission capacity to a congested unit. This affects the allocation of timeslots within the ONCS, but does not affect the NCT. All of this occurs automatically, with no operator or DLP actions required.

The NMU can change the ONCS to redistribute capacity. This function, called **Network Reconfiguration**, causes little or no network interruption. The NMU provides or causes the SNC to generate a new NCS, which can have a different NCT. On successful reconfiguration the NCS becomes the new ONCS.

Media parameters can be modified by the NMU in an attempt to increase the available capacity of the network. This requires the network to be temporarily paused and reinitialized with new parameters, which causes a minor interruption of network operations. This procedure is called **Network Re-Initialization**. The NMU can optionally provide or causes the SNC to generate a new NCS, which can have a different NCT. On successful Re-Initialization the NCS becomes the new ONCS.

Unit congestion arises from two sources: the messages the DLP requests to be transmitted, and the messages received from other units that must be relayed to ensure that the messages are received by their addressees. The DLP has full control over messages it has requested to be transmitted. The DLP could delete selected requests to reduce the congestion, and it could reduce the rate of transmission requests.

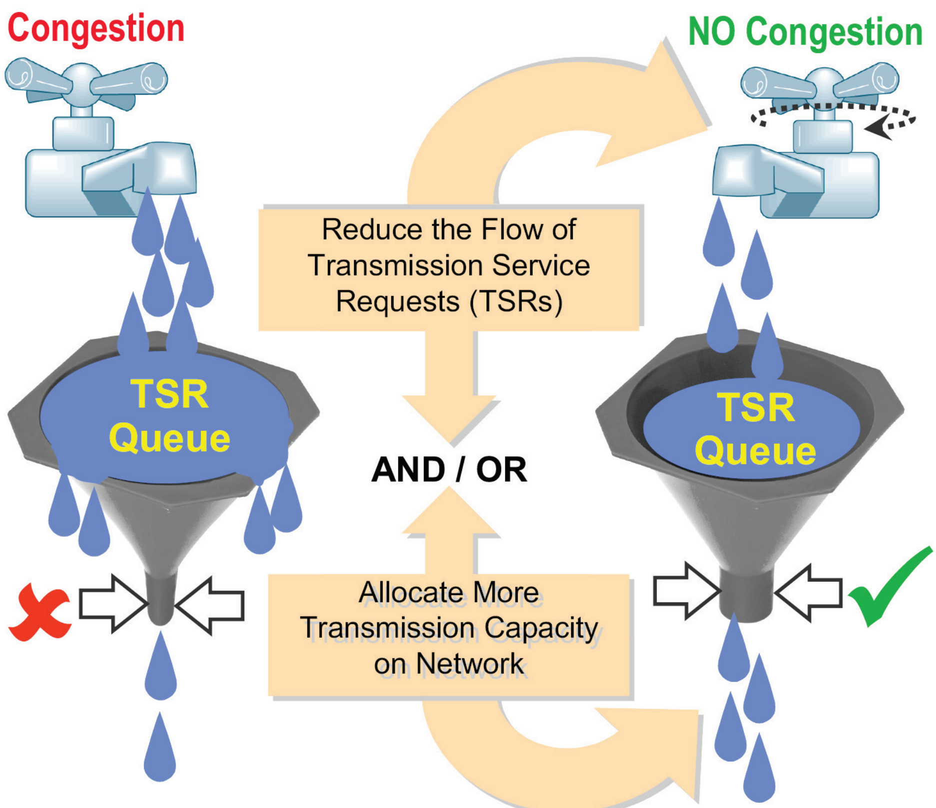


Figure 4-22. Link 22 Congestion Management.

Tactical messages that are being relayed are normally not under control of the DLP. In cases of high congestion, however, the DLP can be informed of the relay messages and decide whether it wants to delete any. This last resort reduces the congestion, but it also affects the delivery of messages. This decision process is called **Relay Flow Control**.

Section D

Benefits

Link 11 is an old tactical data link that does not offer the capabilities and performance required by today's operational community. Link 16 is a complex and robust tactical data link that attempts to meet current operational requirements but is still reasonably old technology. It does not offer recently derived operational concepts, requires extensive planning, and is difficult to manage.

Link 22 offers the latest technology and uses COTS products. It provides a simple-to-use, sophisticated suite of functions that require minimal operator interaction, and that enable it to be used as both an excellent stand-alone tactical data link or in a complementary role with Link 16. Link 22 significantly enhances NATO tactical data link capabilities and meets today's increasing need for successful interoperability within allied operations.

Figure 4-23. Historic Timeline of Tactical Data Links.

□ Comparison with Link 11

Link 11 has been in existence since the mid-1950s. It was conceived to support small numbers of units performing mainly an Anti-Air Warfare (AAW) role on a single network. In normal use (Roll Call) a Link 11 network is controlled by a Net Control Station, which polls each unit in turn to request a transmission. When each unit is polled, it transmits its data without prioritizing the data, so no unit can be polled until the current transmitting unit completes its transmissions. A unit cannot transmit until it is polled.

Link 22 was designed primarily as a maritime tactical data link for anti-surface and subsurface warfare, although, like Link 16, it supports all battle environments. A comparison of Link 11 to Link 22 follows.

Link 11	Link 22
Roll Call Transmission allocation. Increased net cycle times due to increasing numbers of Participating Units (PUs) and tracks. Large access delay	Uses TDMA, which provides deterministic access to the network. Prioritization of messages ensures most important are transmitted before less important
No way to transmit urgent information	The use of Priority Injection timeslots in the TDMA structure can be used to minimize the delay in the transmission of urgent information
Limited number of participants (62)	More units (125)
A restrictive “playing area” based on the ranges of individual platforms, and more importantly, on its method of reporting its position, and that of its tracks, based on its distance from a Data Link Reference Point (DLRP). These factors limit the use of Link 11 in extended areas of responsibility, and also prevent polar operations	Uses the Worldwide Geodetic System (WGS-84), same as Link 16, so no limitation. Each NILE unit can operate simultaneously on up to four networks; a Super Network can be composed of up to 8 networks. This flexibility greatly increases the playing area
All units have to be in RF connectivity with the Net Control Station, again limits the area of operation	The use of routing & relay protocols greatly increases the playing area, even when using line-of-sight UHF
Relatively easy to spoof because of weaknesses in the security of the system	More difficult to spoof, and any attempts to spoof are easier to detect, due to features such as time based encryption
Relatively easy to jam a single HF or UHF fixed frequency network	A single HF or UHF fixed frequency network can still be jammed, however with multiple networks it is more difficult to jam all at the same time. The use of frequency hopping media makes it significantly more difficult to jam
The encryption level is not sufficient for the processing power of modern computers	Uses same crypto chip as Link 16. Crypto technology is being updated to meet future requirements

Figure 4-24. Comparison of Link 11 and Link 22 Capabilities (continued on next page)

Link 11	Link 22
The loss of the Net Control Station will cause the network to collapse	Does not use a Net Control Station. Designed with no single point of failure
The accuracy of Link 11's M-series messages is inadequate for modern targeting	Data items are designed with improved ranges and granularity using same data dictionary as Link 16
Available waveforms limit communications under bad RF conditions (as occur in polar regions)	A variety of more robust waveforms. In bad conditions strong coding can be used to maintain communication at the expense of throughput
M-series messages difficult to translate making data forwarding between links complex	Link 22 is part of the J-series family of messages, uses the same data dictionary as Link 16 and so makes translation and forwarding relatively easy compared to Link 11
Limited Bandwidth (1,800 bps for fast and 1,090 bps for slow)	Range of bandwidths available depending on coding and media for example fixed frequency: HF 1,493 – 4,053 bps UHF 12,666 bps

Figure 4-24. Comparison of Link 11 and Link 22 Capabilities.

☐ Comparison with Link 16

The more modern and complex Link 16 is primarily an AAW tactical data link, although it supports all Environment types. Link 22 is primarily a maritime tactical data link and has been designed to complement Link 16 operation.

Link 16 supports a single network with a large number of units spread across multiple frequencies (stacked nets). The stacked nets can be organized by unit types and tasks. There are peacetime restrictions on the use of certain frequencies.

Link 16	Link 22
UHF is LOS only. Link 16 units require airborne relay support to increase the range of network connectivity. Airborne relays are not required, however, for satellite Link 16	Provides BLOS communication with both HF and HF/UHF automatic relay that is not dependent on airborne relay units being available. It remains operable when an airborne relay is not available

Figure 4-25. Comparison of Link 16 and Link 22 Capabilities (continued on next page)

Link 16	Link 22
UHF fast frequency hopping counters the effects of jamming, making it extremely difficult to jam	A single HF or UHF fixed frequency network can be jammed, however with multiple networks it is more difficult to jam all at the same time. The use of frequency hopping media makes it significantly more difficult to jam
Network Management is very complex to plan and operate	Network Management is highly automated, relatively simple and includes features such as dynamic bandwidth allocation
J-series family message standard	J-series family message standard
15-bit Participant address numbering	Same as Link 16
19-bit track numbering	Same as Link 16
Worldwide Geodetic System (WGS-84)	Same as Link 16
Data transfer rate is between 26,880 and 107,520 bits per second, depending on the data packing structure	UHF fixed frequency data transfer rate is 12,666 bits per second. Link 22 can have multiple networks that can increase the bandwidth

Figure 4-25. Comparison of Link 16 and Link 22 Capabilities.

☐ Data Transfer Rate Comparison

The raw (maximum) data rates (Bits per Second (bps)), shown in the figures are what is available for Tactical Data transmission, after the low-level overheads (Error Detection and Correction (EDAC) bits, synchronization bits, etc.) have been taken into consideration.

Link 11 HF/UHF	Link 16 Joint Tactical Information Distribution System (JTIDS)	Link 22 HF (fixed frequency)	Link 22 UHF (fixed frequency)
1090 or 1800	26,880-107,520	1,493 – 4,053	12,666

Figure 4-26. Comparison of Link 11, Link 16, and Link 22 Data Transfer Rates.

Link 22, unlike Link 11, can perform simultaneous different transmission on up to four networks, which increases bandwidth. Two typical configurations are shown *Figure 4-27*.

3 HF and 1 UHF (fixed frequency)	2 HF and 2 UHF (fixed frequency)
24,825	33,438

Figure 4-27. Typical Link 22 Network Configuration.

Link 22 complements Link 16 by providing additional bandwidth in other frequency ranges and in particular by providing the BLOS and automatic relay capabilities.

Section E

Acquisition

It can be seen from the Link 22 architecture that the following components need to be acquired to add the Link 22 capability to a platform:

- Operator Interface System (TDS/DLP)
- SNC Processor Hardware
- Link-Level COMSEC (LLC)
- Signal Processing Controller (SPC)
- Radio System
- Time of Day (TOD) Source Hardware
- Connecting Cables and Equipment
- Spares

Each listed item will be discussed further. Logistics spares also need to be acquired to provide an adequate level of cover in case of unit failure.

Operator Interface System (TDS/DLP)

The DLP is connected to, or is part of, the TDS of the NILE unit. The DLP processes the received tactical messages and generates tactical messages for transmission in accordance with the unit's national requirements.

If Link 22 is to be added to an existing operator interface or TDS, it may be possible to incorporate the Link 22 TDS/DLP functions within the existing system; otherwise, a new processor will be required to run the functions. However, if the existing system has spare link interfaces, it may be possible to connect Link 22 to the existing system using a spare link interface. In this case, a gateway system that converts from the existing link format to Link 22 would need to be purchased.

SNC Processor Hardware

The SNC software requires a computer processor to execute the code. This would usually be Personal Computer (PC) type hardware, either running Windows XP or Linux operating systems. The SNC software is written in Ada 95 and is easily portable to other platforms as long as there is an Ada 95 compliant compiler available on the platform. The computer does not require significant processor power and any available current technology processor is sufficient. As a guide, a 1 GHz processor with one gigabyte (GB) of memory is more than adequate. The processor needs to support at least one Ethernet connection (preferably 100 Mbps) but, depending on the configuration, two may be required. The processor requires some storage for the operating system, the SNC executable and the TOD interface software. Possible configurations include a VME backplane enclosure with power supply and a VME processor card, or a rack mountable industrial PC.

Link-Level COMSEC (LLC)

A single LLC can handle multiple networks depending on the type of media. The system can use a maximum of four LLCs, which would be one LLC per network, but this would be an unusual configuration. A typical system will only use a single LLC. If more than two UHF Networks are deployed, two LLCs are needed. Associated with the LLC and its key loading, a Data Terminal Device (DTD), which is used to load the keys into the LLC, would need to be acquired from the national crypto agency. Depending on the method of key distribution employed, a paper tape reader KOI-18 may also be required. It is possible to distribute encrypted keys as PC files, in which case a special serial cable would be required to load the file from a PC into the DTD.

The current LLC is a 19-inch rack mountable unit. The manufacturer refers to the LLC as the KIV-21/LLC.

Signal Processing Controller (SPC)

An SPC is required for each network/media that the unit is required to operate on. A single SPC may be configured to use different media. An SPC hardware unit may contain more than one SPC. At the time this book was written, there were three manufacturers of SPCs, which all supported HF and UHF Fixed Frequency media. Frequency hopping media is also supported either within a separate SPC or embedded within a frequency hopping radio. The fixed frequency HF and UHF SPCs were available in 19-inch rack-mountable chassis, with two of them containing VME cards that could be mounted in a suitably configured VME backplane.

Radio frequency and power control by the SPC is optional. Refer to the SPC manufacturers' specifications to determine the options that are available with the supported radios.

Radio System

The appropriate radio system is required for each of the media types that will be used, and consists of the following:

- Radio
- Power Amplifier and Power supply
- Antenna Tuning Unit
- Antenna
- Antenna mounting hardware and cabling infrastructure

The radio, power amplifier, and power supply may be a single unit depending on the output power required. The higher the output power the more likely that separate units will be needed.

One of the goals of the NILE program was to be able to reuse existing modern Link 11 radios and antennas equipment. If there any available this would reduces the equipment that must be acquired.

Time of Day (TOD) Source Hardware

Link 22 needs to be supplied with coordinated universal time (UTC); which, if not already available on the platform, must be acquired.

The TOD needs to be supplied to the DLP, SNC, SPCs, and frequency hopping Radios, if equipped. The recommended TOD input to the SPCs is the Extended Have Quick format as defined in [STANAG 4430].

The SNC is delivered with a separate application (Read TOD) that accepts a Brandywine Serial 485 and 1 Pulse per Second (PPS) input in compliance with [STANAG 4430]. The Read TOD can be customized to supply the SNC with the appropriate time as detailed in Section 3 of the NRS Interface Design Description (IDD). The TDS may also require an accurate time to guarantee synchronization among all the subsystems.

If a reliable source is not available, the Global Positioning System (GPS) TOD hardware required normally consists of the following:

- GPS Antenna and mounting hardware
- Cabling from the GPS antenna to the GPS receiver
- GPS receiver and time code generator
- Connecting cables to supply time code to the system
- Time code cards for the SNC and DLP computers

Connecting Cables and Equipment

The equipment needs to be housed in suitable enclosures appropriate to the environment in which the equipment is to be installed. Whether installed in single or multiple enclosures will depend on the site and the way that communications equipment is usually configured on that platform. Each set of equipment will require power and appropriate allowance for cooling.

The components of the Link 22 architecture have to be inter-connected via appropriate cabling and communications devices.

The DLP-to-SNC interface and the SNC-to-LLC interface both use Transmission Control Protocol / Internet Protocol (TCP/IP). If TCP/IP is communicating within a processor, no cabling is required for the interface, which would be the case if the DLP and SNC were running on the same processor. When on separate equipment or processors, TCP/IP can use many types of network interfaces. The LLC interface uses Ethernet and so the SNC-to-LLC interface has to be Ethernet. Two Ethernet ports can be joined together with a simple cross-over Ethernet cable (point-to-point), or joined together using an Ethernet hub or switch. The use of an Ethernet hub is recommended to allow for monitoring of the interface. If the SNC host processor only has one Ethernet port then a single hub could be used for both the DLP-to-SNC and the one or more SNC-to-LLC interfaces.

The LLC is connected to the SPC via RS-422 serial cable.

The SPC is connected to its radio via a media specific interface, and is a national responsibility. It could even be implemented with the SPC being housed within the radio. Refer to the SPC and radio manufacturers' manuals for exact details of the interface.

Spares

Logistics spares would also need to be acquired to provide an adequate level of cover in case of unit failure. The quantity and level of spares provided is a national responsibility and may vary depending on the platform, location and the number of operational units.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Introduction

The Variable Message Format (VMF) is a message standard (K-series messages) that uses communications protocols that are transmission media-independent.

Section A

Overview of VMF

Variable Message Format (VMF) is a message standard (K-series messages) that uses communications protocols that are transmission media-independent. VMF, one of the J-series family of Tactical Data Links (TDL), is designed to support diverse needs for volume and detail of information. Flexibility is achieved through the information variability of each bit-oriented message and by using message standards that are independent of the textual format of the message. Message elements are adjusted in length to suit the content of the particular message. This makes VMF well suited for communications bandwidth constrained situations, such as when employing Combat Net Radio (CNR) networks.

VMF is the primary TDL system used by US Army and US Marine Corps maneuver and fire support units. Naval surface fire elements use VMF, as well as rotary-wing attack platforms, providing a common capability for most fire support operations. VMF is also implemented by some Close Air Support (CAS) aircraft and ground support kits including: A-10, AC-130H/U, B-52, BAO Kit, F/A-18, F-35, PFED, Tactical Air Control Party-Close Air Support System (TACP-CASS), and TLDHS.

Although VMF is not limited to any particular mission, it has been employed extensively for Close Air Support (CAS) missions. For example, VMF is used for immediate CAS requests via the Tactical Air Direction (TAD) net by Froward Air Controller (FAC), FAC-Airborne (FAC-A), Joint Terminal Attach Controller (JTAC), Tactical Air Control Party (TACP), Air Support Operations Center (ASOC), Direct Air Support Center (DASC), and Support Arms Coordination Center (SACC) across the services. VMF facilitates integration with Advance Field Artillery Tactical Data System (AFATDS), which streamlines the request coordination process. VMF is compatible with multiple communications mediums; including line-of-sight (LOS) and beyond-line-of-sight (BLOS) systems. This provides flexibility for a wide range of operational scenarios. Normally, a request net is required for each division (or equivalent), but more or fewer nets may be needed depending on the anticipated number of requests for a given operation:

- **US Army:** VMF messages are used across all segments of the Army's *Tactical Internet* and on various point-to-point circuits. The term *Tactical Internet* is used to describe the integrated battlespace communications network that integrates commercial Internet technology with Army tactical communications systems. The network communications architecture employs commercial Internet technology (e.g., Internet Protocol (IP) routers) and the open standards protocols (e.g., Transmission Control Protocol (TCP)/IP). Commercial Off-the-Shelf (COTS) IP-based routers and Internet controllers provide the ability to send messages among segments of the tactical battlespace network.
- **US Marine Corps:** The Marine Corps uses VMF messages for Amphibious, Fire Support, CAS, land warfare situational awareness, command and control operations tactical data networks similar to the Army's *Tactical Internet*, and across point-to-point circuits.
- **US Navy:** The Navy uses VMF messages across point-to-point circuits in support of Operational Maneuvers From the Sea (OMFTS) which includes Naval Surface Fire Support (NSFS) and CAS missions.
- **US Air Force:** The Air Force TACP also uses VMF messages to exchange information with ground and air units.

Most VMF architectures exist on a single Service basis. The service appendices of CJCSM 6120.01, VMF Interoperating Procedures (IOP) Supplement to Joint Multi-Tactical Data Link Operating Procedures (JMTOP) provides details. It describes network elements of a VMF architecture and network design which are further detailed in Operational Tasking Data Links (OPTASK LINK) or Air Tasking Order (ATO) messages or Command and Information Systems (CIS) Annex of an Operations Plan or Order.

Section B

VMF Standards

In the case of VMF, Military Standards (MIL-STD) 6017C, 188-220D Change 1 and 2045-47001D Change 1 are the approved standards designed to achieve compatibility and interoperability between command, control and communications systems and equipment of United States and coalition military forces employed or intended to be employed in joint tactical operations.

Each VMF message is preceded by a message header which is defined in MIL-STD-2045-47001 and lower layer protocols defined in MIL-STD-188-220.

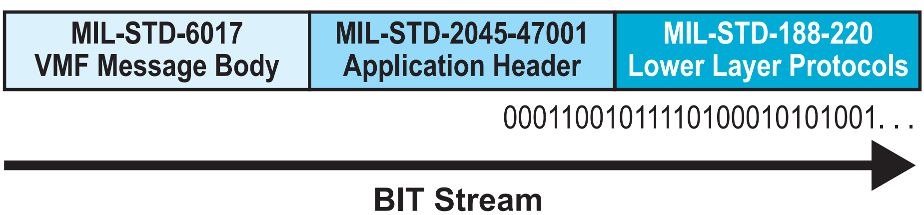


Figure 5-1. VMF and Protocol Data Flow.

☐ MIL-STD-6017

MIL-STD-6017 is issued by the US Joint Staff and presents the general information exchange requirements for VMF platforms. MIL-STD-6017 is used for the definition of VMF message formats, field codings, message coding conventions, and data (Data Field Identifier (DFI), Data Use Identifier (DUI), and Data Item (DI)).

■ VMF Message Formats

The VMF Message Description format contains the message number, title, purpose, index numbers, DFI/DUI numbers, data field names, field lengths, categories, groupings, recurrences, and an internal comments field called “Resolution, Coding, Etc.”. Message descriptions are provided for each VMF message defined by a valid combination of a Functional Area Designator (FAD) and Message Type Number as indicated in *Figure 5-2*.

Message Description						
Message Number: (Kn.m)						
Title: (Message Title)						
Purpose: (Message purpose will be written out)						
Index No.	Reference DFI/DUI DUI Name	# BITS	CAT	Group Code	Repeat Code	Resolution, Coding, Etc.
VMF fields are listed here.						

Figure 5-2. VMF General Message Description.

♦ Message Number

VMF messages are designated with an initial “K” and as such are known as the K-series messages. The numbering convention used for VMF messages is “Kx.y”, where “x” is the FAD and “y” is the message number assigned sequentially. As such, Kx.1 is the assigned to the first message of all currently defined messages within a functional area. For example, K05.1 is the numbering convention for the Land Combat Operations functional area Position Report message. As indicated in the figure below, VMF is designed to support all combat functional areas.

Message Designator	Warfare Functional Area
K00.Y	Network Control Messages
K01.Y	General Information Exchange Messages
K02.Y	Fire Support Operation Messages
K03.Y	Air Operations Messages
K04.Y	Intelligence Operations Messages
K05.Y	Land Combat Operations Messages

Figure 5-3. VMF Functional Warfare Areas.

♦ Index Numbers

Index Numbers provide a line number displaying the numerical position of each field within the message and their individual hierarchical position based on the syntax and repeatability criteria required by presence and recurrence indicators.

♦ DFI/DUIs

The DFI/DUI numbers identify data elements by DFI and DUI numbers. These numbers provide a quick reference to the Data Element Dictionary.

♦ DUI Name

The DUI name identifies uniquely the name of the DUI within the DFI concept.

♦ # Bits

The number of bits is the decimal number of the length of the DUI in binary digits.

♦ CAT

The category column is used to mark the field level minimum implementation for each field within the message. The markings are:

- **"M"** indicates a mandatory field. A field which must be present on each transmission and must be processed as received. Mandatory fields are marked with an "M". Mandatory fields are not discarded.
- **"X"** indicates a discretionary field. A field that need not be present upon each transmission of a message. All systems must be capable of transmitting and processing, as received, all "Discretionary" fields present in the messages they implement. Discretionary fields are marked with an "X". Discretionary fields are not discarded.
- **"#"** indicates an optional field. A field (or group) which need not be present upon each transmission of a message. Systems do not have to be capable of transmitting these fields (or groups) or processing them when they are received. Optional fields are marked with "#".

- There are no category column markings for Field Presence Indicator (FPIs) or Group Presence Indicator (GPIs) within groups, or those Field Recurrence Indicator (FRIs) or Group Recurrence Indicator (GRIs) that are preceded by FPI or GPI.

♦ Group Code

Groups are identified in the Group Code column. These groups will be identified GN where N indicates the numbered grouping (i.e., G1 indicates the first “G” group within the message; G2 indicates the second “G” within the message; etc.). G1/G2 indicates G2 is nested within G1.

♦ Repeat Code

The repeat code column identifies the fields or groups of fields that are repeatable. Repeatability of a, or group of fields is indicated with a “RN” in the repeat code column, where N indicates the sequential number for the repeated field/group (i.e., R1 indicates the first repeatable field or group within the message; R2 indicates the second repeatable field or group with the message; etc.). R1/R2 indicates R2 is nested within R1.

♦ Resolution, Coding, Etc.

The Resolution, Coding, Etc. column provides internal descriptive notes and titles for groups of fields as well as specifying the identity of field representations, such as Unit Reference Number (URN).

■ VMF Message Syntax

VMF message syntax provides a means of variability of the message length and is achieved through the use of four 1-bit syntax fields, the FPI, FRI, GPI, and GRI.

VMF Data Element Dictionary

The VMF Data Element Dictionary (DED) is located in MIL-STD-6017, Appendix B and contains the data elements in this media. Data elements are specifically identified through the use of two numbers, the DFI and its DUI. The DFI presents a single concept and is the generic representation of the DUIs grouped under it. The associated DUIs reflect the DFI concept topically and contain the DIs used to compose the data element.

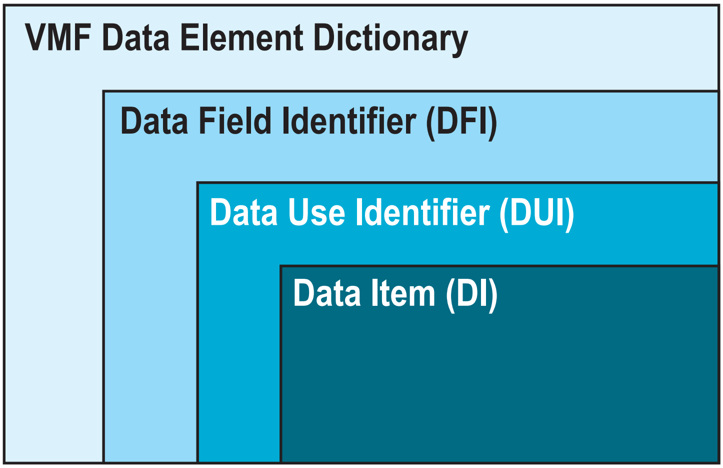


Figure 5-4. VMF Data Element Dictionary.

VMF Message Processing

Most VMF operations are carried out using Single Channel Ground-to-Air Radio System (SINCGARS), single-frequency Ultra High Frequency/Very High Frequency (UHF/VHF), or HAVEQUICK media using MIL-STD-188-220 CNR protocols. Recently SATURN protocol has begun to be fielded; however it is not part of MIL-STD-188-220 CNR protocols. VMF message processing may include cases for each use of a multi-purpose message and provides inter-element conditionalities within the message for basic processing. Message processing rules also include specific conditions, defaults, service restrictions, expected responses, special considerations and case level minimum implementation.

Joint VMF Message Minimum Implementation

MIL-STD-6017 mandates any system implementing VMF must at least achieve the Joint message level minimum implementation as specified in *Figure 5-5* below. These messages must be implemented as both transmit and receive.

Message Number	Message Title	Message Purpose
K01.1	Free Text	To provide information that does not fall into a structured format.
K01.2	Unit Reference Query/ Response	To request or distribute the data associated with a unit reference number.
K05.1	Position Report	To provide friendly unit location data.

Figure 5-5. VMF Joint Message Level Minimum Implementation.

Close Air Support Message Level Minimum Implementation

The Joint CAS community has defined in MIL-STD-6017 the only sub-functional warfare area message level minimum implementation. *Figure 5-6* is the list of CAS message level minimum implementation messages.

Message Number	Message Title	Message Purpose
K02.27	Close Air Support Request	To request immediate or preplanned close air support.
K02.28	Close Air Support Mission Battle Damage Assessment (CASBDA) Report	To report battle damage assessment after the completion of a CAS mission.
K02.31	Mission Request Rejection	To inform a requestor that a planned or immediate CAS mission(s) request is rejected.
K02.32	Close Air Support Request Acceptance	To inform command and control agencies that a close air support mission request has been accepted for a planned or immediate mission.
K02.33	Close Air Support Aircrew Briefing	To provide aircrews all essential information for a close air support mission.
K02.34	Aircraft On-Station	For the pilot or flight leader to notify the control agency that he and his flight have arrived at the prescribed control station.

Figure 5-6. Joint Close Air Support Message Level *(continued on next page)*

Message Number	Message Title	Message Purpose
K02.35	Aircraft Depart Initial Point	For the pilot or flight leader to notify the control agency that he and his flight are departing the initial point to complete the assigned air support mission.
K02.57	Aircraft Attack Position and Target Designation	To provide aircraft location, target location and aircraft system status to the FACs.
K02.58	CAS Aircraft Final Attack Control	To provide the ability to conduct final attack (terminal) control and the CAS Aircraft to respond to an abort code mismatch.
K02.59	Request for K02.57 Aircraft Attack Position and Target Designation	To provide the FAC with means to schedule, start, and stop CAS aircraft attack position and target designation reporting message.

Figure 5-6. Joint Close Air Support Message Level Minimum Implementation.

☐ *Upper-Lower Layers and VMF Message Structure Overview*

The transfer of VMF messages will pass through several layers before the actual VMF message can be decoded. The layers that the system will encounter are summarized in *Figure 5-7*. The lowest layer (shown as modulation and Physical Layer in the figure) represents the actual radio like SINCGARS or TACP-CASS.

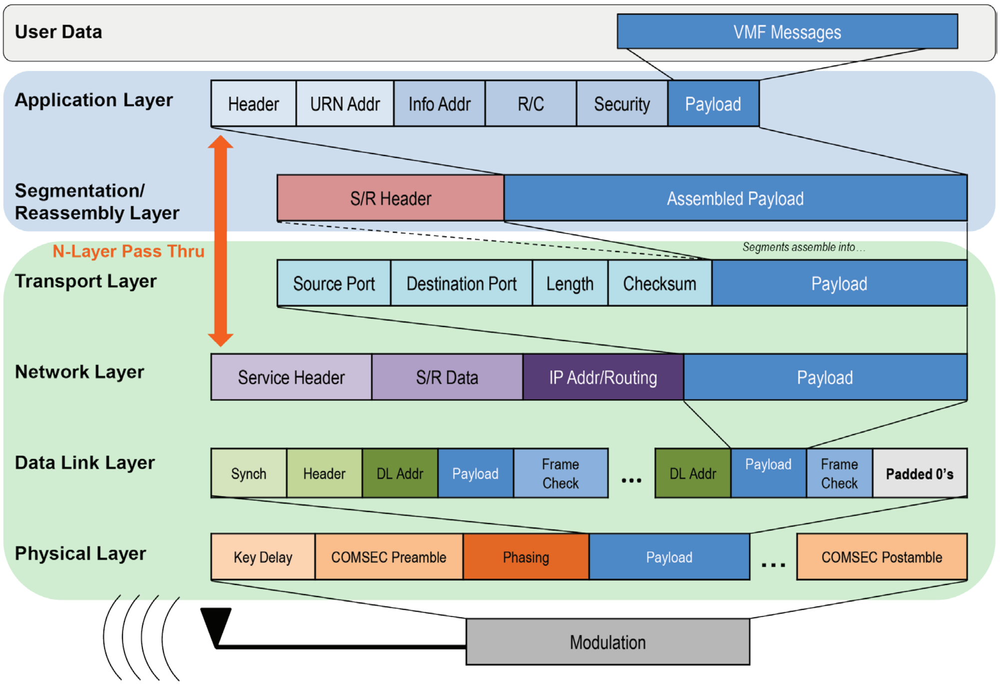


Figure 5-7. Layers of a VMF Transfer.

■ MIL-STD-2045-47001

MIL-STD-2045-47001 presents the minimum essential technical parameters in the form of a mandatory system standard and optional design objectives for interoperability and compatibility among VMF participating units using digital data for information transfer over limited bandwidth communication channels. The header is an essential part of the transmission because it contains message identity, addressing data, receipt/compliance information (Can Comply (CANCO), Will Comply (WILCO), and Cannot Comply (CANTCO) responses), date-time and perishability, security classification and message handling information.

The header identifies "User Data" that is concatenated, these User Data formats may include: Link 16 (J-series Messages), Binary files, VMF messages, National Imagery Transmission Format System (NITFS) files, Redistributed Messages (RDM), United

States Message Text Formats (USMTF), Extensible Markup Language (XML) - Message Text Format (MTF), and Extensible Markup Language (XML) – Variable Message Format (VMF). For our discussion we will consider VMF has been selected.

When a system receives a Header/Message data block it will take the data block and process it into one or more VMF messages marked with source information (who sent it, when, what priority, what response is needed) and will initiate machine receipt or Cannot Process (CANTPRO) responses.

■ MIL-STD-188-220

MIL-STD-188-220 provides the technical parameters for the data communications protocols that support VMF interoperability. It provides mandatory system standards for planning, engineering, procuring, and using VMF in tactical digital communications systems. This standard specifies the lower layer (Physical through Intranet) transport protocols for interoperability of Command, Control, Communications, Computers Intelligence (C4I) systems. It defines the layered protocols for the transmission of single or multiple segmented messages over broadcast radio subnetworks and point-to-point links. It provides minimum essential data communications parameters and protocol stack required to communicate with other data terminal devices. The standard supports SINCGARS (VHF), single frequency UHF/VHF/High Frequency (HF), and HAVEQUICK operations.

VMF systems operate like an Ethernet, using open system architecture based on the commercial Open Systems Interconnection (OSI) 7-Layer Model. In essence, the system is composed of a network of many low-level local area networks connected via routers to larger wide-area networks. Most of the system is line-of-sight and low bandwidth. MIL-STD-188-220 defines numerous options for providing exactly what is required for any specific scenario, although this can constrain interoperability. For VMF systems, network planning is of paramount importance, and it is essential that all of the many options are disseminated to all potential participants in a timely manner before operations begin. MIL-STD-188-220 lower layer protocols are depicted in the highlighted portion of *Figure 5-8*.

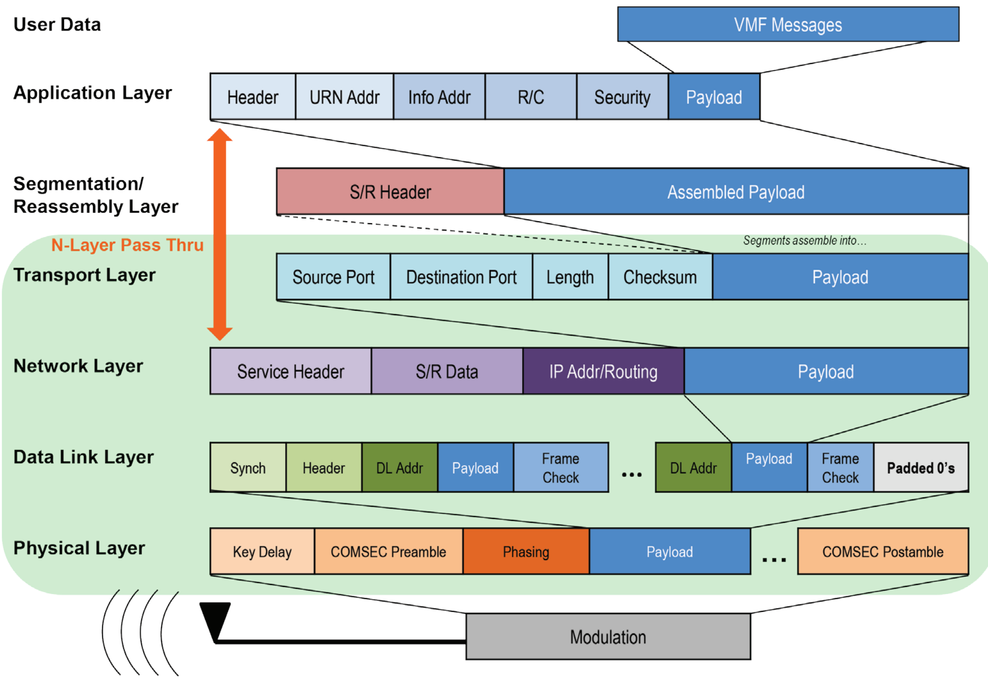


Figure 5-8. MIL-STD-188-220 Protocol Layers.

♦ Physical Layer Protocol

The Physical Layer (PL) provides the control functions required to activate, maintain, and deactivate the connections between communications systems. MIL-STD-188-220 does not address the electrical or mechanical functions normally associated with PL protocols.

■ Robust Protocol

The Robust Communications Protocol (RCP) is an optional physical layer protocol for Digital Message Transfer Devices (DMTD) and interfacing C4I systems (Data Terminal Equipment (DTE)) and applies only to HAVEQUICK II compatible systems that require interoperability with radios that do not have data buffering or synchronization capability. RCP provides the additional processing necessary to aid the transfer of secure and non-secure digital data when concatenated with the link processing of the MIL-STD-188-220 protocol. The additional processing of this protocol allows for a higher level accuracy with an error correcting capability equal to rate 1/2 Golay to transfer a burst of data containing up to 67,200 data symbols with better than 90% probability of success in a single transmission, this being over an active HAVEQUICK II compatible link with a random bit error rate of 0.1 or less. The second goal of this physical protocol is for the required performance to be achieved entirely in software using current systems with modest processing capability.

■ Exchange Network Parameters (XNP)

XNP is optional and represents an additional capability of a CNR protocol stack. When used, XNP reduces the network management burden by providing a mechanism whereby MIL-STD-188-220 XNP messages are transacted to automate address and timing parameter assignment to all stations on the network. Except for XNP configuration and status, these message transactions are largely transparent to mission software applications and/or operators.

Combat Network Radio Working Group (CNRWG) Interface Change Proposal (ICP) PD10-002R2 replaced the previous version with XNP Version 2 of MIL-STD-188-220. XNP Version 2 corrects several errors and adds numerous improvements easing the burden of Close Air Support operators and was granted a Request For Exemption (RFE) to implement in advance of this change being entered into MIL-STD-188-220E (not published yet). The protocol specified in PD10-002R2 is XNP Version 2 supersedes the previous version and the two are not interoperable. Inasmuch as there are differences, XNP Version 2, fundamentally, performs the same functions that XNP Version 1 was intended to provide.

It should be noted that the US Joint Staff Digitally Aided Close Air Support (DACAS) Block I implementation includes XNP Version 2.

♦ Data Link Layer

The Data Link layer provides the control functions to ensure the transfer of information over established physical paths, to provide framing requirements for data, and to provide for error control. Zero bit insertion is applied to the Transmission Header and Data Link Frame.

♦ Intranet Layer

The Intranet Layer (IL), routes data packets between a source and possibly multiple destinations within the same broadcast network. The IL also accommodates the exchange of topology and connectivity information packets to support Intranet relaying path discovery. To maintain a high speed of service for small high precedence messages, the IL will break a larger IL-Unitdata Request into multiple smaller IL Data Packet fragments prior to transmission via the data link layer. The destination IL transparently reassembles the IL Protocol Data Unit (PDU) fragments received via the data link layer to recreate the original data prior to generating an IL-Unitdata Indication.

♦ Transport Layer

The Transport Layer is not defined in any military standard. TCP or User Datagram Protocol (UDP) may be selected; however the use of TCP is discouraged when used with MIL-STD-188-220 protocols.

When N-Layer Pass Through is used the Transport Layer becomes a null layer.

♦ Lower Layer Protocol Network Settings

MIL-STD-188-220 requires a large number of parameters that makes it difficult to achieve interoperability between operational systems. Table XIV of MIL-STD-188-220D Change 1 provides a list of pre-defined set of lower layer protocol parameters is designed to reduce interoperability problems. The table is a listing of typical numbered low level Operational Parameter Sets (OPS).

Network managers may select predefined OPS and promulgate its OPS number to all intended users. Users may look up that OPS number and set the defined parameters in their system. A system option may be used to automate the process so that when the system is initialized with an OPS number, the parameters are automatically implemented. A new system wishing to join an established network can be provided with the OPS number for that network. This process reduces the probably of errors when given a long string of parameters. The use of the table is optional but strongly recommended.

Section C

Coordinated Implementation Required (CIR)

It should be noted that if systems engaged in VMF operations are not built to implement exactly the same military standard at the message, header, data link, and radio frequency levels there will be interoperability issues that have the potential to seriously impact mission accomplishment. This was acknowledged in CJCSM 6120.01D-3 when it stated, *"...fielded VMF systems are to be designed to the same set of standards at all times. VMF capabilities are therefore designed to have upgrades fielded at the same time similar to changing over crypto. This requirement is known as coordinated implementation required (CIR)…Any VMF capable system upgrading its fielded capabilities ahead of or behind other fielded systems; using software not programmed to the exact same standards; not upgrading with other fielded systems regardless of the reason, will result in non-interoperability."* Effort in coordinated implementation must be addresses to ensure the interoperability challenge for current and future versions of the involved standards.

☐ VMF-CNR Network Issues

The VMF Combat Net Radio network is still an evolving tactical data link. As new systems, platforms, capabilities and technologies are added, many of these are adopted in anticipation of immediate fielding. Multiple versions of the three VMF-related standards are implemented by different VMF platforms in various combinations. The resulting dissimilar VMF implementations are, in some cases, non-interoperable. For example, most of the following versions are currently in use in various combinations:

- MIL-STD-6017 has nine versions (TIDP-TE Reissues 2 – 6, MIL-STD-6017, MIL-STD-6017A - C)
- MIL-STD-2045-47001 has four versions (MIL-STD-2045-47001 B – D Change 1 (Version E is due out late 2014)) (Note: There was no MIL-STD-2045-47001A)
- MIL-STD-188-220 has four versions (MIL-STD-188-220 B – D Change 1 (Version E is due out late 2014)) (Note: There was no MIL-STD-188-220A)

- Additionally, the following factors impact the VMF interoperability dilemma:
- Newer versions of the standards are not always backward compatible with previous versions.
- The introduction of retroactive changes to previous versions incorporating changes to standards after release. For example, some implementers claim "B+" or "C-" , even though no such version was ever officially published.
- Too many options:
  - Not all of the fields in the messages or Application Header are mandatory.
  - Not all of the functionality of the Application Layer Protocol is mandatory.
  - Not all of the functionality of the Lower Layer protocols is mandatory; two systems can both implement MIL-STD-188-220, in full compliance with the standard and be non-interoperable.
- Existing messages have been modified:
  - New fields added or old ones moved around inside the message.
  - Interpretation of existing fields is changed.
  - Values added to existing fields.
  - Modifications to messages have not been made backward compatible.
- Legacy systems cannot interpret revised messages.

Section D

Summary

In conclusion, the VMF/CNR network is a common means of exchanging data among combat units at varied organizational levels made up of a bit-oriented digital information standard consisting of variable length messages as a means to transfer the data through the upper and lower protocol stack. The message payload has the ability of transferring data supporting any warfare functional area with varying requirements for volume and detail of information. Furthermore, VMF is not limited to any specific media or waveform it can operate over any digital-capable radio frequency (RF) broadcast or point-to-point system. To ensure maximum interoperability implementers should address CIR issues at all levels of the VMF/CNR data transfer.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

CHAPTER 6
The Enhanced Position Location Reporting System

Introduction

The Marine Corps developed the Position Location Reporting System (PLRS) during the Vietnam conflict to prevent fratricide amongst the troops. PLRS allowed troops to communicate data and share position locations on the battlefield. Improvements were made to the system by the Army as part of the Enhanced Position Location Reporting System (EPLRS). The Navy soon adopted the PLRS and EPLRS technologies on several amphibious ships.

Section A

Introduction to EPLRS

Overview

Military services use EPLRS as a technology system for communication, identification, position location, and navigation. This is possible through two key components, EPLRS Network Manager (ENM) and Radio Sets (RS). EPLRS is capable of communicating at High-Data-Rates (HDR), as well as real-time routing. An internal router in each RS allows routing that is contention-free, where a single RS can appear as up to 32 different radios. Network management is distributed by the ENM to the RSs, and contains information, such as system monitoring, network planning, and key management. The equipment that makes up an ENM includes an EPLRS radio and operator workstation.

Capabilities and Features

The following are capabilities and features of EPLRS:

- One ENM can host a network of many RSs
- The RSs use communication paths to exchange messages, known as "needlines"
- The network architecture uses Time Division Multiple Access (TDMA)
    - Timeslots are used within this architecture for RSs to transmit or receive messages
    - Time synchronization is achieved by every RS to ensure TDMA is successful
- EPLRS is a Communications Security (COMSEC) equipment that also has Over-The-Air-Rekeying (OTAR) capability
- The Ultra-High Frequency (UHF) operating frequencies are 420-450 MHz, and eight available channels are actually used by EPLRS

- Frequency hopping for transmission security is optional for each network
- Up to 57.6 Kbps data rates
- Interfaces include X.25, RS-232, and Ethernet
- Network capacity is increased and interference is minimized through Frequency Division Multiple Access (FDMA)
    - This allows a single RS to simultaneously communicate through multiple needlines
- Communications over a network can overcome geographic limitations and distances through relays
- RSs can automatically setup an alternative network route if a communication path fails
- Does not depend on Global Position System (GPS) location and position data

Section B

Terminals and Interfaces

There are two versions of the RS: a vehicle-mounted, high-power and a Micro-Light, low-power.

Figure 6-1. EPLRS Vehicle-Mounted Radio.

The RS communicates messages (e.g., position and location) via Ethernet, which is managed by the ENM. The ENM would provide the port number and Internet Protocol (IP) for each RS in the network. As for the messages, they follow the Joint Services Variable Message Format.

EPLRS Terminals

Position data is delivered from an EPLRS RS over an Ethernet link as multicast packets with the IP address and port number configurable via the ENM. It is distributed in Joint Services Variable Message Format (JVMF) using K05.01 and K05.19 message types. The following Interface Control Documents (ICD) can be used to decode the header and content of the Variable Message Format (VMF) messages:

- MIL-STD-2045-47001 for the header format
- MIL-STD-6017 for K05.01 and K05.19 message format (controlled document)

Section C

Network Communications

Each RS is can be configured to support multiple network communications. The following are three types of EPLRS networks, not including the ENM-to-RS communications. The purpose of the Acquisition Network is to synchronize RSs in a network upon initial entry. This is achieved through a time-sync by the RS. The purpose of the Coordination Network is to coordinate communication tasks, to include relay paths for needlines and IP resolution. The purpose of the Communication Network is to exchange messages after the network has been formed and communication paths have been established. The ENM communicates to the RS through their respective Simple Network Management Protocol (SNMP) agent.

☐ Needlines

Needlines are virtual circuits that form communications between RSs. They can be either broadcast or point-to-point. Multiple needlines can be supported by each RS, which increases the amount of data that can be exchanged over the network. The following are four types of needlines:

- **HDR Duplex** – is used for a high data transfer rate and reliable communications, as each RS must acknowledge the receipt of data sent by the other RS.
- **LDR Duplex** – is used for a low data transfer rate and reliable communications, as each RS must acknowledge the receipt of data sent by the other RS.
- **Carrier-Sense Multiple Access** (CSMA) – is used for large networks exchange Situational Awareness (SA) and Command and Control (C2) data.
- **Multi-Source Group** – is used for exchanging data at a low-latency and provided few-to-many communications.

Operational Support

EPLRS supports various operations to include combat operations, amphibious operations, and littoral warfare. Ground forces often use EPLRS as a backbone to military networks in theater. This utilizes EPLRS mainly as a data link, but position and location data can also be shared amongst the combat forces. Amphibious operations can be coordinated by shipboard and shore-based forces over an EPLRS network. In addition, EPLRS can add value to littoral warfare by providing Navaid support and communication between mission elements.

Section D

SADL Network

Introduction

The Situational Awareness Data Link (SADL) is much like the ground EPLRS, with slightly different firmware in the radio. With the turn of a switch, the radio can convert from SADL to EPLRS. More than 700 have been built for F-16s and A-10s.

SADL Communication Services

Air-to-Ground

Air Force F-16 and A-10 fighter aircraft are using the EPLRS SADL to connect into the Army's tactical Internet. With SADL, the aircraft "nets up with the ground community" for close air support missions, so they can look on the ground for friendly forces. EPLRS network information can still be recorded while the SADL radio is sharing air-to-air data.

Air-to-Air

Aircraft that are equipped with SADL radios use a MIL-STD-1553 cable to interface with the onboard avionics. This allows the pilot to share data between air and ground units; however, network control by an EPLRS unit is not needed for SADL air-to-air communications.

Gateway into Link 16

SADL provides a "gateway" to Link 16 networks, and runs in a different portion of the frequency spectrum than Link 16. The data received by a SADL gateway radio can be received from a Link 16 network and shared with a SADL network.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

CHAPTER 7 Introduction to the Joint Range Extension Application Protocol

Introduction

Joint Range Extension Application Protocol (JREAP) is an application protocol that enables the transmission of tactical data link messages over media that was not originally designed for Tactical Data Links (TDLs). Supported communication media are:

- Satellite communications – JREAP A
- Point-to-Point – JREAP B
- IP Networks – JREAP C

Section A

JREAP Overview

The Joint Range Extension Application Protocol is an application protocol, governed by MIL-STD-3011B, that enables tactical data to be transmitted over digital media and networks not originally designed for tactical data exchange. This capability permits the transmission of TDL messages over a variety of transmission methods, enhancing the ability for distributed Command and Control.

The JREAP standard was developed to reduce reliance on service unique protocols such as Satellite TADIL J (STJ), TDL J, Serial J, Super High Frequency Satellite Communictions (SHF SATCOM), and Socket J that provided the ability for units to share information beyond the line of sight capabilities of radio frequency (RF) based communication systems. As many of these service unique protocols used a variety of communication media, the JREAP protocol was develop with three different appendices. These appendices (JREAP-A, JREAP-B, and JREAP-C) further define how JREAP should be implemented to support the various transmission media already in place among the various services.

Traditionally, extending the range of tactical data links beyond the line of sight is accomplished by introducing relay or forwarding units into the theater of operations; however, this becomes cumbersome and expensive to maintain. JREAP provides a standardized application layer protocol that allows Tactical Data Link messages to be forwarded to units beyond the transmission ranges of Tactical Data Link radios. This allows tactical data exchange between units that can be used for increased situational awareness, planning, and decision making.

Section B

JREAP Message Structure

The JREAP protocol, defined in MIL-STD-3011B, is separated into two functional modes, Full Stack and Application. Full-Stack operations incorporate Message Group Headers and Transmission Block Headers. The Full Stack implementation of JREAP incorporates methods for ensuring accurate addressing, timing, and error detection and correction of transmitted messages. The Application mode relies on services provided on lower levels of the Open Systems Interconnection (OSI) to ensure proper network operations.

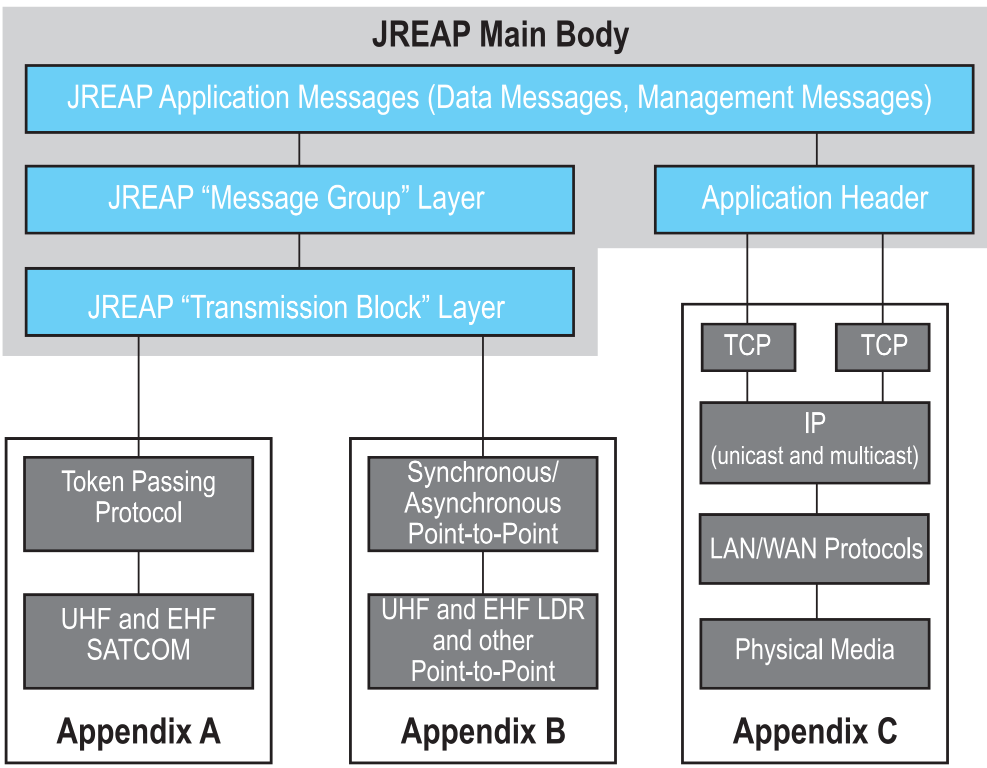


Figure 7-1. JREAP Message Structure.

JREAP-A

JREAP-A uses a token passing protocol over half-duplex communication channels to send and receive Tactical Data Link messages. JREAP-A implements the full-stack header and uses a token passing protocol, where one unit is allocated a particular period of time to transmit data while all other units listen and receive the data. JREAP-A is commonly used over 25kHz Ultra High Frequency (UHF) Demand Assigned Multiple Access (DAMA)/Time Division Multiple Access (TDMA), Extremely High Frequency (EHF) Low-Data Rate (LDR), and 5/25kHz UHF Non-DAMA SATCOM systems. These communication links are multi-participant satellite communication networks.

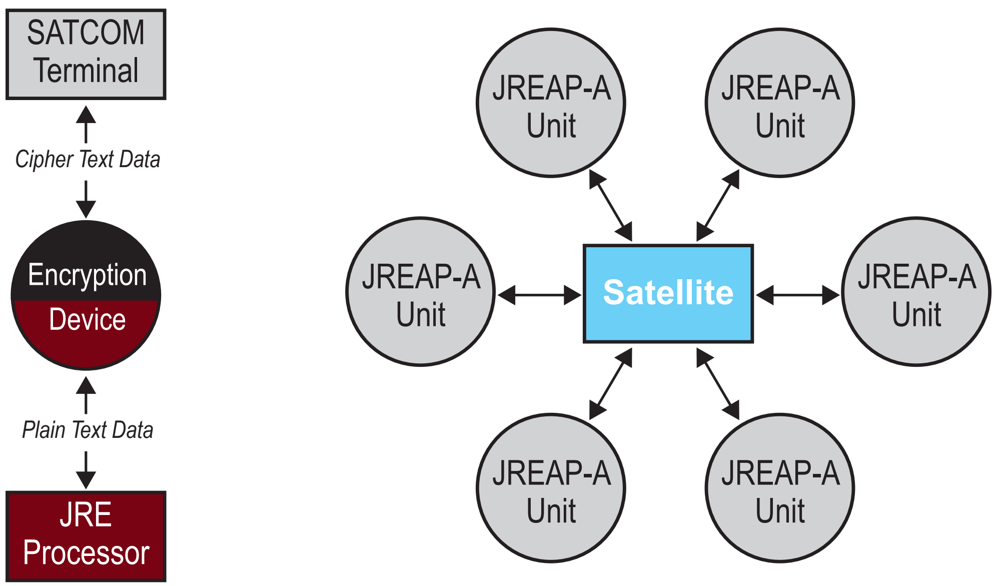


Figure 7-2. Sample JREAP-A Network.

JREAP-B

JREAP-B is used in synchronous or asynchronous point-to-point communications. JREAP-B is commonly used with full-duplex serial data communications carried by protocols such as TIA/EIA RS-232 and RS-422 and implements the full-stack header of the JREAP protocol. These communication networks can be local, or they can use long haul transmission media such as secure telephone circuits.

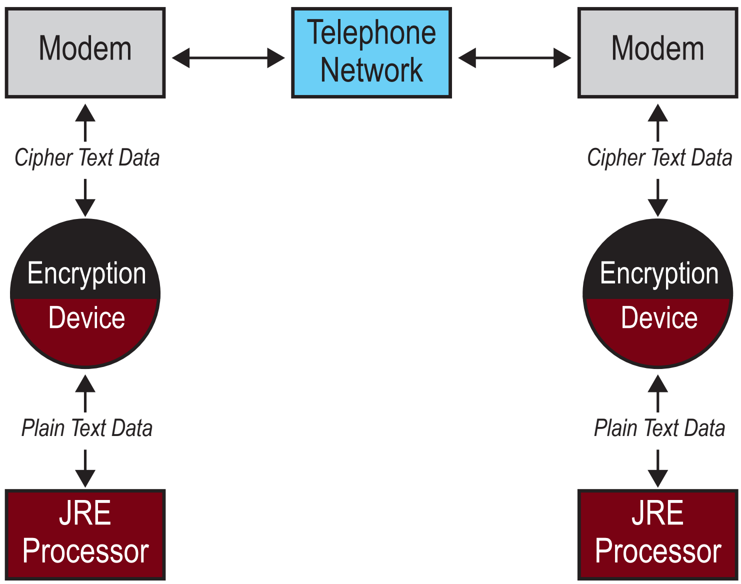


Figure 7-3. Sample JREAP-B Network.

JREAP-C

JREAP-C is an implementation of the JREAP protocol that transmits Tactical Data Link messages over Internet Protocol networks such as Secret Internet Protocol Router Network (SIPRNET). JREAP-C differs from JREAP-A and JREAP-B by implementing the application header instead of the full stack header. This is done because the error detection and correction, and addressing is not necessary as they are handled by the lower layers of the stack. This permits fast and reliable transmission of messages over a network.

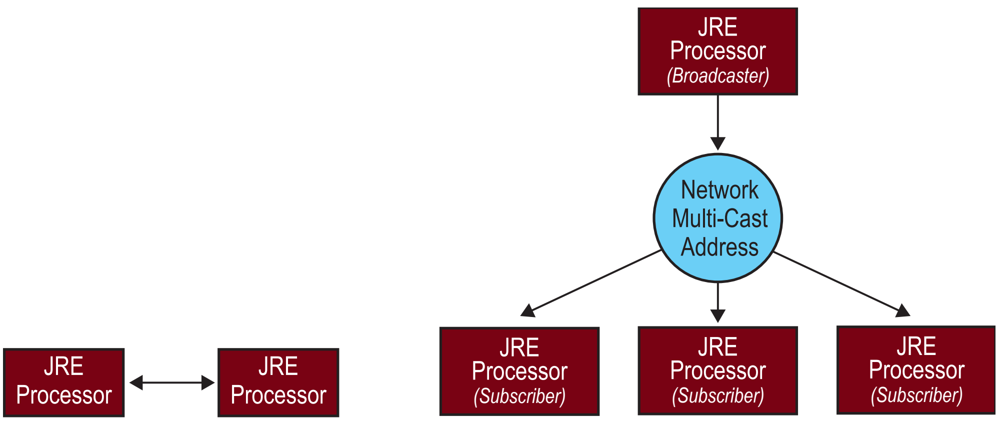


Figure 7-4. Sample JREAP-C Network.

JREAP-C defines two modes of operation, unicast and multicast. Unicast operations are used to send data link messages to a particular unit and operate as a one-to-one or peer-to-peer data link. Multicast operations are used to broadcast data link messages to a collection of users.

Section C

Transmission Media

☐ Serial Data Communications (RS-232)

RS-232 serial communications are common in JREAP-A and JREAP-B networks. The RS-232 standard defines how a computer's Data Terminal Equipment (DTE) communicates with a modem, data circuit-terminating equipment (DCE). RS-232 can operate in a synchronous or asynchronous mode of operation. Synchronous requires the DTE and DCE to share a common reference signal in order to determine the start and stop of each message that is transmitted. Asynchronous operations do not require a common synchronous clock signal. Understanding the RS-232 interface requirements between equipment is very important when developing a JREAP-A or JREAP-B network. Another important consideration is data security. JREAP-A and JREAP-B do not contain any means of data encryption. For secure JREAP-A and B operations, it is necessary to pass the messages through an encryption device before the data is passed to a modem.

☐ Internet Communications

JREAP-C operations require an available IP based network. These networks operate by connecting Local Area Networks (LANs) together to form a larger Wide Area Network (WAN). LANs are a collection of computers and networking devices that act together to ensure that data is reliably transferred from one computer to another. This is commonly accomplished using a combination of protocols, they include:

- Internet Protocol version 4 (IPv4)
- Transmission Control Protocol (TCP)
- Universal Datagram Protocol (UDP)

Internet communications rely on other networking equipment that must be properly configured per the individual operating requirements of each network:

- Hubs
- Switches
- Routers
- Firewalls

These devices are managed and maintained by networking professionals. Coordination with networking professionals in regards to the requirements for JREAP-C operations will ensure reliable and secure JREAP-C network communications.

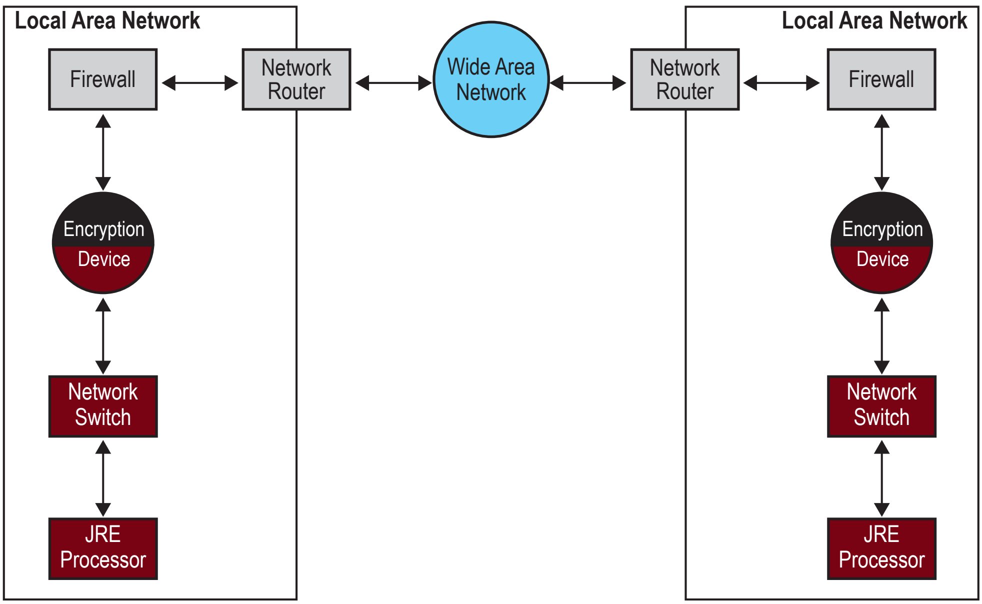


Figure 7-5. Sample JREAP-C Network (using WAN and LANs).

Internet Protocol Version 4 (IPv4)

Internet Protocol (IP) Address

An Internet Protocol v4 address is comprised of two parts. A host address, used to identify the individual computer, and a network address. Each of these components is 32-bits in length. IPv4 addresses are commonly expressed in dotted-decimal notation. Each computer on a network must have a unique address.

IP Address				
Binary	11000000	10101000	00000001	00000001
Dotted Decimal	192	168	1	1

Figure 7-6. IP Address Format.

Subnet Mask

The Subnet Mask is used in conjunction with an IP address to define a network address. This information is used by network devices to determine where information travels outside of the LAN. Bits in the subnet mask that are set to a logical high (1) represent the portion of the address that designate the network, and bits that are set to a logical low (0) represent the host. Computers on the same network segment will share the subnet mask.

	Dot-Decimal				Binary			
IP Address	192	168	1	1	11000000	10101000	00000001	00000001
Subnet Mask	255	255	255	0	11111111	11111111	11111111	00000000
Network Address	192	168	1	0	110000000	10101000	00000001	00000000
	n	n	n	h	nnnnnnnn	nnnnnnnn	nnnnnnnn	hhhhhhhh

Figure 7-7. Subnet Mask Format.

Transmission Control Protocol (TCP)

Transmission Control Protocol is a connection-oriented protocol that is used to ensure reliable and accurate transmission and reception of IP based network traffic through error correction and detection. TCP ensures that all message segments are received and re-assembled in the proper order, manages the retransmission of lost data packets, and manages network traffic congestion. Transmission Control Protocol is commonly used in network connections where the accuracy of the data outweighs its timely arrival.

Universal Datagram Protocol (UDP)

Universal Datagram Protocol is connection-less protocol that does not include many methods of error detection and correction. As UDP does not have the overhead of establishing a connection and lacks the error correction and detection of TCP, it is commonly used for sending network traffic where the speed of delivery is more important than accuracy. UDP is commonly used for video streaming and data that updates very quickly.

Hubs

Networking hubs are static devices that allow multiple computers to be connected to one another through Ethernet cables within a LAN. Hubs work well for small independent networks where only a small amount of data is transmitted between the computers. Hubs can also be used to provide a connection between LANs. Hubs operate by transmitted all received data packets to all connected devices.

Switches

Networking switches are also used to connect individual computers together to form a LAN. Switches differ from hubs in that they do not broadcast all received data packets to all computers on the network. Instead, switches use the Layer 2 Media Access Control (MAC) address of each computer to determine where to send addressed packets of data. As a result, the network throughput of the LAN segment improves and can support a greater amount of data in a shorter period of time.

Routers

Networking routers are used to connect LAN segments to one another. These LANs can be internal to an organization, or can also connect a LAN to a larger network, a WAN, like the World Wide Web (WWW). Routers operate at Layer 3 of the OSI, leveraging the IP address of the devices connected. The router maintains a list of known IP addresses. These IP addresses are the addresses of other routers, switches, and any computers connected to the router. A common requirement for a network is the Default Gateway or Router.

Default Gateway/Router

An additional component that is necessary is the default gateway or default router. This is also a 32-bit address that is used by the LAN to forward packets of data that are addressed to computers that do not exist on the LAN. The default gateway/router forwards these packets to a network router, where the router figures out to where to send the data packets in order to reach their final destination.

Firewalls

Security is very important for IP based networks. Firewalls are common security devices that are present on IP networks. Firewalls are often found as software applications and networking hardware. Firewalls are configured to explicitly prevent or allow the transmission of data based on IP address, protocol, and ports. When setting up a JREAP-C communication link, it is important that coordination occurs between the network planners and network management staff to ensure that firewalls are configured to permit participating computers to communicate with one another over the designated ports.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

CHAPTER 8
Fifth Generation Aircraft: An Overview of IFDL and MADL

Introduction

Fifth generation fighters include the F-22 Raptor fighter and F-35 Lightning II joint strike fighter that are known for their stealth characteristics. That is also true for the fifth-generation TDLs they utilize. The F-22 utilizes the Intraflight Data Link (IFDL) and the F-35 incorporates the Multifunction Advanced Data Link (MADL) developed and integrated by Northrop Grumman.

Fighter Jets by Generation

The military community categorizes jet fighters by generation. The first generation began with subsonic aircraft from the WWII and Korean War era. The first three generations of jet fighters lasted about a decade each. The fourth generation began around 1970 and continues to constitute most fighters in service. Certain fighter platforms that have been significantly improved are sometimes called generation 4.5. This category includes the F-15 Eagle and F-16 Falcon, both of which incorporate Link 16 capability.

Fifth Generation Fighters

Fifth-generation fighters incorporate the latest technological and materials advances in airframe and propulsion and incorporate highly sophisticated avionics including flight control systems. Most notably, fifth generation fighters have low observability stealth characteristics. These fighters also utilize a wealth of sophisticated sensors and communication systems integrated into the onboard avionics to enable them to be key participants in net-centric military operations. Currently, only two fifth-generation fighters have been fielded—the F-22 Raptor fighter and the F-35 Lightning II joint strike fighter. The F-22 production completed in 2012 with a total fielded fleet more than 180.

Figure 8-1. An F-22 Raptor utilizes the IFDL data link. IFDL provides both point-to-point data as well as voice communications. IFDL also provides a secure, low-observable data communication link.

The F-35 is a stealthy, supersonic, multirole fighter designed to meet the requirements of the United States (US) and allied defense forces worldwide for an affordable next-generation fighter. It will replace a wide range of aging fighter and strike aircraft currently in the inventories of the US Air Force, Navy, Marine Corps and allied defense forces.

Northrop Grumman is a principal member of the F-35 industry team, which is developing and producing three variants. The F-35A is the conventional takeoff and landing variant, the F-35B is the short takeoff-vertical landing variant, and the F-35C is the carrier variant. The F-35B is expected to reach initial operational capability late 2015.

Figure 8-2. The F-35 Lightning II Joint Strike Fighter will be fielded with three variants and will be deployed to multiple allied nations.

While the F-22 is strictly a US Air Force platform, purchase of the F-35 by the US armed forces and partner countries combined with foreign military sales are expected to exceed 4,000 total aircraft.

Fifth-Generation Fighter Tactical Data Links

Low observability, superior capabilities and rich sensor package data are key assets for fifth-generation fighters. This is also true for the TDL waveforms they utilize. The F-22 utilizes the IFDL and the F-35 incorporates the MADL developed and integrated by Northrop Grumman. These fifth-generation waveforms provide superior shared situational awareness with similar F-22 or F-35 platforms. While this enhances low observability, it also means that the rich sensor data and situational awareness their advanced systems collect are currently only shared between fifth-generation platforms.

Multifunction Advanced Data Link (MADL)

Northrop Grumman developed MADL as one of the functionalies of the AN/ASQ-242 integrated communications, navigation and identification (CNI) avionics that are critical to the F-35 mission systems suite. MADL is a high-data-rate, directional communications link. The advanced data link allows coordinated tactics and engagement to bring significant operational advantages to fifth-generation aircraft operating in high-threat environments.

Northrop Grumman designed and produced the AN/ASQ-242 CNI system, which can be dynamically programmed to arm the F-35 pilot with multiple-mission capabilities engineered for seamless transition from one mission phase to the next. In addition, to MADL, the F-35 CNI system also includes Link 16 for communicating with other aircraft including close air support. However, Link 16, while secure and encrypted, can be more readily monitored by enemy signal intelligence and so is not utilized for transmission by the F-35 when operating in low observable mode.

As a fifth-generation data link, MADL provides for cooperative engagement among members of a flight group without compromising low observability performance.

In operation, MADL joins the communications, navigation and identification (CNI) Link 16 and variable message format network present on an F-35 aircraft, and data is correlated with information from other F-35 sensors by a fusion system to form a simplified situational awareness picture on the pilot's cockpit displays.

Northrop Grumman's integrated CNI system provides to F-35 pilots the equivalent capability of more than 27 avionics subsystems. By using its industry-leading software-defined radio technology, Northrop Grumman's design allows the simultaneous operation of multiple critical functions while greatly reducing size, weight and power demands on the advanced fighter. These functions include Identification Friend or Foe, automatic acquisition of fly-to points, and various voice and data communications, including MADL, which was approved by the US Department of Defense Joint Requirements Oversight Council for use on all low-observable platforms.

Figure 8-3. The F-35 Lightning II operates with MADL and Link 16. The Northrop Grumman-developed MADL provides an airborne data link that supports cooperative engagements between stealth aircraft without compromising stealth observability performance. Integrating the avionics and incorporating MADL allows the F-35 pilot to view a rich, integrated situational awareness picture in the cockpit.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Introduction

Tactical gateways and voice bridging are not Tactical Data Links (TDLs) in themselves; rather, they make the performance of TDLs and radio communications more effective, secure and assured across an entire theatre of operations—whether military or civilian.

Overview of Tactical Gateways and Voice Bridging

Modern warfare is as dependent on information and communication as it is on military strategy and tactics, high-tech weapons, and the skills of the warfighter. Tactical data link and voice communications are the means by which the Services, North Atlantic Treaty Organization (NATO), or coalition forces execute complex missions to make the world a safer place.

Over time, radio and data link technologies evolved for different branches of the Service or for different platforms using their own defined frequencies or waveforms. The result? Ground forces, aircraft, ships, and command and control platforms often could not communicate with each other—putting a strain on joint interoperability.

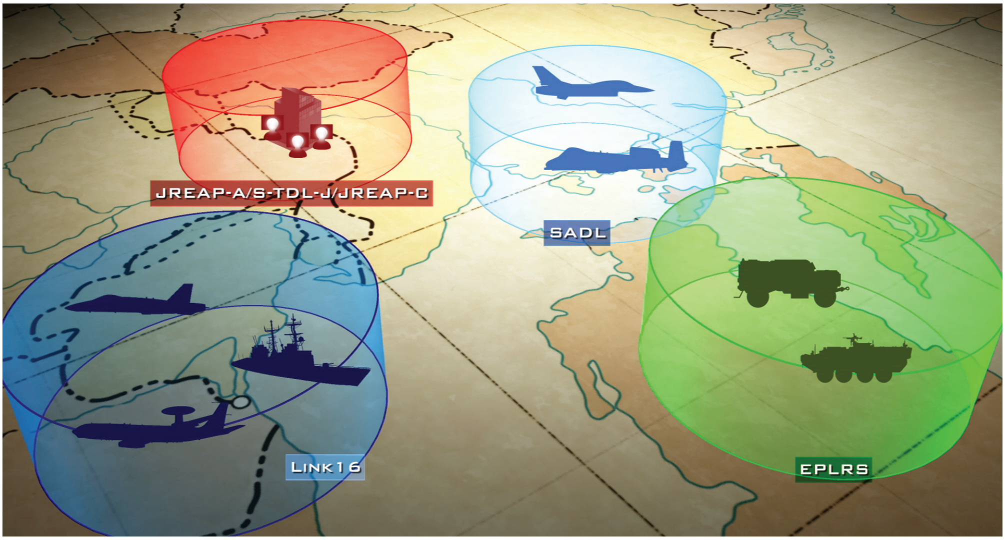


Figure 9-1. Networks can be segregated due to distance and line-of-sight limitations. Networks are also limited by different equipment, TDL protocols and frequencies utilized by different military forces or emergency civilian personnel.

Tactical gateways and voice bridging can provide a major improvement in communication by leveraging hardware, software and—in the case of airborne tactical gateways—high altitude—to overcome line of sight (LOS) limitations from terrain, and incompatible frequencies between allied forces on the battlefield or emergency responders at the scene of a natural disaster.

Tactical Gateways and TDLs

The purpose and nature of a TDL such as Link 16 is to enable all participants in the network to share the situational awareness of all others in the network. If a forward-deployed High Mobility Multipurpose Wheeled Vehicle (HUMVEE) or a fast-moving F-16 detects something significant, all others in the network can see it as well—and at the same time—if there are no obstacles such as limited LOS. The airborne tactical gateway effectively overcomes the worst obstacles presented from canyons or mountains by virtue of being high in the sky and usually within LOS of all participants. The impact of having such an airborne tactical gateway is to effectively position a network participant with an antenna high in the sky where LOS limitations are less of a factor.

Figure 9-2. When an airborne tactical gateway becomes a participant in the network, that aircraft can be positioned high enough in the sky to maintain line of sight to all participants. This allows the airborne gateway to relay, translate or forward TDL data to all participants, dramatically improving interoperability and communication.

Voice Bridging

In today's environment, maintaining voice communications is imperative and challenging. In some cases, a unit may be relying on a lower power vehicle radio or manpack with limited range. In mountainous terrain, a signal can be lost easily due to line of sight limitations for secure communication. And in many cases, different service branches or emergency civilian personnel utilize radios that operate on different frequencies and so cannot communicate with other units regardless of range or terrain. These are just some of the challenges of voice communications faced by coalition forces. These same challenges have faced first responders and emergency personnel dealing with devastating natural disasters. Without unified and dependable communications, critical life-saving actions are limited or delayed due to the inability to share a unified communications capability.

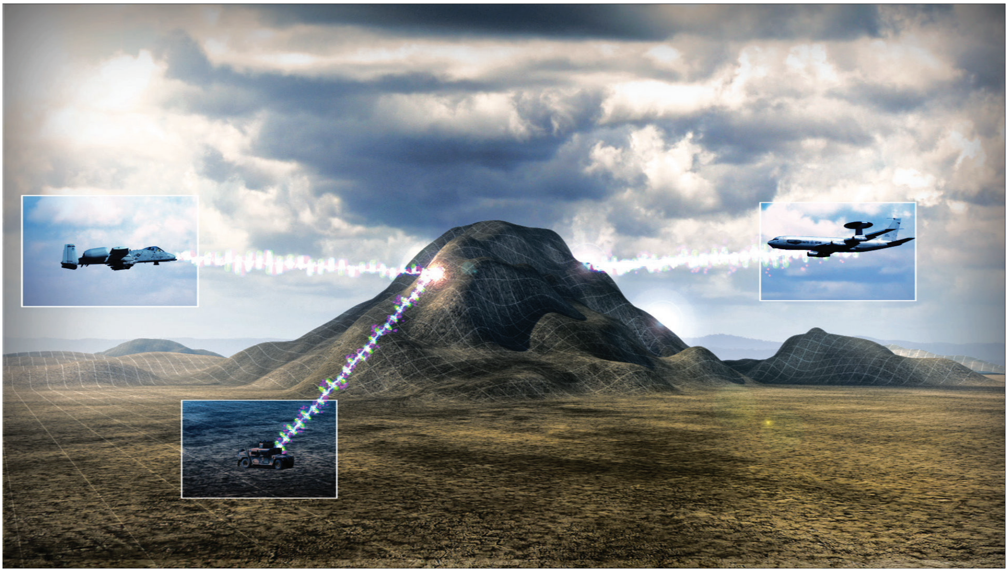


Figure 9-3. Voice communication can be easily disrupted by terrain and different radios and frequencies utilized by various service branches or emergency responders. This challenge to voice communications is faced by aircraft beyond line of sight as well as troops just over a rise.

The term "voice bridging" can be considered as the ability to transmit and receive over two or more disparate frequencies. The process works when an individual or aircraft transmits on a given frequency using normal protocol and crypto. High in the sky, the voice bridge platform receives that radio transmission and then retransmits it on a second given frequency with improved power and reach, all the while maintaining crypto and LOS to all participants from its high altitude. This voice bridging effectively removes many of the challenges due to LOS, low power and frequency disparity. Participants in voice bridging communicate as they normally would but now they can communicate across longer distances and with forces and platforms that would have been inaccessible before. This process can continue indefinitely when the airborne tactical gateway is deployed.

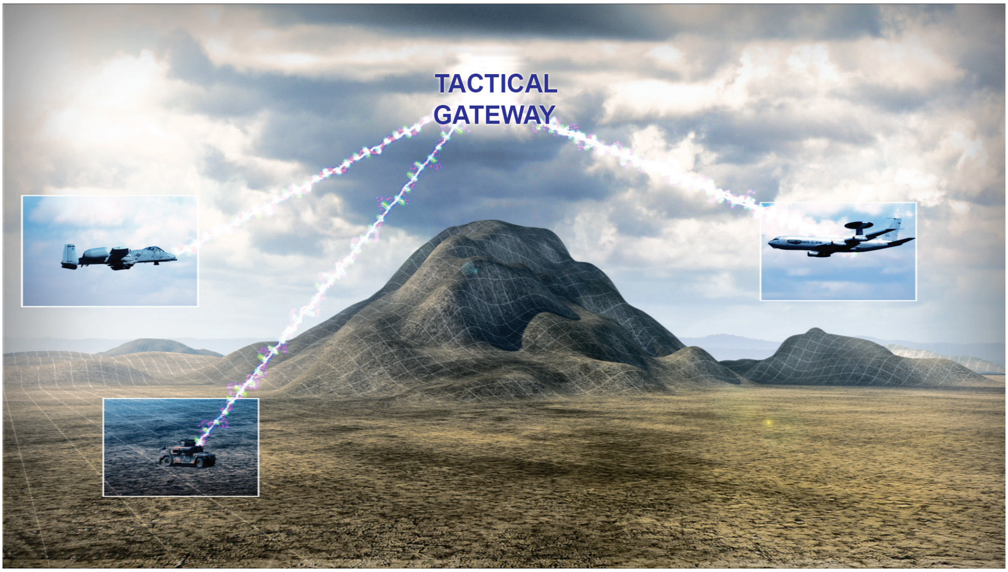


Figure 9-4. The airborne tactical gateway effectively places an antenna high in the sky within LOS of most participants to dramatically improve TDL and voice communications.

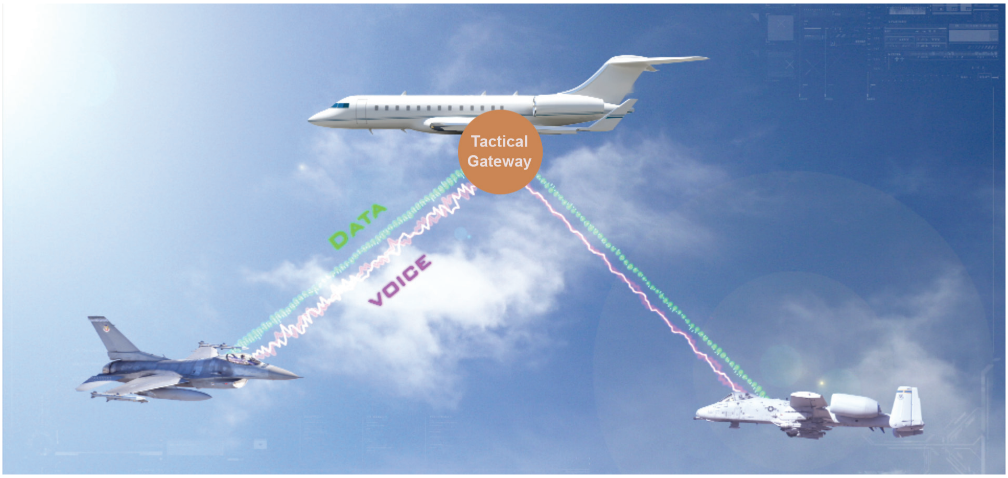


Figure 9-5. Capabilities of the tactical gateway are dependent upon the specific configuration of hardware and software. TDL forwarding and relay is separate from voice bridging. However, an airborne tactical gateway can provide both capabilities if so equipped with the designated terminals, radios and software.

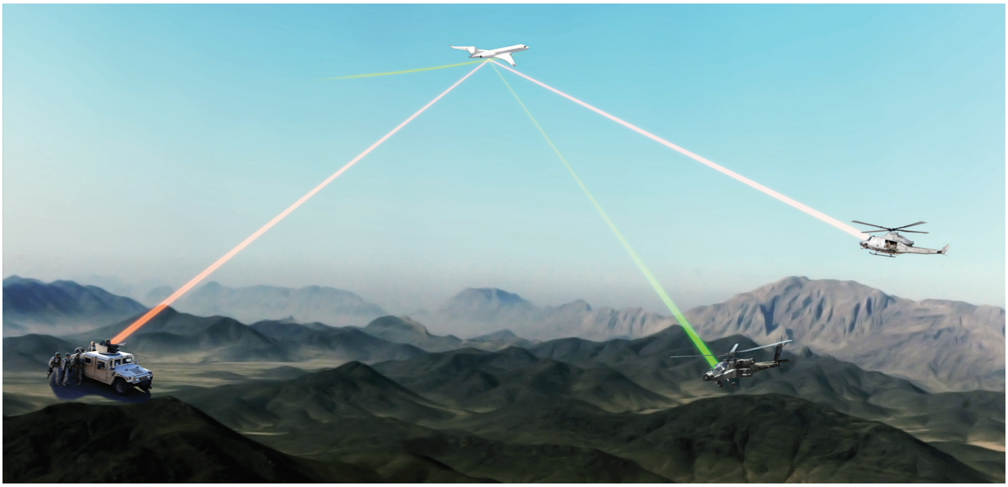


Figure 9-6. With the tactical gateway high in the sky, LOS and power limitations are mitigated and participants can communicate over longer distances. Voice bridging may also allow participants to communicate normally over disparate frequencies if the voice bridge is so configured.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Chapter 10 Northrop Grumman Products

Introduction

As a leader in the development and production of tactical data link communication products for over 52 years, Northrop Grumman provides "best in class" products and services for the United States and its allies. We continue to develop and deliver excellence, strive for continuous improvement and respond vigorously to change.

This section provides overview information on Northrop Grumman's products. For more detailed information, follow the uniform resource locator (URLs), Quick Response (QR) codes, or call one of our product sales managers listed at the end of the chapter.

■ Icons and Links

With each product you will see a QR icon that resembles this black square. This QR code can be read by downloading a free application (QR Code Reader from the Internet) to your mobile phone or tablet device. By scanning this QR code, additional information about the product may be obtained. A URL or brochure will be provided to those who do not have the capability of using a QR reader.

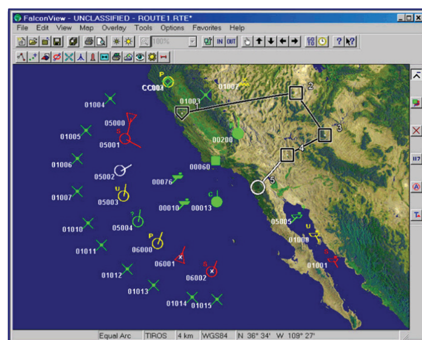
http://www.northropgrumman.com/Capabilities/DataLinkProcessingAndManagement/Pages/default.aspx

Gateway Manager (GM)

Gateway Manager is a powerful data link router and forwarder that gives commanders the ability to network multiple platforms communicating on different protocols while providing a comprehensive operational picture in real time. Adaptable, scalable, and dependable, with the inherent economy provided by Commercial Off-the-Shelf (COTS) hardware, the system assures situational awareness to operational participants at all levels of the command structure. GM is offered commercially and on Naval Sea Systems Command's (NAVSEA's) hardware and engineering service contracts and is used on Battlefield Airborne Communications Node (BACN) and Roll-On Beyond-line-of-sight Enhancement (ROBE), as well as in the Thales Raytheon Battle Control System-Fixed (BCS-F) Program.

Northrop Grumman's GM supports virtually all tactical communications, including:

- Link 16
- Link 11
- Distributed Information Systems (DIS)
- Satellite TADIL J (SAT J)
- MIL-STD-3011 (Joint Range Extension Application Protocol (JREAP))
- Embedded National Tactical Receiver (ENTR)



Gateway Manager is compatible with the Portable Flight Planning Software (PFPS) and FalconView.

Northrop Grumman continues to evolve the Gateway Manager, adding new capabilities that can be applied to existing systems, making it the tactical router not only for today, but for the future.

http://www.northropgrumman.com/Capabilities/GatewayManager/Pages/default.aspx

Link Management System (LMS)

Modern tactical data links (TDLs) provide superior surveillance, command and control, secure voice, jam resistance and security functions, combined with high throughput, granularity and capacity. These powerful capabilities lead to complex and greater challenges in establishing reliable network performance. The LMS presents a real-time tactical situation display, the status of each network participant, and the overall network performance and health. LMS enables operators to customize displays to their specific needs of network performance and identify participants experiencing problems.

The Link Management System was developed for Link 16 and other TDLs to provide the Joint Interface Control Officers (JICO) and other network managers with rapid planning, dynamic management and accurate analysis of theater communications during real-world operations.

LMS allows operators to customize the information display to whatever configuration is most useful.

LMS features multiple views of data link performance:

- TDL Network Summary and Status Whiteboard
- Tactical Situational Analysis
- Link 16 Connectivity Evaluation Support
- Adherence to Link 16 network design
- Link 16 Time Slot Duty Factor/Frequency Clearance Agreements (TSDF/FCA)
- Link 16 network usage
- Link 16 signal quality
- Link 16 network trend analysis

LMS has proven itself on the battlefield with deployments in Kosovo, Afghanistan and the Persian Gulf (Operation Iraqi Freedom and Operator Enduring Freedom), where LMS was an excellent ally when warfighters needed information during operations.

http://www.northropgrumman.com/Capabilities/LMS/Pages/default.aspx

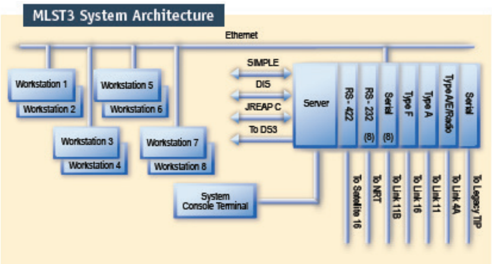
NORTHROP GRUMMAN

Multi-Link System Test and Training Tool (MLST3)

The MLST3 generates simulated tactical scenarios to stimulate data link networks for testing. It is used by the US Navy, Air Force and joint testing organizations to test conformance with tactical data link standards and interoperability certification requirements. MLST3 is deployed throughout the world as the leader in data link testing, contributing to multination interoperability.

The MLST3 enables users to input pre-scripted scenarios or manually inserted events to generate a flexible interactive environment. This pre-scripted scenario ensures desired capabilities to be tested, while manual insertions allow flexibility during training or development investigation. To support these capabilities, MLST3 operates in three modes:

- Pre-Test Application
- Real-Time Application
- Post-Test Analysis



For Link 16, MLST3 interfaces via MIL-STD-1553B or Ethernet. For Link 11, it uses MIL-STD-1397A or ATDS. MLST3 communicates with JREAP C and SIMPLE and with DIS via Ethernet.

The MLST3 Test Control User Interface features the look and feel of conventional Windows interfaces. Operators use dynamic, menu-selectable displays to control the system during testing. Its Message Monitor Display shows all transmitted and received tactical messages, as well as the scenario and operator-initiated events. The Tactical Situation Display depicts filterable track symbology with background geopolitical maps scalable from global to one square mile.

http://www.northropgrumman.com/Capabilities/MLST3/Pages/default.aspx

Tactical Data Link Integration Exerciser (TIGER)

The TIGER is based on the leading Department of Defense data link test system, the MLST3, and predecessor systems. TIGER generates tactical data link messages and outputs them as a complete tactical exercise scenario to the system under test. The system under test is considered interoperable, when it receives and interactively processes and displays the output and complies with appropriate specifications.

The TIGER software suite supplies Pre-Test, Real-Time, and Post-Test Analysis applications. Its hardware includes rack mountable, portable, laptop, and cabinet configurations. The cabinet option can include a Multifunctional Information Distribution System - Low Volume Terminal (MIDS LVT) and a remote power supply.

TIGER hardware configurations are available in laptop, portable, desktop, rack-mountable and cabinet.

Using a powerful battlespace simulator and a flexible array of analysis capabilities, TIGER is a proven interoperability test system used worldwide. The TIGER stimulates systems under test with tactical scenarios and works with:

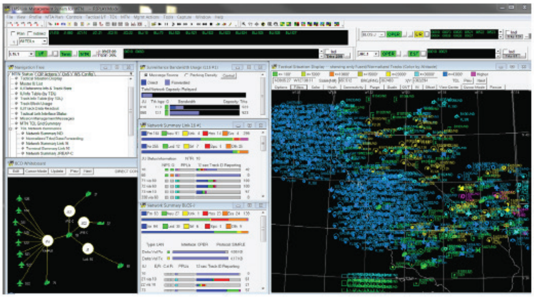
- Link 16
- Link 11
- Link 22
- Distributed Interactive Simulation (DIS)
- Joint Range Extension Applications Protocol (JREAP) C
- Standard Interface for Multiple Platform Link Evaluation (SIMPLE) [STANAG 5602]
- and more

http://www.northropgrumman.com/capabilities/tiger/Pages/default.aspx

Tactical Edge Advanced Management (TEAM)

Tactical Edge Advanced Management is based on 17 years of exercise and deployed operational use and provides the JICO with rapid planning, dynamic management and accurate analysis of theater communications.

TEAM is a laptop-based multi-TDL management and network-level diagnostics tool. Its two high-definition customizable displays ensure each user has a full understanding of the network. TEAM is composed of two major components: TEAM LMS (Link Management System) for TDL monitoring, management and analysis, and TEAM View which powers 3D situational awareness displays that present the operational picture.



TEAM LMS is the engine for TDL monitoring, management and analysis.

TEAM supports the following TDLs:

- Link 16: MIDS
- JREAP-A
- JREAP-C: MIL-STD-3011, Appendix C
- Other Internet Protocol (IP) J-series protocols
- Situational Awareness Data Link (SADL), 11xy, 11z
- Enhanced Position Location Reporting System (EPLRS)
- SAT J
- Variable Message Format (VMF) Radio UIDM

http://www.northropgrumman.com/Capabilities/TacticalEdgeAdvancedManagement/Pages/default.aspx

Multi-Link Service Gateway (MLSG)

Multi-Link Service Gateway is a modular, scalable multi-link processor that provides full TDL capability for Link 16, Link 22, Link 11, and/or VMF. Designed as an upgrade for existing platforms, MLSG is suitable for individual or multi-link implementation in maritime, land, and headquarters installations. Northrop Grumman is the only U.S. vendor of Link 22 processing recognized by the Link 22 international program office. As a result, all of the Link 22 message sets are coded and available.

MLSG's rugged industrial design meets most maritime environmental requirements.

The MLSG is based on Northrop Grumman's GM, which has been fielded on several U.S. and foreign military platforms, including Battle Control System-Fixed and FLOres Ralus Komsys (Switzerland). A proven COTS product, the GM has been certified by the Joint Interoperability Test Command as a multi-link forwarder for JREAP A, B, and C; Link 16; Link 11; and Link 11B.

MLSG is adaptable to platform-specific requirements and will provide reliable and affordable performance.

http://www.northropgrumman.com/Capabilities/MultiLinkServiceGateway/Pages/default.aspx

Distributed Simulation and Stimulation System (DS3)

Distributed Simulation and Stimulation System provides high fidelity sensor simulation for a multitude of sensors, including rotating radars, phased array radars, and identification, friend or foe transponders.

DS3's tactical environment simulator stimulates combat systems with sensor, navigation and weapon system inputs. An adaptable, modular and scalable DS3 architecture accommodates emerging requirements brought about by the need to test, train and certify combat system evolutions in response to rapidly-changing threats.

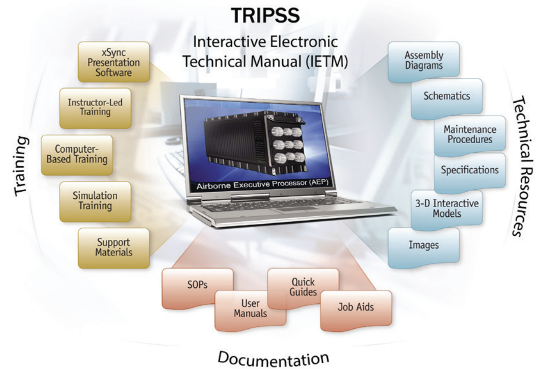
DS3 shares high-fidelity simulations of air, surface, and ballistic missile tracks over a DIS-compliant network and communicates with tactical systems in real time. The DIS interface enables additional DS3s to accommodate other interfaces or multiple platforms under test with the same simulated environment, and interconnects with other DIS-compliant simulations.

The DS3 simulates motion and activities of thousands of air and surface tracks simultaneously and models sensors and the environmental effects on them. These effects include terrain track masking; display and sensor effects such as track suppression, multipath, ducting, and radar accuracy; clutter such as storm cloud, surface clutter, and specular clutter (short-duration tracks).

http://www.northropgrumman.com/Capabilities/DS3/Pages/default.aspx

Training and Technical Resources Integrated Performance Support System (TRIPSS)

Training and Technical Resources Integrated Performance Support System is a custom training and technical documentation solution that is cost effective, while making training and technical data available to all users whenever and wherever up-to-date information is needed.



The customized TRIPSS environment is a comprehensive training and technical data support, integrated into a single access point that provides on demand, 24/7 availability. Users experience one intuitive interface and gateway to expert training and technical documentation. Under the hood, multiple capabilities unite to provide total performance support: xSync, Computer-based Training/ Web-based Training (CBT/WBT) Modules, Multimedia and printable job aids, and Interactive Electronic Technical Manual (IETM).

For fundamental understanding and training, consider our digital courseware for:

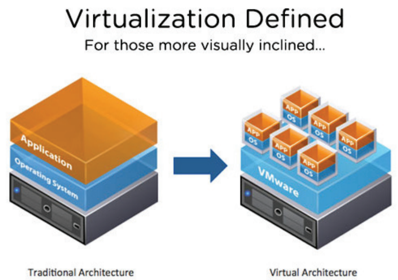
- Understanding Link 16
- Introduction to Tactical Data Links
- Introduction to the Link 16 Management System (LMS)
- Introduction to Gateway Manager (GM)

http://www.northropgrumman.com/Capabilities/TIPSSAndTRIPSS/Pages/default.aspx

Joint Interface Control Cell (JICC) in a Box (JIB)

The JIB is a deployable mobile platform for Joint Interface Control Cell applications. This innovative platform is a hardware platform that supports tactical data link applications and replaces stovepiped systems with more efficient virtualized computing and networking ones with improved performance and availability through load balancing and failover.

Designed to have configurable options for serial and parallel radio communications protocols, this system is making tactical data link and IP networking available when you need it. Its ability to consolidate all TDL applications on a single server provides a small footprint, and in turn, eliminates the need for much of the currently used hardware.

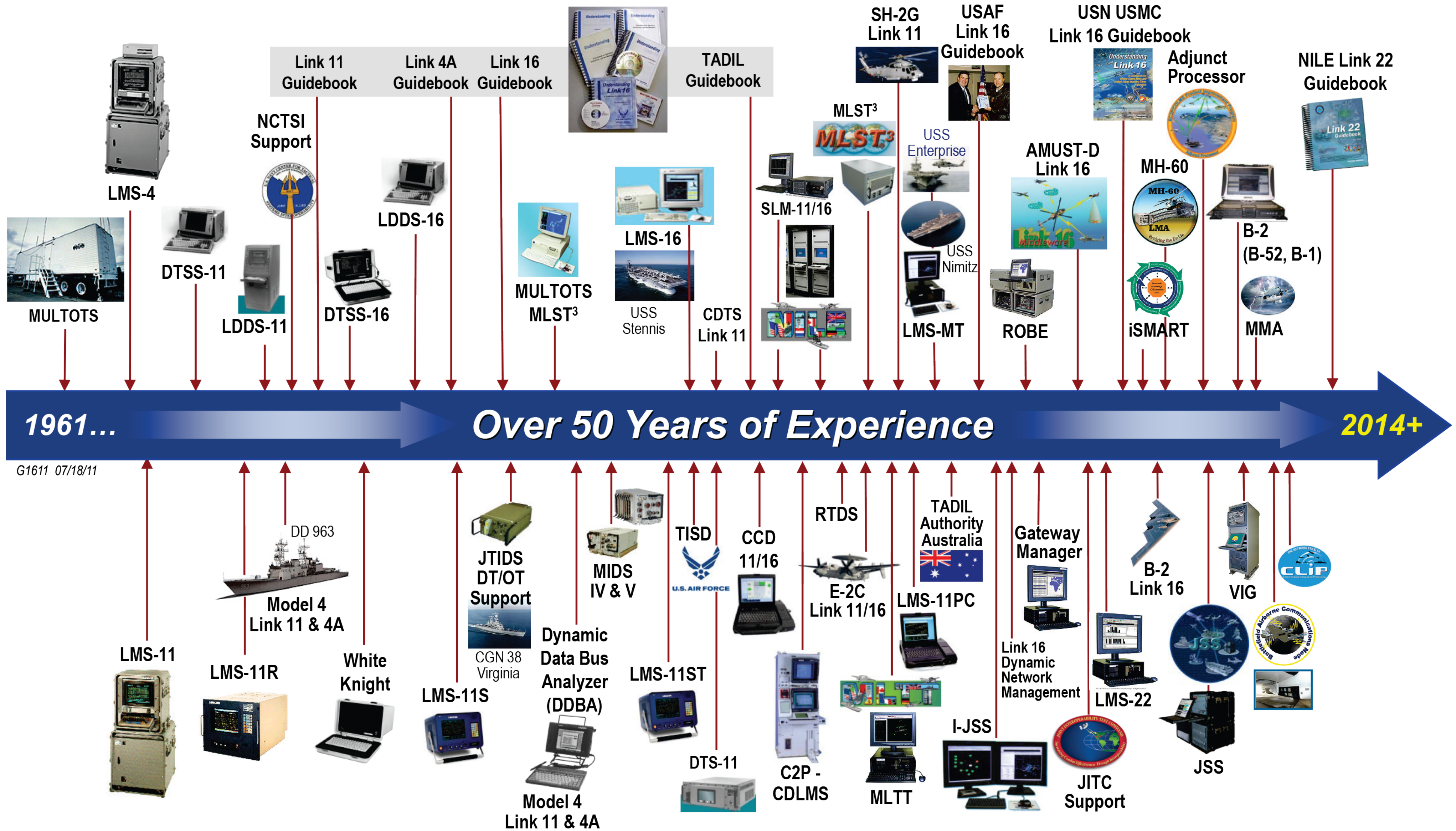


The JIB supports the following TDL protocols and radios:

- Link 11
- Link 16 (Radio Frequency (RF,) JREAP-A/B/C, SAT-J, Serial-J)
- Link 22
- VMF
- Integrated Broadcast Service/Common Message Format (IBS/CMF)
- MIDS LVT
- PRC-117 F/G

http://www.northropgrumman.com/Capabilities/DataLinkProcessingAndManagement/Documents/JIB_datacard.pdf

Tactical Data Link History



Count on the Tactical Communications Leader – **Northrop Grumman**

Northrop Grumman
9326 Spectrum Center Boulevard
San Diego, CA 92123

Contact us 24 hours a day, 7 days a week
1-877-784-HELP (4357)
Email: cis.productsupport@ngc.com
Website: www.tacticalnetworks-ngc.com

Products and Program Information:

Scott Alexander
858-514-9769
Email: scott.w.alexander@ngc.com

Yuri Wyatt
858-514-9141
Email: yuri.wyatt@ngc.com

Nina Hughes
858-514-9204
Email: nina.hughes@ngc.com

Training Conduct and Development Information:

Daniel Akers
TRIPSS and Training Conduct / Development
858-514-9338
Email: daniel.akers@ngc.com

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Appendix A

Tactical Data Link Training Opportunities

From expert instructor-led training to cutting-edge, technology-based blended training, we provide a gamut of services. Whatever your need may be, our services are tailored to meet your requirements:

- Instructor-led and on-the-job training that is customized for advanced topics and delivered to either your site or the Northrop Grumman San Diego Spectrum Center campus.
- Digital training providing fundamental on-demand training for Tactical Data Links (TDLs) and Northrop Grumman TDL tools, setting the stage for more advanced instructor-led future training.
- Customized Training and Technical Resources Integrated Performance Support System (TRIPSS) blended learning tools immersing your personnel in total training and technical documentation support. With TRIPSS, users can always access current, accurate training and documentation at the point and time of need.

TDL and Product Training

Northrop Grumman offers comprehensive training for all its products, including tailored classes on Link 16, Link 11, and Link 22. We authored the well-known Understanding series of data link guidebooks. The Understanding Link 22 guidebook can be downloaded in its Overview version which has been approved for public release (Chapter 1 plus selected appendices). Other guidebooks are also available from Northrop Grumman.

Training and Technical Resources Integrated Performance Support System (TRIPSS)

Imagine a custom training and technical documentation solution, lowering costs, while making training and technical data available to all users whenever and wherever up-to-date information is needed. With TRIPSS, imagination is a reality as users are immersed in a total training and technical documentation support system, enabling true blended training, just-in-time learning, and interactive technical, and maintenance documentation at the point and time of need.

For more information, visit http://www.northropgrumman.com/Capabilities/DataLinkProcessingAndManagement/Documents/tipss_tripss.pdf

Link 16

Northrop Grumman offers a Link 16 seminar for operators, field support personnel, programmers, and engineers, at either a customer site or at Northrop Grumman's San Diego facility, as required. The course focuses on the Link 16 waveform and messages.

Link 11

Northrop Grumman offers a Link 11 seminar for operators, field support personnel, programmers, and engineers, at either a customer site or at Northrop Grumman's San Diego facility, as required. The course focuses on the Link 11 waveform and messages.

■ Link 22

Replacing the aging Link 11 standard and interoperable with Link 16 networks. Link 22 enables participating North Atlantic Treaty Organization (NATO) nations to procure tactical data systems that are interoperable and compatible with those of the other participating Link 22 nations. Northrop Grumman was there at the beginning in 1992.

Northrop Grumman offers a Link 22 seminar for operators, field support personnel, programmers, and engineers, at either a customer site or at Northrop Grumman's San Diego facility, as required.

■ Tactical Data Link Management Systems Training

Operator courses for Northrop Grumman's data link management systems—the Link Management System (LMS™), the Gateway Manager (GM), Tactical Edge Advanced Management (TEAM), and Link Monitoring System for Link 11 (LMS-11)—are also available. Typically, these courses are conducted at a customer installation site, but they may be conducted at Northrop Grumman's San Diego facility, as required.

♦ Link Management System (LMS)

LMS is a proven link management capability extended to a multi-TDL environment. Manage TDL networks in real-time with this "all-services" Commercial Off-the-Shelf (COTS) Joint Interface Control Officer (JICO) tool.

♦ Gateway Manager (GM)

GM is a powerful data link router and forwarder that gives commanders the ability to network multiple platforms communicating on different protocols while providing a comprehensive operational picture in real time. GM hosts and emulates more Joint Tactical Information Distribution System/Multifunctional Information Distribution System (JTIDS/MIDS) terminals than any gateway available. It controls data communications locally and remotely, making it a flexible tool for managing tactical networks.

♦ Tactical Edge Advanced Management (TEAM)

TEAM is composed of two major components: TEAM LMS (the Link Management System engine for TDL monitoring, management and analysis) and TEAM View (which powers 3-D situational awareness displays that present the operational tactical picture).

♦ Link Monitoring System for Link 11 (LMS-11)

LMS-11 has been monitoring Link 11 networks and improving data link communications for more than two decades. LMS-11 enables Link 11 management, net monitoring, net troubleshooting, equipment testing, and distributed serial communications.

■ Data Link Simulator Training

Northrop Grumman also produces data link simulators, which are used for scenario generation, simulation exercises, testing, and TDL message certification. All courses are typically conducted at customer sites.

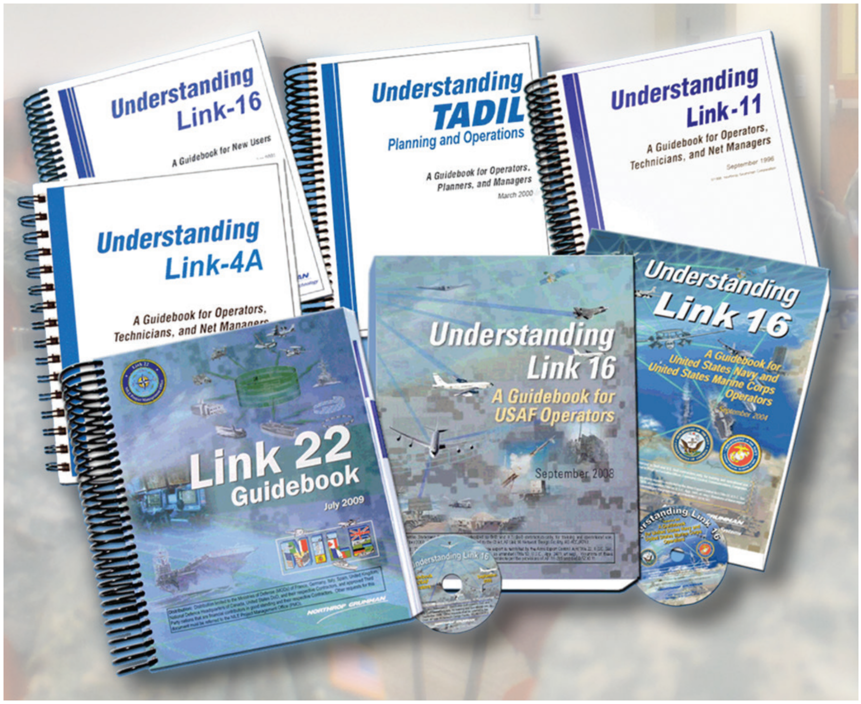
♦ Multi Link Simulation Training and Test Tool (MLST3)

MLST3 is the standard certification tool used to exercise tactical data systems when they are tested and certified for compliance with US Military Standards (MIL-STDs), NATO STANAGs, and joint publications, as well as ensuring interoperability with joint and coalition forces.

♦ Tactical Data Link Integration Exerciser (TIGER)

TIGER is proven interoperability stimulation/simulation system with Link 11, Link 16, Link 22, JREAP C, DIS, SIMPLE, SWIF, and TIF capabilities. TIGER is used worldwide, can be tailored to meet customer requirements, and comes in a variety of mobile and fixed hardware configurations.

We Wrote the Book!



Northrop Grumman's Understanding Link 16 and TDL guidebook series is the definitive Department of Defense standard for TDLs and operational procedures. Our experienced operator instructors provide a thorough grounding in basic and advanced TDLs and Link 16, including Link 11, Link 22, and other various TDLs. They continue to provide in person and virtual expert knowledge, training, and support in all TDL areas, including operator training for Northrop Grumman's TDL tools, such as LMS, GM, TIGER, and TEAM.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Appendix B

Acronyms and Abbreviations

The following acronyms and abbreviations may be found in this document, as well as in certain supporting references.

Acronym	Definition
µs	Microsecond
	A
AAA	Anti-Aircraft Artillery
AADC	Area Air Defense Commander
AEELS	Automatic Electronic Emitter Location System
AB	Air Base
ABE	Air Battle Execution
ABL	Airborne Laser
AC/TMD	Air Control/Theater Missile Defense
ACA	Airspace Control Authority
ACAT	Acquisition Category
ACC	Air Combat Command
ACC/A3YJ	Air Combat Command/C2ISR Operations Division - Link 16 Network Design Facility
ACCS	Air Command and Control System (NATO)
ACDS	Advanced Combat Direction System
Ack	Acknowledgement
ACM	Airspace Control Means
ACO	Airspace Control Order
ACP	Airspace Control Plan
ACQ	Acquire
ACR	Air Control Revision
ACS	Air Control Squadron
Act.	Action Code
ACUS	Army Common User System
ACW	Air Control Wing
ADA	Air Defense Artillery (US Army)
ADAM	Air Defense Airspace Management (US Army cell)
ADCP	Air Defense Communications Platform (US Marine Corps)
Addr	Address

Acronym	Definition
ADP	Air Defense Plan
AEELS	Automatic Electronic Emitter Location System
AEHF	Advanced Extremely High Frequency
AETACS	Airborne Elements of the Tactical Air Control System
AF	Air Force
AF DCGS	Air Force Distributed Common Ground Station
AF GCIC	Air Force Global Cyberspace Integration Center
AF NDF	Air Force Link 16 Network Design Facility
AF PEO/C2&CS	Air Force Program Executive Officer for Command and Control and Combat Support
AFAPD	Air Force Applications Program Development
AFATDS	Air Force Airborne Tactical Data System;
	Advanced Field Artillery Tactical Data System
AFB	Air Force Base
AFCENT	Air Force Central
AFEUR	Air Force Europe
AFFOR	Air Force Forces
AFMSS	Air Force Mission Support System
AF NDF	Air Force Network Design Facility
AFNMWG	Air Force Link 16 Network Management Working Group
AFNORTH	Air Force North
AFOIRG	Air Force Operational Interoperability Requirements Group
AFPAC	Air Force Pacific
AFPD	Air Force Policy Directive
AFROK	Air Force Republic of Korea
AFSOC	Air Force Special Operations Command
AFSOF	Air Force Special Operations Forces
AFSOUTH	Air Force South
AFSPC	Air Force Space Command
AFSTRAT	Air Force Strategic Command

Acronym	Definition
AFTRG	Air Force Tactical Data Network Requirements Group
AFTTP	Air Force Tactics, Techniques, and Procedures
AIMS	Air Traffic Control Radar Beacon System Identification Friend or Foe Mark XII System
AIU	Antenna Interface Unit
AJ	Antijam
AK	Air Key
aka	Also Known As
AKO	Army Knowledge Online
AMC	Air Mobility Command
AMD	Air Mobility Division
AMDPCS	Air and Missile Defense Planning and Control System (US Army)
AMOS	Air Mobility Operations Center
AMP	Amplification
AMSS	Airborne Mission System Specialist
ANDF	Army Network Design Facility
ANG	Air National Guard
ANSI	American National Standards Institute
AOC	Air and Space Operations Center
AOCE	Alpha-Omega Change Engineering
AOCFTU	Air Operations Center Formal Training Unit
AOCP	Airborne Operational Computer Program
AOD	Air Operations Directive
AOG	Air Operations Group
AOI	Area of Interest
AOP	Areas of Probability
AOR	Area of Responsibility
AOS	Air Operations Squadron
AR	Air Refueling
ASCIET/JCIET	All Services/Joint Combat Identification Evaluation Team

Acronym	Definition
ASIT	Adaptable Surface Interface Terminal
ASO	Air Surveillance Officer
ASOC	Air Support Operations Center
ASU	Anti-surface Warfare; Aircraft Sector Understanding; Antenna Switching Unit
ASW	Anti-submarine Warfare
ATACC	Advanced Tactical Air Control Center
ATCRBS	Air Traffic Control Radar Beacon System
ATDL-1	Army Tactical Data Link 1
ATDS	Airborne Tactical Data System
ATO	Air Tasking Order
ATTN	Attention
AU	Australia
AWACS	Airborne Warning and Control System
AWACS ADS	AWACS Airspace Deconfliction System
AWACS AIU	AWACS Avionics Interface Unit
AWACS CC-2E	AWACS Central Computer Version 2E
AWACS CDU	AWACS Control Display Unit
AWACS CPS	AWACS Communications Processing Subsystem
AWACS DDP	AWACS Distributed Data Processing
AWACS ECSP	AWACS Electronic Command Signal Processor; AWACS Electronic Control Signal Processor
AWACS EGI	AWACS Embedded Global Positioning System/Inertial Navigation Unit
AWACS ETK	AWACS Embedded Toolkit
AWACS HDS	AWACS Hard Disk Subassembly
AWACS HPA	AWACS High Power Amplifier
AWACS HPAG	AWACS High Power Amplifier Group
AWACS IU	AWACS Image Understanding

Acronym	Definition
AWACS LPF	AWACS Low Pass Filter
AWACS PDU	AWACS Power Distribution Unit
AWACS RFA	AWACS Radio Frequency Amplifier
AWACS SDC	AWACS Signal Data Converter
AWACS SDU	AWACS Secure Data Unit
	B
BAO	Battlefield Air Operations
BC3	Battle Command and Control Center
BCP	Battery Command Post (US Army)
BCS-F	Battle Control System-Fixed
BCS-M	Battle Control System-Mobile
BDA	Battle Damage Assessment
BDHI	Bearing Distance Heading Indicator
BE	Belgium
BHI	Bomb Hit Indication
BIM	Bus Input Message
BIT	Built-in Test
Bldg	Building
BLK	Block
BLOS	Beyond Line of Sight
BM	Battle Management
BMC2	Ballistic Missile Command and Control
BMC4I	Battle Management Command, Control, Communications, Computers, and Intelligence
BMD	Ballistic Missile Defense (US Army)
BMDS	Ballistic Missile Defense System
BO	Bailout
BOM	Bus Output Message
bps	Bits per Second

Acronym	Definition
	C
C	Conditional
C&D	Command & Decision [system] (US Navy)
C/S/A	Combatant Commands, Services, and Agencies
C2	Command and Control
C2BMC	Command and Control/Battle Management/Communications
C2I	Command, Control, and Intelligence
C2ISR	Command, Control, Intelligence, Surveillance, and Reconnaissance
C2P	Command and Control Processor (US Navy)
C2WAC	Command and Control Warrior Advanced Course
C2WS	C2 Warrior School
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
CA	Canada
CAC	Common Access Card
CAC2S	Common Aviation Command and Control System (US Marine Corps)
CAF	Combat Air Forces
CANCO	Can Comply
CANTCO	Cannot Comply
CANTPRO	Cannot Process
CAOC	Combined Air and Space Operations Center
CAOC N	Combined Air Operations Center, Nellis AFB
CAOC-X	Combined Air Operations Center, Experimental
CAP	Combat Air Patrol
CAS	Close Air Support
CASBDA	Close Air Support Mission Battle Damage Assessment
CASS	Close Air Support System
CAT	Category
CB	Cobra Ball
CBT	Computer-Based Training

Acronym	Definition
CC	Compass Call; Central Computer
CCC	Common Core Capability
CCD	Common Connectivity Device
CCIP	Common Configuration Implementation Program
CCITT	Consultative Committee International Telegraph and Telephone
CCO	Combat Control Officer
CCPD	Current Cryptoperiod Designator
CCSK	Cyclic Code Shift Keying
CDL	Common Data Link
CDP	Conditioned Diphase
CDLI	Common Data Link Interface (US Army)
CDLIM	Common Data Link Interface Module
CDMA	Code Division Multiple Access
CSMA	Carrier Sense Multiple Access
CDO	Change Data Order
CDP	Conditioned Diphase
CFACC	Combined Forces Air Component Commander
CG	Guided Missile Cruiser (US Navy)
CGN	Guided Missile Cruiser, Nuclear (US Navy)
CGS	Common Ground Station
CH	Switzerland
CID	Combat Identification
CIO	Concurrent Interface Operations
CIU	Concurrent Interface Unit
CIR	Coordinated Implementation Required
CIS	Command and Information Systems
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJCSM	Chairman, Joint Chiefs of Staff Manual

Acronym	Definition
CJTF	Commander, Joint Task Force
CMS	Control Monitor Set
CNR	Combat Net Radio
CNRWG	Combat Network Radio Working Group
CMUP	Conventional Mission Upgrade Program
COCOM	Combatant Command; Combatant Commander
COD	Combat Operations Division
COLE	Concept of Link Employment
COMAFFOR	Commander, Air Force Forces
COMINT	Communications Intelligence
COMSEC	Communications Security
CONCOPS	Concurrent Operations
CONE	Concept of Network Employment
CONUS	Continental United States
CoP	Community of Practice
COP	Common Operational Picture
COS	Combat Operations Squadron
CoT	Cursor-on-Target
COTS	Commercial Off-the-Shelf
CPD	Crypto Period Designator; Combat Plans Division
CPOD	Communications Plan-of-the-Day
CPSM	Continuous Phase Shift Modulation
CPU	Central Processing Unit
CRC	Control and Reporting Center
CRYPDAT	Crypto Data (USMTF SETID)
CS	Combat Sent; Combat Support

Acronym	Definition
CSAR	Combat Search and Rescue;
	Combined Search and Rescue
CSAR-X	Combat Search and Research-X
CSIA	Core – Subscriber Interface Assembly (US Army)
CSM	Common Software Module
CSO	Communications System Operator
CSP	Common Signal Processor
CSS	Cartridge Support System
CST	Communication Systems Technician
CT	Communications Technician
CTN	Common Track Number
CTP	Cypher Text Processor
CU	Control Unit;
	Controlling Unit
CUI	Common User Interface
CUR	Controlling Unit Report
CV	Cryptovariable;
	Aircraft Carrier (US Navy)
CVLL	Cryptovariable Logical Label
CVM	Common Variable Mode
CVN	Aircraft Carrier, Nuclear (US Navy)
CVSD	Continuously Variable Slope Delta
	D
DACAS	Digitally Aided Close Air Support
DAMA	Demand Assigned Multiple Access
DAP-NAD	Deterministic Adaptive Prioritized – Network Access Delay
DASC	Direct Air Support Center
DAV-NAD	Data and Voice – Network Access Delay
dB	Decibels
dBm	Decibels Referenced to One Milliwatt

Acronym	Definition
DCE	Data Circuit-terminating Equipment
DCGS	Distributed Common Ground Station
DCI	Digital Communications Initiative
DDG	Guided Missile Destroyer (US Navy)
DDP	Digital Data Processor
DE	Germany
DED	Data Element Dictionary
DERG	Data Extraction and Reduction Guide
DFI	Data Field Identifier
DFI/DUI	Data Field Identifier and Data Use Identifier
DGT	Designated Ground Target
DHCP	Dynamic Host Configuration Protocol
DI	Data Item
DII/COE	Defense Information Infrastructure/Common Operating Environment
DIS	Distributed Information Systems
DIS IP	Digital Imaging Surveillance Interchange Protocol
DISA	Defense Information Systems Agency
DIVJ	Training Division J
DK	Denmark
DL	Data Link
DLMC	Data Link Management Cell
DLO	Data Link Operator
DLRN	Data Link Reference Number
DLRP	Data Link Reference Point
DME	Distance Measuring Equipment
DMTD	Digital Message Transfer Devices
DMPI	Designated Mean Point of Impact
DMPI Modify	Modify Desired Mean Point of Impact
DOD	Department of Defense
DPCP	Data Processor Computer Program

Acronym	Definition
DPG	Data Processor Group
DR	Data Radio
DSCS	Defense Satellite Communications System
DSSS	Direct Sequence Spread Spectrum
DTB	Data Transfer Block
DTC	Data Transfer Cartridge
DTDMA	Distributed Time Division Multiple Access
DTE	Data Terminal Equipment
DTI	Data Transfer Interrupt
DTM	Data Transfer Module
DTS	Data Terminal Set
DTSS	Data Terminal Set Simulator
DUI	Data Use Identifier
DUR	Data Update Request
	E
EA	Electronic Attack
EACS	Expeditionary Air Control Squadron
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
ECO	Electronic Combat Officer
ECW	Electronic Combat Wing
EDAC	Error Detection and Correction
EDM	Enhanced Data Mode
EFX	Expeditionary Force Experiment
EHF	Extremely High Frequency
EKMS	Electronic Key Management System
ELAG	Equipment Lag Time
ELINT	Electronic Intelligence
ELSG	Electronic Systems Group
ELSW	Electronic Systems Wing

Acronym	Definition
EMC	Electromagnetic Compatibility
EMCON	Emission Control
EMD	Engineering and Manufacturing Development
ENM	Enhanced Position Location and Reporting System Network Manager
EO/IR	Electro-Optical/Infrared
EOS	End-of-Slot
EPLRS	Enhanced Position Location and Reporting System
EPRE	Equipment Preamble Time
ES	Electronic Support;
	Electronic Surveillance;
	Spain
ESC	Electronic Systems Center
ESD	Exploitation Support Data
ESM	Electronic Support Measures
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
ETE	End-to-End
ETR	External Time Reference
EW	Electronic Warfare
EW/I	Electronic Warfare (EW) Intelligence
EW/ISR	EW Intelligence, Surveillance, and Reconnaissance
EWC	Electronic Warfare Coordinator
	F
F2T2EA	Find, Fix, Track, Target, Engage, and Assess
FAA	Federal Aviation Administration
FAAD	Forward Area Air Defense
FAC	Forward Air Controller
FAC-A	Forward Air Controller - Air
FAD	Functional Area Designator
Faker	Exercise Hostile

Acronym	Definition
FBCB2	Force XXI Battle Command, Brigade-and-Below
FCA	Frequency Clearance Agreement
FDL	Fighter Data Link
FDMA	Frequency Division Multiple Access
FEBA	Forward Edge of Battle Area
FEC	Full Expeditionary Capability
FFF	Form, Fit, and Function
FIDL	Fully Integrated Data Link
FIM	Functional Input Message
FIO	Fighter Data Link Input/Output
FJU	Forwarding JTIDS Unit
FJUA	Forwarding JTIDS Unit on Link 11
FJUAB	Forwarding JTIDS Unit on Link 11 and Link 11B
FJUB	Forwarding JTIDS Unit on Link 11B
FLOT	Forward Line of Own Troops
FLTSAT	Fleet Satellite
FMP	Fleet Modernization Program
FOAR	Frequency of Access Ranking
FOB	Forward Operating Base
FOIP	Fiber-Optic Interface Panel
FOM	Functional Output Message
FORSCOM	US Army Forces Command
FOV	Field of View
FPI	Field Presence Indicators
FR	France
FRI	Field Recurrence Indicator
FS	Fighter Squadron
FSatU	Forwarding Satellite Unit (UK)
FSK	Frequency Shift Keying
FT	Free Text

Acronym	Definition
FTI	Fixed Target Indicator
FTU	Formal Training Unit;
	Field Training Unit
FW	Fighter Wing
FWF	Fixed Word Format
	G
GAAC	Geographic Area Assignment Controller
GARS	Global Area Reference System
GAT	Gate Key
GCCS-J	Global Command and Control System with Link 16
GCIC	Global Cyberspace Integration Center
GCIC/RINIS	Global Communications and Information Division/Warfighting Networks, Integration and Standards Branch
GCS	Ground Control Station
GDOP	Geometric Dilution of Precision
GE	Germany, German
GHz	Gigahertz
GLONASS	Global Orbiting Navigation Satellite System
GM	Gateway Manager
GND	Ground Key
GNSS	Global Navigation Satellite System
GPC	General Purpose Computer
GPI	Group Presence Indicator
GPS	Global Positioning System
GR	Greece
GRI	Group Recurrence Indicator
GSM	Ground Station Module
GTACS	Ground Element of the Tactical Air Control System
GTS	Ground Tactical Data Link System

Acronym	Definition
	H
HAVCO	Have Complied
HDR	High Data Rate
HF	High Frequency
H-NAD	Hybrid – Network Access Delay
HPA	High Power Amplifier
HPAG	High Power Amplifier Group
HQ	Headquarters
HUR	High Update Rate
Hz	Hertz
	I
I/O	Input/Output
IBCS	Integrated Battlefield Control System
IBS	Information Broadcast Service
ICC	Information and Coordination Central (US Army)
ICD	Interface Control Document
ICO	Interface Control Officer
ICP	Interface Change Proposal
ICMP	Internet Control Message Protocol
ICT	Interface Control Team; Interface Control Technician
ID	Identification, Identity
IDL	Initialization Data Load
IDM	Improved Data Modem
IE	Initial Entry
IEJU	Initial Entry JTIDS Unit
IER	Information Exchange Requirement
IEUJ	Initial Entry JTIDS Unit
IFF	Identification Friend or Foe
IFF/SIF	Identification Friend or Foe/Selective Identification Feature

Acronym	Definition
IFTU	In-Flight Target Update
IGMP	Internet Group Multicast Protocol
IIU	Indirect Interface Unit
IJMS	Interim JTIDS Message Specification
IL	Intranet Layer
IMINT	Image Intelligence
IMTDS	Improved Multi-TDL Distribution System
Info	Information
INS	Inertial Navigation System
INT	Intelligence
IO	Information Operations
IOC	Initial Operating Capability
IOP	Interoperating Procedures
IP	Internet Protocol
IPF	Interference Protection Feature
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR	Infrared
IR5	Interim Release 5
IRAC	Interdepartment Radio Advisory Committee
IS	Intelligence Squadron
ISO	International Standards Organization
ISR	Intelligence, Surveillance, and Reconnaissance
ISRD	Intelligence, Surveillance, and Reconnaissance Division
ISRN	Internal System Reference Number
IT	Italy
ITS	Initialization Time Slots
IU	Interface Unit

Acronym	Definition
	J
JAC2C	Joint Aerospace Command and Control Course
JACAC	Joint Aerospace Computer Applications Course
JAOC	Joint Air and Space Operations Center
JAOP	Joint Air Operations Plan
JASAC	Joint Aerospace Systems Administrator Course
JASSM	Joint Air-to-Surface Standoff Missile
JCS	Joint Chiefs of Staff
JDAM	Joint Direct Attack Munition
JDS	JTIDS/MIDS Deconfliction Server
JFACC	Joint Forces Air Component Commander
JFC	Joint Forces Commander
JFCOM	Joint Forces Command
JFCOM-JID	Joint Forces Command - Joint Interoperability Division
JHMCS	Joint Helmet Mounted Cueing System
JIB	JICC in a Box
JICC	Joint Interface Control Cell
JICO	Joint Interface Control Officer
JIEO	Joint Information Engineering Organization
JITC	Joint Interoperability Test Command
JLENS	Joint Land Attack Cruise Missile Defense Elevated Netted Sensor (US Army)
JM	JTIDS Module (US Marine Corps)
JMPS	Joint Mission Planning System
JMTOP	Joint Multi-Tactical Data Link (TDL) Operating Procedures
JMTS	Joint Multi-TDL School
JNDA	Joint Network Design Aid
JNDL	Joint Tactical Information Distribution System (JTIDS/MIDS) Design Library
JNDT	Joint Network Design Team
JNETWORK	JNL Network Descriptions and Platform IDLs (USMTF SETID)

Acronym	Definition
JNL	Joint Tactical Information Distribution System (JTIDS/MIDS) Network Library
Joint STARS	Joint Surveillance Target Attack Radar System
JP	Japan
JPEG	Joint Photographic Experts Group
JREAP	Joint Range Extension Application Protocol
JSF	Joint Strike Force;
	Joint Strike Fighter
JSOW	Joint Standoff Weapon
JSSC	Joint Aerospace Operations Senior Staff Course
JSTARS	Joint Surveillance Target Attack Radar System
JSTNETS	Stacked Nets Set Identifier (USMTF SETID)
JSUG	JTIDS/MIDS Spectrum Users Guide
JTAC	Joint Terminal Attack Controller
JTAGS	Joint Tactical Ground Station (US Army)
JTAO	Joint Tactical Air Operations
JTEP	Joint Range Extension Transparent Multi-Platform Gateway Equipment Package
JTF	Joint Task Force
JTIDS	Joint Tactical Information Distribution System
JTIDS TIDP-TE	JTIDS Technical Interface Design Plan (Test Edition)
JTRS	Joint Tactical Radio System
JTTP	Joint Tactics, Techniques, and Procedures
JU	JTIDS Unit
JUDATA	JTIDS Unit Data (USMTF SETID)
	K
K	Effective Earth Radius
kb	Kilobit
kbps	Kilobits per Second
KEYMAT	Keying Material
kHz	Kilohertz

Acronym	Definition
KR	Republic of Korea
	L
LAK	Link 16 Alaska
LAT	Latitude
LANTIRN	Low-Altitude Navigation and Targeting Infrared, Night
LCC	Amphibious Command Ship (US Navy)
LCN	Logical Channel Number
LDDS	Link Data Distribution System
LFE	Large Force Exercise
LHA	Amphibious Assault Ship (US Navy)
LHD	Amphibious Landing Ship (US Navy)
	Landing Helicopter Dock
LMS™	Link Management System
LMS™-16	Link Management System – Link 16
LMS™-MT	Link 16 Management System-Multi-TDL
LNKXVI	Link 16
LOB	Line of Bearing
LOS	Line of Sight
LONG	Longitude
LPD	Landing Platform Dock (US Navy)
	Low Probability of Detection
LPI	Low Probability of Intercept
LTPO	Lower Tier Project Office
LTTI	Long Term Transmit Inhibit
LUM	Link 16 Unit Manager
LVT	Low Volume Terminal (MIDS)
LVT-1	MIDS Low Volume Terminal Type 1
LVT-2	MIDS Low Volume Terminal Type 2
LVT-3	MIDS Low Volume Terminal Type 3
LVT-4	Low Volume Terminal Type 4

Acronym	Definition
LVT-6	Low Volume Terminal Type 6
LVT-7	MIDS Low Volume Terminal Type 7
LVT-11	MIDS Low Volume Terminal Type 11
	M
m	Millisecond;
	Mandatory
MAC	Media Access Control
MAD	Mission Assignment Discrete
MAGTF	Marine Air Ground Task Force
MAPS	Mission Area Plans
MCD	Mission Commander Display
MCE	Modular Control Equipment
MCEB	US Military Communications Electronics Board
MCO	Major Combat Operations
MCS	Modular Control System
MDA	Missile Defense Agency
MDR	Medium Data Rate
MDTCI	Multiplex Data Transfer Complete Interrupt
MF	Medium Frequency
MHz	Megahertz
MIDS	Multifunctional Information Distribution System
MIDS LVT	MIDS Low-Volume Terminal
MIDSCO	MIDS consortium
MILSTAR	Military Strategic and Tactical Relay Satellite
MIL-STD	Military Standard
MIN IMP	Minimum Implementation
MLST3	Multiple Link Simulation Test and Training Tool
Mode S	Mode Select Beacon System
MOOTW	Military Operations Other Than War
MOS	MIDS-on-Ship (US Navy and US Marine Corps)

Acronym	Definition
MPCD	Multipurpose Cockpit Display
MR	Machine Receipt
ms	Milliseconds
MSCT	Multiple Source Correlator Tracker
MSD	Maintenance Support Device
MSEC	Message Security
Msg	Message
MSGID	Message Identifier (USMTF SETID)
MSIP	Multi-Stage Improvement Program
MT	Main Terminal
MTA	Multi-TDL Architecture
MTI	Moving Target Indicator
MTS	Marine Tactical System
MUX	Multiplex
	N
NATO	North Atlantic Treaty Organization
NATO NDF	NATO Network Design Facility
NAV	Navigation
NAVAID	Navigation Aid
NBDT	Net Busy Detect Time
NC	Navigation Controller
NCTSI	Navy Center for Tactical Systems Interoperability
NDA	Network Design Aid
NDF	Network Design Facility
NDL	Network Data Load
NECT	Net Entry Control Terminal
NETE	Net Entry Transmit Enable
NEW	Network Enabled Weapons
NFA	Notch Filter Assembly

Acronym	Definition
NGA	National Geospatial-Intelligence Agency
NI	Received but Not Interpreted
NICP	Network Interface Computer Program
NILE	NATO Improved Link Eleven
NIPG	Network Interface Program Group
NIPRNET	Non-classified Internet Protocol Router Network
NITFS	National Imagery Transmission Format Standard
NL	Netherlands
NLP	N Layer Pass-Through
nm	Nautical Miles
NMSC	Navy Marine Corps Spectrum Center
NO	Norway
NonC2	Non-Command and Control
NonC2 JU	Non-Command and Control JTIDS Unit
NPG	Network Participation Group
NRZ	Non-Return-to-Zero
NS	No Statement
ns	Nanosecond
NSA	National Security Agency
NSFS	Naval Surface Fire Support
NSS	National Security Systems
NT	NATO; Not Transmitted
NT/NI	Not Transmitted/Not Interpreted
NTDS	Naval Tactical Data System
NTIA	National Telecommunications and Information Administration
NTISR	Nontraditional Intelligence, Surveillance, and Reconnaissance
NTN	NATO Track Number
NTR	Network Time Reference

Acronym	Definition
NTRE	Network Time Reference, ETR-Enabled
	O
O	Optional
OCU	Operations Console Unit
OEF	Operation Enduring Freedom
OFP	Operational Flight Program
OIF	Operation Iraqi Freedom
OM	Operations Module
OMFTS	Operational Maneuvers From the Sea
OPEVAL	Operational Evaluation
OPF	Operational Flight Program
OPS	Operational Parameter Sets
OPFAC	Operational Facility
OPLAN	Operational Plan
OPORD	Operation Order
OPR	Office of Primary Responsibility
OPTASK LINK	Operational Tasking, Data Links (USMTF)
ORD	Operations Requirement Document
ORN	Other Reference Number
OSI	Open Systems Interconnection
OSP	Operational Special Project
OSW	Operation Southern Watch
OTAR	Over-the-Air Rekeying
	P
P	IJMS Position and Status
P2	Packed-2
P2DP	Packed-2 Double Pulse
P2SP	Packed-2 Single Pulse
P4	Packed-4
P4SP	Packed-4 Single Pulse

Acronym	Definition
PACAF	US Air Force, Pacific
Patriot BCP	Patriot Battery Command Post (US Army)
Patriot ICC	Patriot Information and Coordination Central (US Army)
PBA	Predictive Battlespace Awareness
PDS	Passive Detection System
PDT	Primary Designated Target
PDU	Protocol Data Unit
PERIOD	Period of Operation (USMTF SETID)
P-NAD	Prioritized – Network Access Delay
PFED	Precision Forward Entry Device
PGM	Precision-Guided Munitions
PJHI	Position Location Reporting System/JTIDS Hybrid Interface
PL	Poland;
	Physical Layer
PN	Pseudorandom Noise
POC	Point of Contact
POM	Program Objective Memorandum
PPLI	Precise Participant Location and Identification
PR	Position Reference
PRU	Primary User
PSK	Phase-Shift Keying
PT	Portugal
PTB	Plain Text Bus
PTP	Plain Text Processor
PTT	Push-to-Talk
PU	Participating Unit (Link 11)
PVM	Partitioned Variable Mode
	Q
Qp	Position Quality
Qpg	Geodetic Position Quality

Acronym	Definition
Qpr	Relative Position Quality
Qt	Time Quality
	R
R	Receive
R-S	Reed-Solomon
R/C	Receipt/Compliance
R/T	Receiver/Transmitter
R2	Reporting Responsibility
R-NAD	Random – Network Access Delay
RAF	Royal Air Force (UK)
RAOC	Regional Air Operations Center
RAP	Recognized Air Picture
RCN	Radar Controlled Track No Guidance
RCP	Radio Control Parameter
	Robust Communications Protocol
RCT	Radar Controlled Track
RDECOM	Research, Development, and Engineering Command (US Army)
RDF	Radio Direction Finding
RDM	Redistributed Messages
RE-NAD	Radio Embedded – Network Access Delay
REFPOINT	Reference Point
RELNAV	Relative Navigation
Reprom	Repromulgation
RF	Radio Frequency
RFA	Request for Frequency Assignment
RICO	Regional Interface Control Officer
RIMM	Removable Interchangeable Media Module
RINIS	Warfighting Networks, Integration and Standards Branch
RJ	Rivet Joint
RMA	Removable Media Assembly

Acronym	Definition
ROI	Regions of Interest
ROK	Republic of Korea
rpm	Revolutions per Minute
RPS	Remote Power Supply
RRN	Recurrence Rate Number
RS	Reconnaissance Squadron;
	Radio Silence;
	Radio Set
RSO	Remote Split Operations
RSR	Radar Service Request/Response
RTO	Range Training Officer
RTT	Round-Trip Timing
RTT-A	Round-Trip Timing Message - Addressed
RTT-B	Round-Trip Timing Message - Broadcast
RTT-I	Round-Trip Timing Message - Interrogation
RTT-R	Round-Trip Timing Message - Reply
RU	Reporting Unit (Link 11)
RW	Reconnaissance Wing
	S
SA	Situational Awareness
SACC	Support Arms Coordination Center
SACP	Stand-Alone Control Panel
SADL	Situation Awareness Data Link
SADO	Senior Air Defense Officer
SAM	Surface-to-Air Missile
SAMOC	Surface-to-Air Missile Operations Center
SAR	Synthetic Aperture Radar;
	Search and Rescue
SAT J	Satellite TADIL-J
SATCOM	Satellite Communications

Acronym	Definition
SAT J	Satellite Link 16
SatU	Satellite Unit (UK)
SATURN	Second Generation Anti-Jam Ultra High Frequency Radio for NATO
SCA	Software Communications Architecture
SCDL	Surveillance and Control Data Link
SD	Strategy Division
SDU	Secure Data Unit
SE	Sweden
SEAD	Suppression of Enemy Air Defense
SED	Software Engineering Directorate (US Army)
SETID	Set Identifier (USMTF)
SFSTRAT	Air Force Strategic Command
SHF	Super High Frequency
SHORAD	Short Range Air Defense
SICO	Sector Interface Control Officer
SICP	Subscriber Interface Computer Program
SIF	Selective Identification Feature
SIGINT	Signals Intelligence
SIMPLE	Standard Interface for Multiple Platform Link Evaluation
SINCGARS	Single Channel Ground-to-Air Radio System
SIPG	Subscriber Interface Program Group
SIPRNET	Secret Internet Protocol Router Network
SJU	Satellite JTIDS Unit
SKL	Simple Key Loader
SLAMRAAM	Surface Launched Advanced Medium Range Air-to-Air Missile (US Army)
SM&C	System Management and Control
SMO	Sensor Management Officer
SMP	Signal/Message Processor
SNC	Secondary Navigation Controller (Link 16); System Network Controller (Link 22)

Acronym	Definition
SOCAL	Southern California
SOF	Special Operations Forces
SP	Spain
SPC	Signal Processing Controller
SPI	Special Processing Indicator
SPINS	Air Tasking Order Special Instructions
SPO	System Program Office
SRN	System Reference Number
SS	Senior Scout
SSDS	Ship Self-Defense System (USN)
SSE	SADL Support Equipment
SST	Senior Surveillance Technician
STANAG	Standardization Agreement (NATO)
STD	Standard
STD-DP	Standard Double Pulse
STDL	Satellite Tactical Data Link (UK)
S-TADIL J	Satellite Link 16 (USN)
STE	Secure Telephone Equipment
STGU	Satellite TDL Gateway Unit
STN	Source Track Number
STRN	System Time Reference Network
STU	Secure Telephone Unit
SU	Secondary User
SWA	Southwest Asia
	T
T	Transmit; IJMS Limited Track
T&E	Test and Evaluation
T/R	Transmit/Receive
TACAN	Tactical Air Navigation

Acronym	Definition
TACC	Tactical Air Command Center (US Marine Corps);
	Tanker Airlift Control Center
TACOPDAT	Tactical Operations Data
TACP	Tactical Air Control Party
TACP-CASS	Tactical Air Control Party – Close Air Support System
TACS	Tactical Air Control System
TAD	Theater Air Defense
TAOC	Tactical Air Operations Center
TAOM	Tactical Air Operations Module
TBD	To Be Determined
TBM	Theater Ballistic Missile
TBMCS	Theater Battle Management Core Systems
TCAS	Traffic Collision Avoidance System
TCG	Tactical Communications Group
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCS	Tactical Command System
TCT	Time Critical Targeting
TD	Tabular Display
TDC	Track Data Coordinator
TDL	Tactical Data Link
TDL SPO	Tactical Data Links System Program Office
TDMA	Time Division Multiple Access
TDN	Tactical Data Network
TDS	Tactical Data System
TECHEVAL	Technical Evaluation
TEK	Traffic Encryption Key
TES	Test and Evaluation Squadron
THAAD	Terminal High Altitude Area Defense
TIDP-TE	Technical Interface Design Plan (Test Edition)

Acronym	Definition
TIG	Tactical Information Gateway
TIGER	Tactical Data Link Integration Exerciser
TIM	Terminal Input Message
TIO	Tailored Input/Output
TJRS	TDL J Requirements Specification
TJU	TDL J Upgrade (JSTARS)
TLDHS	Target Location Designation Handoff System
TMD	Theatre Missile Defense
TMPG	Transparent Multi-Platform Gateway
TN	Track Number
TNR	Track Number Reference
TOA	Time of Arrival
TOAi	TOA of the Interrogation
TOAr	TOA of the Reply
TOD	Time of Day
TOM	Terminal Output Message
TPA	Track Production Area
TQ	Track Quality
TR	Turkey
TRI-TAC	Tri-Service Tactical Communications
TS	Test Squadron
TSA	Time Slot Assignment
TSB	Time Slot Block
TSDF	Time Slot Duty Factor
TSEC	Transmission Security
TSR	Time Slot Reallocation
TST	Time-Sensitive Target; Time-Sensitive Targeting
TTP	Tactics, Techniques, and Procedures
TW	Threat Warning

Acronym	Definition
	U
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UFN	Until Further Notice
UFO	Ultrahigh Frequency Follow-On
UHF	Ultrahigh Frequency
UK	United Kingdom
UNCLAS	Unclassified
US	United States
US&P	United States and Possessions
USA	United States of America; United States Army
USAF	United States Air Force
USAFE	United States Air Force, Europe
USJFCOM	United States Joint Forces Command
USMC	United States Marine Corps
USMTF	United States Message Text Format
USN	United States Navy
USNO	United States Naval Observatory
URN	Unit Reference Number
USW	Undersea Warfare
UT	Universal Time
UTC	Coordinated Universal Time
	V
VACAPES	Virginia Capes
VHF	Very High Frequency
VMF	Variable Message Format
Vocoder	Voice Encoder/Decoder

Acronym	Definition
VOR	Very High Frequency Omnidirectional Range
VORTAC	Very High Frequency Omnidirectional Range - Tactical Air Navigation
VSD	Vertical Situation Display
	W
WAS	Wide Area Surveillance
WFHQ	Warfighting Headquarters
WG	Wing
WGS 84	World Geodetic Survey 1984
WIFT	Weapon In-flight Track
WILCO	Will Comply
WNW	Wideband Networking Waveform
WPN	Weapon
WSC	Weapons System Coordinator
WSO	Weapon System Officer
WX	Weather
	X, Y, Z
XML	Extensible Markup Language
XNP	Exchange Network Parameters
XOR	Exclusive Or
XOR'd	Exclusively-Or'd

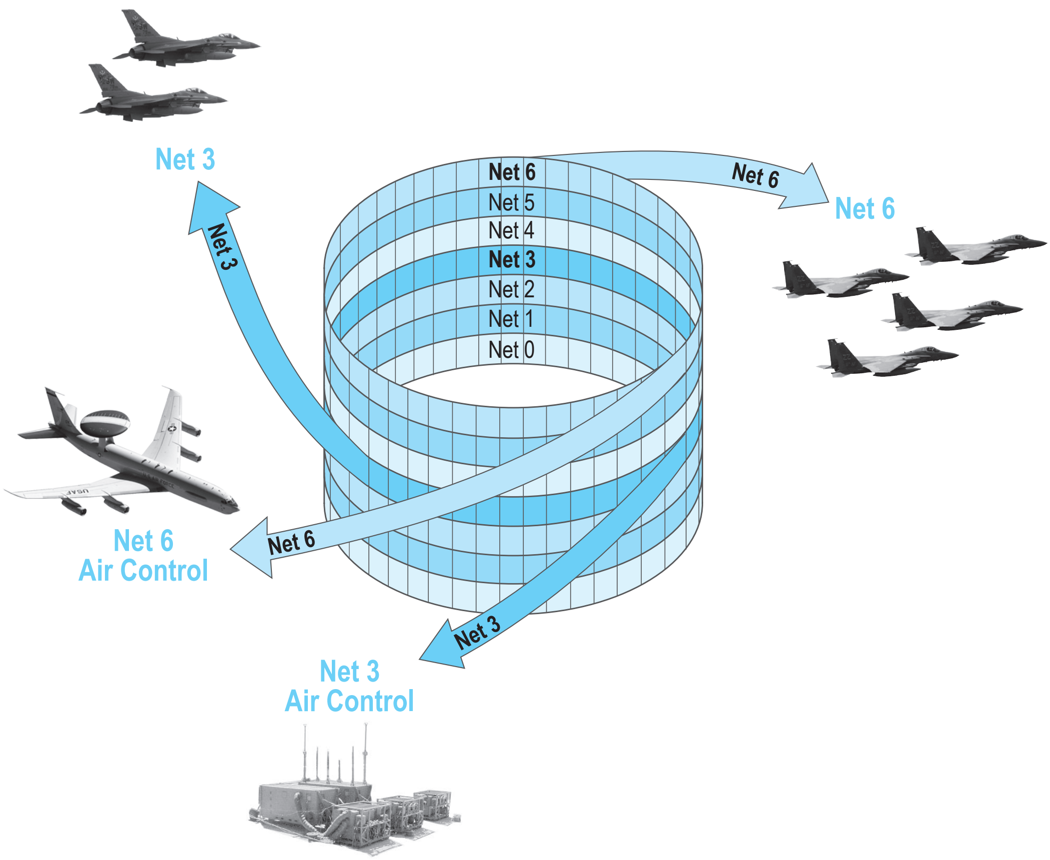
NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com

Appendix C

Glossary



The following terms have been used or defined in this guidebook. Terms in *italics* are cross-references to other terms in this Glossary.

Access Rate The assigned rate that determines the frequency of a Link 16 terminal's *contention* access to an assigned time-slot block.

Active Synchronization The Link 16 terminal's procedure for transmitting *round-trip timing* messages to refine and maintain its estimate of system time.

Address A number applied to an *Interface Unit* to associate information and directives with other Interface Units interface units for digital and voice communication on Link 16 and on Link 11.

Air Control The *Network Participation Group* (NPG 9) that provides the means for *command and control* (C2) Link 16 units (JUs) to control *nonC2* JUs.

Antijam Margin The degree of protection against jamming provided by several characteristics inherent in a communications architecture. Factors contributing to the antijam margin of the Link 16 signal include error-correction encoding, pseudorandom noise, transmission redundancy, *jitter*, and *frequency hopping*.

Automatic Acknowledgement A machine verification function whereby a terminal that receives a message addressed to it retransmits a copy of that message back to the source during a later *time slot*, verifying the receipt of the original message.

Backlink An adjective describing the *time slots* that are dedicated to the transmitted responses of controlled aircraft. It also applies to aircraft equipped with Link 16 that are capable of transmitting them.

Bailout Indicator A field in an AIR PPLI indicating a J3.1 Emergency Point message.

Bilingual The ability of certain JTIDS terminals to process both *IJMS* and JTIDS messages.

Bit A binary digit. A bit has only two possible values: zero and one.

Blind Relay A *relay* in which a Link 16 relaying unit is initialized with the correct *transmission security* (TSEC) cryptovariable for receiving and retransmitting messages, but is initialized with a different *message security* (MSEC) cryptovariable, which prevents it from being able to decrypt the messages it relays.

Buffer An area in computer memory that is reserved for the temporary storage of data. Tactical data systems reserve buffers for input and output.

Carrier An electromagnetic wave or alternating current whose modulations are used as signals in radio transmissions.

Chipping Sequence A transformation, produced by *cyclic code-shift keying*, of the interleaved symbols of message codewords for transmission. This transformation produces for each 5-bit symbol a sequence of 32 bits, or chips.

Change Data Order (CDO) A Track Management order (J7.0) from a designated authority that changes the environment and identification.

Coarse Synchronization The initial procedure of Link 16 net entry, during which a Link 16 unit attempts to receive an Initial Entry message without adjusting its internal clock for the propagation time of the message. During this synchronization state, the Link 16 terminal can receive and process messages and achieve fine synchronization.

Codeword A sequence consisting of 31 5-bit symbols that correspond to a sequence of 155 *Reed-Solomon*-encoded bits, which in turn correspond to a 75-bit data word to which 80 bits have been added for error detection and correction.

Combat Override All *interference protection features* are overridden. This should be used only when continued operation is imperative - in spite of a known IPF failure, and realizing that navigation systems will probably be jammed.

Command and Control (C2) Unit A platform equipped to direct the activities of other Link 16 units (JUs) over Link 16.

Common Track Number (CTN) The track number held by all *Interface Units* for a contact and used in voice and other communications to identify it.

Common Variable Mode A Link 16 communications security (COMSEC) mode in which identical cryptovariable logical labels are assigned to *message security* (MSEC) and *transmission security* (TSEC).

Communication Mode A setting on the Link 16 terminal that controls the degree of *message security* (MSEC) and *transmission security* (TSEC) employed. This can include slot usage and whether *frequency hopping* is employed. Three communication modes are recognized by NATO and the United States Armed Services.

Concurrent Interface Unit (CIU) A unit participating concurrently, but not as a *forwarding unit*, on both Link 11 and Link 16.

Concurrent Operations (CONCOPS) Operations by a single unit on both Link 16 and Link 11 at the same time. The unit so operating does not forward data.

Conditional Relay A *relay* mode in which Link 16 units (JUs) selectively activate or deactivate their relay function based on which JU can provide most efficient coverage.

Contention Access The assignment of *time slots* to a group of units for transmission purposes, such that any or all of the units may be transmitting simultaneously during the assigned time slots. However, each JU will transmit at a specified rate in the time slot block by selecting time slots for transmission pseudorandomly. Receipt is determined based on proximity of the transmitting unit.

Continuation Word The final portion of a *fixed format* message. It contains 70 data bits, 4 parity bits, and 1 spare bit.

Continuous Phase-Shift Modulation (CPSM) The process of modulating the frequency of a carrier in such a way that the phase remains continuous.

Controlled (nonC2) Unit	A platform equipped to accept the direction of its activities over Link 16 by a *command and control* (C2) JU.
Cryptonet (Crypto Isolated)	A communications net whose participants are isolated from other participants by the use of a separate encryption key.
Cryptoperiod Designator (CPD)	A number, either 0 or 1, which designates to a Link 16 terminal which *cryptovariable* of a today/tomorrow pair to use when encrypting and decrypting Link 16 transmissions.
Cryptovariable (CV)	A binary key used by the Link 16 terminal to encrypt and decrypt data or transmissions. *Cryptovariables* are assigned during network design and are loaded into the *Secure Data Unit* during terminal initialization.
Cryptovariable Logic Label (CVLL)	A label that applies to a *cryptovariable* in a Link 16 network. The CVLL is a number between 0 and 127.
Current CPD	Current cryptoperiod designation for any day is either 0 or 1. It is established on the date in which the terminal is initialized.
Cyclic Code Shift Keying (CCSK)	A method of encoding and decoding data using a class of codes that is particularly effective in detecting and correcting multiple errors. For Link 16, cyclic code shift keying is applied to a five-bit symbol to produce a 32-bit *chipping sequence* by shifting leftward the bits of a 32-bit starting sequence number by a number of places that corresponds to the numerical value of the symbol.
Data Field Identifier (DFI)	A category of data whose specification includes one or more *Data Use Identifier* (DUI) specifications. Each DUI's class of data must fall within the bounds of the DFI category.
Data Filter	A technique for including or excluding data of certain types for transmission and/or reception.

Data Forwarding	The process of receiving data on one digital data link and outputting the data, using the proper format and link protocols, to another type of digital data link. In the process, a message received on one link is translated to an appropriate message on another link. Data forwarding is accomplished by the selected forwarding units simultaneously participating on more than one type of data link. The data that is forwarded is based on the data received and is not dependent upon the local system data of the data forwarding unit or its implementation of the received message or the forwarded message. CRCs and Navy ships can be utilized as data forwarders.
Data Link Reference Point (DLRP)	A fixed geographic reference point, specified by appropriate authority, from which Link 11 participating units calculate the relative positions of own unit and local tracks, and from which all tracks are reported over this link. The DLRP is the origin of the force X/Y-grid.
Data Mile	A unit of distance used in tactical data link messages that is equal to 6000 feet.
Data Silence	A setting on the Link 16 terminal that inhibits the transmission of data. Voice and TACAN transmissions, however, remain enabled. A Link 16 unit (JU) functioning in data silence becomes a Secondary User on the Link 16 network.
Data Transfer Blocks	A message structure defined for the exchange of information between the Link 16 terminal's *Subscriber Interface Computer Program* (SICP) and its *Network Interface Computer Program* (NICP).
Data Use Identifier (DUI)	A JTIDS data element (class of data). The DUI specification determines the name and permitted contents of each message field to which the DUI is assigned. (See DFI, above.)
Dedicated Access	The assignment of *time slots* to a uniquely identified unit for transmission purposes, such that only that unit transmits during the assigned time slots.

Distance Measuring Equipment (DME)	A civilian system of navigation, used for measuring distance, which consists of an airborne interrogator and a ground transponder.
Donated Time Slot	A *time slot*, assigned to a particular Link 16 unit (JU), which the unit temporarily donates to the receiver of a message that requires an automatic acknowledgement, and during which the receiving JU transmits its required response.
Double Buffering	Alternately switching back and forth between two buffers.
Double-pulse	A Link 16 transmission format for redundantly conveying message data, employing two *pulse symbol packets* that are transmitted on two different carrier frequencies.
Drop Track Report	Manually dropping any local track (J7.0) when it can be no longer be supported or is no longer of interest.
Effective Earth Radius	A modification to the radius of the earth that allows the propagation path of radio waves uniformly bent by the atmosphere to be treated as though it were straight-line propagation. The ratio of the effective earth radius to the true earth radius, which is denoted by K, can range between 0.6 and 5.0. In temperate climates, its average value is approximately 1.33.
Electronic Warfare (EW)	(1) Generally, the use of radiated electromagnetic energy to passively establish the location, course, and speed of another platform. (2) The Link 16 Network Participation Group (NPG 10) that supports these functions by conveying orders and parametric data.
Engagement Coordination	NPG that is used solely by the U.S. Army for inter-Army coordination of engagements by Patriot and THAAD units.
Emergency Report	Alert that indicates the existence of a life-threatening condition that requires immediate action or assistance.

Epoch	The period of longest duration in the *time division multiple access* (TDMA) structure of the Link 16 architecture. A single day consists of 112.5 epochs. One epoch occupies 12.8 minutes. Epochs are subdivided into 64 *frames* and three *sets* of *time slots*. An epoch contains 98,304 time slots, which are its smallest division of time.
Error Correction Encoding	The JTIDS forward error correction encoding function that utilizes *Reed-Solomon encoding* of data.
Error Detection Encoding	An encoding process that allows the detection of a residual message error condition after the error correction function (*Reed-Solomon*) is executed.
Exercise Status Order	Directs all IUs to cease reporting tracks as Exercise tracks.
Extended Range	The longer of two range options for a Link 16 Terminal, providing a line-of-sight range capability of 0-500 nautical miles with respect to the allocated propagation for message transmission.
Extension Word	The second portion of a *fixed format* message. It contains 70 data bits, 4 parity bits, and 1 spare bit.
Fighter-To-Fighter Target Sorting	A *Network Participation Group* (NPG 19) used by *nonC2* units, such as fighter aircraft, to exchange radar, sensor, and target data.
Fighter Data Link (FDL)	Term used when referring to the Link 16 terminals employed by F15s. It is a member of the Multifunctional Information Distribution System (MIDS) family of Low Volume Terminals (LVTs), specifically LVT-3.
Fine Synchronization	Part of a procedure for entering a Link 16 network, during which a Link 16 unit (JU) adjusts its internal clock to correct for propagation time. Fine synchronization must be achieved in order to participate on the network. A Link 16 terminal may employ either *active synchronization* or *passive synchronization* to achieve this state.

Fixed Format	A Link 16 *message format* consisting of multiple words, each containing 70 data bits, 4 parity bits, and 1 spare bit. Fixed format messages consist of an initial word, and may be followed by one or more extension words, and one or more continuation words.
Flood Relay	A network design strategy in which every Link 16 unit (JU), including the originator, acts as a *relay* by retransmitting messages that it receives.
Force Tell Reports	Alert that indicates that a condition exists which, although it does not meet the criteria for an Emergency Alert, is sufficiently important to ensure that all C2 IUs are aware of the track's presence.
Forwarding JTIDS Unit (FJU)	A network role assigned to a Link 16 unit (JU) that will forward data between tactical data links during a multilink operation. An FJU that translates and forwards data between *Interface Units* (IUs) using J-series and M-series messages. An FJU is either an FJUA (TDL A), FJUB (TDL B), or FJUAB.
Frame	A period of time in the Link 16 *time division multiple access* (TDMA) architecture equal to one sixty-fourth of one epoch. A frame is 12 seconds in duration and contains 1,536 time slots.
Free Text	A type of Link 16 message structure that uses all bits for data. A bit-oriented message whose information bits may be used to represent digitized voice, teletype, and other forms of Free Text information.
Frequency	The number of cycles a wave completes during one second.
Frequency Hopping	A transmission technique in which the carrier frequency is changed for each pulse of a pulsed signal. For Link 16, 51 different frequencies are used, and the duration of each pulse is 6.4-microseconds. The pseudorandom assignment of frequency establishes a hopping pattern and is part of the transmission encryption process.

Frequency Modulation (FM)	The transmission technique that modulates or shifts the carrier frequency of the signal to convey information.
Frequency Shift Keying	A method of encoding data by shifting a carrier frequency between two predetermined values.
Functional Input Messages (FIMs)	Messages that transfer data from a host computer to the MIDS terminal over a specified multiplex data bus to the host computer.
Functional Output Messages (FOMs)	Messages that transfer data over a specified multiplex data bus from the MIDS terminal to a host computer.
Geodetic Grid	An earth-based coordinate system used by Link 16 units (JUs) to report positions by specifying latitude, longitude, and altitude. The geodetic grid is always active.
Geodetic Position Quality (Qpg)	A measure of the quality of a Link 16 terminals' geodetic position reported in the terminal's Position and Status Reports. Geodetic Position Quality is reported as an integer from 0-15, where the higher numbers correspond to the higher qualities.
Gigahertz (GHz)	A measure of frequency equal to a billion hertz.
Global Memory	An area in the Link 16 terminal's memory that is reserved for the sharing and exchange of information among the multiple processors within the terminal.
Handover	A procedure for passing the control of an aircraft from one controller to another.
Header	The leading bits of each message are coded as a (16, 7) *Reed-Solomon codeword* that provides 35 bits of information and 45 bits of associated forward error correction code.
Hertz	A unit used to measure frequency. One hertz equals one vibration, or cycle, per second.
High TN Block	A block of contiguous, assignable Link 16 track numbers, including the octal track numbers 10000 through 77777 and the alphanumeric track numbers 0A000 through ZZ777. No track numbers in this block correspond to Link 11 track numbers.

Housekeeping Words	Blocks of information that are exchanged, in either direction, between the JTIDS terminal's Subscriber Interface Computer Program (SICP) and its Network Interface Computer Program (NICP). Their primary purpose is to convey information required for the encryption and decryption of the signal.
Identification Friend or Foe (IFF)	An interrogator, which can be either ground-based (with the Air Traffic Control Radar Beacon System) or airborne, that transmits pulses and receives replies containing the responding aircraft's identity, altitude, and other essential information.
Imagery	*Network Participation Group* 11, for image files.
Indirect Precise Participant Location and Identification (Indirect PPLI)	The *Network Participation Group* (NPG 14) on which USN Forwarding Link 16 units (FJUs) transmit to other Link 16 units (JUs) the Precise Participant Location and Identification messages of units not participating on the Link 16 network.
Initial Entry	The procedure by which a subscriber terminal becomes a system participant initially and may achieve *coarse synchronization* with system time. Initial Entry is also one of the *Network Participation Groups* (NPG 1).
Initial Entry JTIDS Unit (IEJU)	A Link 16 unit (JU) that transmits *Initial Entry messages* for the purpose of assisting other units in achieving synchronization with, and entry into, a Link 16 network.
Initial Entry Message	A Link 16 message transmitted by a Link 16 unit (JU) to facilitate the entry of other units into the Link 16 network.
Initial Word	The first portion of a *fixed format* message. It contains 70 data bits, 4 parity bits, and 1 spare bit.
Interface Unit (IU)	A JU on Link 16, Participating Unit (PU) on — Link 11, or Reporting Unit (RU) on — Link 11B, which is communicating directly or indirectly on the interface.

Intelligence The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas, or forces of tactical interest, gained by means other than radar, sonar, or electronic support measures (ESM).

Interference Protection Feature (IPF) An automatic function of the Link 16 terminal that monitors its own transmissions and disables the terminal whenever it detects that they are in any way improper. Three settings of IPF are available on the terminal: normal, exercise, and *combat override*.

Interim JTIDS Message Specification (IJMS) Messages An early implementation of messages exchanged between the Class-1 JTIDS terminals. The Air Force Class 2 terminals retain both an IJMS and JTIDS message capability, and can translate between them. NPGs 30 and 31 are provided for the exchange of IJMS messages.

Interleave To arrange in an alternating sequence or order. Time slots of the three sets (— A, B, and C) — are interleaved, as are the transmission symbols of the message and data codewords.

Jamming The process of obstructing, or rendering unintelligible, a transmitted message by sending out interfering signals or messages.

Jitter The first portion of the *time slot*, during which the transmitter is silent. Jitter may be either applied or not applied within a time slot and when applied, it may be of varying duration. Its purpose is to render the actual start time of the data transmission impossible to predict.

Joint Precise Participant Location and Identification A *Network Participation Group* (NPG 27) in which identification and location information is exchanged during Joint operations.

Joint Tactical Information Distribution System (JTIDS) — (1) The method, hardware, and software by which tactical information is disseminated over Link 16. (2) Commonly, the JTIDS terminal, which modulates, transmits, receives, and demodulates messages for a participant in a Link 16 network.

JTIDS Net — One of 127 time division structures comprising a Link 16 network. Each net consists of a continuous stream of time intervals (*time slots*) with 98,304 times slots per 12.8-minute epoch, during which digital data whose signal characteristics are determined by a cryptographic variable in conjunction with a unique net number are distributed.

JTIDS Unit (JU) — A platform equipped to participate in Link 16 communications. A JU is either a *Command and Control* (C2) unit or a controlled (*nonC2*) unit. JTIDS Unit (JU) is synonymous with Link 16 unit.

J-series Message — The fixed format messages, containing tactical data and commands, which are used to exchange information over Link 16. These messages adhere to the standards defined in MIL-STD-6016C, Change 1.6016B.

Kilohertz (kHz) — A measure of frequency equal to 1,000 hertz.

Lx Band — A portion of the RF UHF band stretching from 390 MHz to 1.550 GHz. Link 16 operates within this band on frequencies between 960 and 1216 MHz.

Line of Sight (LOS) — The direct line in which radio waves travel, without bending over mountains or the curvature of the earth.

Link 11 — The tactical digital data link protocol, formerly known as TADIL A, specified by MIL-STD-6011, for communications among a multiple number of units. Its netted communications are characterized by a round-robin, designated Roll Call, in which every participant reports in turn when requested to do so by one unit, designated the Net Control Station. The messages exchanged over Link 11, known as M-series messages, adhere to the Link 11 message standard.

Link 11B	The tactical digital data link protocol, formerly known as TADIL B, specified by MIL-STD-6011, for point-to-point communication over landline between two units. The messages over Link 11B, known as M-series messages, adhere to the Link 11 message standard.
Link 16	The secure, jam-resistant, high-capacity, nodeless tactical digital data link, formerly known as TADIL J, which utilizes the JTIDS/MIDS terminal and its *time division multiple access* (TDMA) architecture for multinetted communications. The information exchanged on this link is conveyed in the J-series messages, which conform to the operational specifications contained in MIL-STD-6016 Series.
Link 16 Network	The Link 16 structure (usable only with Mode 1 communications) having a total usable capacity of 98,304 *time slots* per *epoch*, per *net*, with a maximum number of nets being 127. All nets are synchronized so that each time slot of each net is time-coincident with the corresponding time slot (same net and number) of every other net.
Link 22	The tactical digital data link protocol specified for netted communications among multiple nets, each consisting of multiple numbers of units. Its TDL-J-series messages use the Link 16 data dictionary. Commonly referred to as NATO Improved Link Eleven, or NILE.
Long-Term Transmit Inhibit (LTTI)	A setting on the Link 16 terminal that inhibits all radio transmissions, including voice and TACAN as well as data.
Low Probability of Intercept (LPI)	A characteristic of the *frequency-hopping* technique that makes the Link-16 signal extremely difficult to locate.
Low TN block	The block of assignable Link 16 track numbers that range from 0 to 07776. The track numbers in this block correspond to all Link 11 assignable track numbers.
M-series Messages	Messages transmitted over Link 11 and Link 11B between participating units.

Machine Receipt (MR) A Link 16 message, automatically transmitted by a Link 16 terminal, which acknowledges the receipt of certain types of other messages.

Main Net The default net in a network design on which housekeeping and overhead functions are preformed.

Megahertz (MHz) A measure of frequency equal to 1 million hertz.

Message Formats For a given tactical data link, the set of sequences of fields, composed of prescribed numbers of bits, that may be encoded into prescribed sets of values to convey specific information. The values of their prescribed data items are supplied in the message specification for the given tactical data link.

Message Header That portion of a Link 16 message, consisting of a single codeword, that specifies the format of the message data, whether the data is encoded, which *packing structure* has been used for its transmission, the *Secure Data Unit* serial number, and the track number of the Link 16 terminal that originated the message.

Message Security (MSEC) A cryptovariable that is used by a Link 16 unit (JU) to encrypt message data for transmission on Link 16.

Message Standard A set of protocols consisting of rules, procedures, formats, data element definitions, or other conventions for information exchange and related interactions agreed upon between cooperating systems to ensure interoperability.

Microsecond (µs) One one-millionth of a second.

Millisecond (ms) One one-thousandth of a second.

Mission Management The *Network Participation Group* (NPG 8) that provides a means for coordinating weapons and engagements for the Battle Group.

Mode 1 Communication	Mode 1 Link 16 transmissions consist of a sequence of wide-band transmission symbol packets (*single-pulse*, 13-microsecond packets and *double-pulse*, 26-microsecond packets), the pulses of which are formed by *continuous phase shift modulation* (CPSM) of the carrier frequency. The signal processing required to transform baseband data to the JTIDS waveforms for transmission includes baseband data encryption, forward error correction encoding, error detection encoding, *cyclic code shift keying* (CCSK) encoding, data symbol *interleaving*, and the selection of a variable start time.
Mode 2 Communication	Mode 2 Link 16 transmissions are identical to Mode 1, except that Mode 2 operates in the narrow-band mode.
Mode 4 Communication	Mode 4 Link 16 transmissions have waveform characteristics identical to Mode 2, except that Mode 4 does not employ baseband data encryption signal processing.
Multifunctional Information Distribution System (MIDS)	A terminal that modulates, transmits, receives, and demodulates messages for a participation in a Link 16 network. Its predecessor is the Joint Tactical Information Distribution System (JTIDS) terminal.
Multiplex (MUX) Cycle	Exchange of input and output messages that takes place cyclically.
Mux Data Transfer Complete Interrupt (MDTCI)	An interrupt triggered by the host, notifying the terminal that it has finished reading data from the terminal.
Nautical Mile (nm)	A unit of distance used in air and sea navigation based on the length of a minute of arc of a great circle of the earth. The unit used by the U.S. is equal to 6076.115 feet, or approximately 1.15 statute miles.

Navigation Controller (NC)	A *network role*, assigned to a mobile unit that acts as the reference unit for the grid. The NC establishes the origin and north orientation of the U, V relative grid for the *Relative Navigation* function. By definition, the NC's Position Quality is 15 and its Azimuth Quality is 7, the maximum values.
Net	A group of participants exchanging messages among themselves. For Link-16, this is one of the 127 possible net numbers. (0-126).
Needline Participation Group	A functional grouping of Link 16 message formats that supports a particular type of messages used by the United States Army. Needline participation groups constitute a subclass of *Network Participation Groups*. Netted subscribers compiled without regard to the specific messages they exchange with each other.
Net Entry Control Terminal (NECT)	A *network role* that propagates the system time to units beyond line of sight of the *Network Time Reference* by transmitting the *Initial Entry message* in *time slot* A-0-6. By definition, an NECT is not a Network Time Reference (NTR). Also called *Initial Entry JTIDS Unit* (IEJU).
Network Interface Computer Program (NICP)	A software program, residing within the Link 16 terminal, which has overall responsibility for communications with the RF network.
Network Management	The *Network Participation Group* (NPG 4) during which commands are transmitted for managing the operation of a particular Link 16 network.
Network Management Messages	The messages transmitted in *Network Participation Group* (NPG 4), consisting of commands that are transmitted for managing the operation of a particular Link-16 network.
Network Participation Group (NPG)	A unique list of applicable messages used to support an agreed-upon technical function without regard to subscriber identities. This list is a means of transmitting a common set of messages to all interested users.

Network Role	A function assigned, on the basis of platform capabilities and expected platform position, to a *command and control* (C2) Link 16 unit (JU), either by initialization or by operator entry. Network roles support network synchronization, navigation, and interlink operations.
Network Time Reference (NTR)	A *network role* assigned uniquely to a single *command and control* (C2) unit. The NTR's clock establishes the timing for the network and is the reference with which all other units must achieve and maintain fine synchronization to remain in the network. By definition, the NTR's Time Quality is 15, the maximum value.
Normal Mode	The standard mode of terminal operations with respect to receipt and transmission of messages.
Normal Range	The shorter of two range options for a Link 16 terminal, providing a line-of-sight coverage capability of 0-300 nautical miles with respect to the allocated propagation for message transmission.
No Statement Word	A data word (J31.7I) supplied by the Link 16 terminal when there is an insufficient number of words that are required to complete a message packing format for transmission.
OPTASK LINK	That portion of the Operation Tasking Order that applies to tactical data link communications involving participating platforms.
Over-the-Air Rekeying (OTAR)	Allows a function controlled by a C2 unit that manages terminal rekeying over the air J-Messages.
Passive Synchronization	A secondary method of net entry, employed by Link 16 units (JUs) in radio silence, during which fine synchronization is achieved and maintained by passively monitoring the messages on the Precise Participant Location and Identification Network Participation Groups.
Packing Structure	The grouping of Link 16 message words, of any format, into a Link 16 transmission. These groups can contain 3 words, 6 words, or 12 words.

Packed-2 Format A message consisting of six words that may be transmitted redundantly within a single *time slot*. Nonredundant transmission is referred to as Packed-2 *Single-Pulse* (P2SP) format, and redundant transmission is referred to as Packed-2 *Double-Pulse* (P2DP) format.

Packed-4 Format A message consisting of 12 words that are transmitted within a single *time slot*. Its nonredundant transmission is also referred to as Packed-4 *Single-Pulse* (P4SP) format.

Paired Slot Relay A type of *relay* in which the time slot of the original transmission is paired with a second time slot after a specified delay for the retransmission of the message by the relaying unit.

Parallel Interface A computer interface in which multiple bits are transferred in parallel, at the same time, along separate lines.

Parametric Data For electronic warfare (EW), the unprocessed data that is collected by sensors, which includes lines of bearing, pulse width, pulse repetition frequency, antenna scan period, etc. A *Network Participation Group* (NPG 10) is reserved for the transmission of this parametric data before it is evaluated by a tactical data system.

Partitioned Variable Mode A Link 16 communications security (COMSEC) mode in which different *cryptovariable logic labels* are assigned to *message security* (MSEC) and *transmission security* (TSEC).

Phase-Coherent Binary Frequency Shift Keying
The application of two frequencies whose periods differ by precisely one-half wavelength during a specified interval to a carrier, such that the higher frequency represents one value or condition and the lower frequency represents its opposite. For Link 16, the difference in frequencies represents a change in the value of contiguous constituents of chipping sequences, rather than the absolute value of any constituent. The higher frequency is applied whenever a constituent differs from the previous constituent, and the lower value is applied whenever they are identical. For Link 16, the period over which the requisite frequencies are maintained is precisely 200 nanoseconds.

P-messages
A designation for *Interim JTIDS Message Specification* (IJMS) Position and Status messages transmitted on the *Network Participation Group* (NPG 30) reserved for this purpose.

Platform Status Messages
The J13.x messages, which provide additional unit information. These are periodically transmitted in the unit's PPLI time slot.

Pool
One or more time slot blocks that can be used to satisfy a particular functional requirement, or the total JTIDS capacity that can be divided into pools to satisfy all functional requirements.

Position Quality (Qp)
A value between 0 and 15 that indicates the accuracy with which a Link 16 unit (JU) fixes its own position. Two Position Qualities are maintained: the *Geodetic Position Quality* (Qpg) and the Relative Position Quality (Qpr). When the geodetic grid is operational, the maximum value is assigned to JUs acting as *Position References*. When the relative grid is operational, the maximum value is assigned to the JU acting as *Navigation Controller*. The maximum value, 15, indicates a positional accuracy of within 50 feet.

Position Reference (PR)	A network role that is always assigned to a well-surveyed, stationary site whose *Position Quality* is 15, the maximum value. This role is not required and may not be assigned in every network.
Positive Identification	The means of identifying a Link 16 unit (JU), during *Network Participation Groups* dedicated to *Precise Position Location and Identification* information, which consists of a unique JU number, Identification Friend or Foe (IFF) codes, platform type, and information on the platform's movement and link activity.
Precise Participant Location and Identification (PPLI)	Two *Network Participation Groups* (NPG 5 and 6) during which Link 16 units (JUs) transmit their precise location, identification, fuel and weapons status, and communications data. Controlling units use NPG 6, PPLI and Status, Pool B; controlled units such as fighter aircraft use NPG 5, PPLI and Status, Pool A, to transmit more rapid position updates.
Primary User (PRU)	A network role assigned to every Link 16 unit (JU) that is actively maintaining synchronization with its Link 16 network. The *Network Time Reference*, as the unit that establishes the timing of the network, does not need to maintain synchronization and is therefore not considered a primary user.
Propagation	The fifth and final portion of the *time slot*, during which no pulses are transmitted and the signal is allowed to propagate.
Pseudorandom Noise	A 32-bit sequence which, when exclusively OR'd bitwise with a 32-bit *chipping sequence*, produces another 32-chip sequence, the *transmission symbol*. The 32-chip pseudorandom noise sequence, which is determined by the *transmission security* (TSEC) cryptovariable, changes continuously.

Pulse Symbol Packet	A 13-microsecond transmission period within the time slot. A single -pulse symbol packet consists of a 6.4-microsecond pulse of modulated carrier frequency followed by 6.6 microseconds of dead time. A double-pulse symbol packet, which consists of two single-pulse symbol packets, is 26 microseconds in duration.
Radio Horizon	The distance to the horizon, as defined by the slightly curved path followed by a radio wave. This distance can be determined from the *effective earth radius*.
Receipt/ Compliance (R/C)	The protocol by which certain messages are acknowledged and responded to by the machine and, in some cases, by the operator. For Link 16, the machine receipt function is performed automatically by the Link 16 terminal.
Recurrence Rate	The total number of *time slots* per *epoch* assigned or deleted in a single time block assignment, specified as an integer, R, whose values range from = 0 to 15.
Reed-Solomon (R-S) Encoding	The scheme employed for encoding Link 16 message data that consists of the addition of error detection and correction bits to 75-bit words to form 155-bit sequences, which are then taken, in groups of five, to create 31 symbols.
R-S Codeword	An R-S encoded data word consist of 31, 5-bit *transmission symbols*.
Relative Grid	A three-coordinate flat-plane system used by Link 16 units (JUs) to report their position from the relative grid origin. The relative grid is active when there is a grid origin provided by the *Navigation Controller* (NC).
Relative Grid Origin	The origin, calculated by the network's *Navigation Controller* (NC), which inherently includes the NC's own geodetic navigation errors.
Relative Navigation (RELNAV)	An automatic and constant function of the Link 16 terminal, used for synchronizing all platforms in the network and for determining the distance between platforms.

Relay	A *network role* assigned to a Link 16 unit. Messages received within designated *time slots* are retransmitted after a specified delay. The retransmission of messages by airborne relay platforms allows information to be propagated to other units that are not within *line of sight* of the original transmitters.
Relay Delay	A fixed offset, from 6 to 31 time slots, between the time slot during which a Link 16 message is originally transmitted and the time slot during which it is retransmitted by a relaying unit.
Relay Function	A JTIDS/MIDS terminal capability.
Relay Pair	The first and *relay*-repeated transmissions of a single message.
Relay Hops	The retransmissions required to extend Link 16 connectivity beyond *line of sight*.
Reporting Responsibility (R2)	The requirement for the IU with the best positional data on a track to transmit track data on the interface. Automatic procedures exist to limit the number of units reporting a particular radar contact, or track, to a single unit. This determination is based on track qualities, and the unit designated as having responsibility for reporting the track is said to have R2.
Repromulgated Relay	A *relay* technique, used by the U. S. Army, in which any suitably initialized receiver will relay a transmitted message during the next *time slot*.
Residual Message NPG	A *Network Participation Group* (NPG 29) in which messages not specifically assigned to other NPGs may be exchanged.
Round-Trip Timing (RTT)	The process used by a Link 16 terminal to directly determine the offset between its clock and that of another Link 16 terminal. This is used to achieve and maintain fine synchronization and to improve the terminal's time quality. This process involves the exchange of RTT Interrogation and Reply messages.

Round-Trip Timing (RTT) Message	One of a set of messages that support fine synchronization between the units of a Link 16 network. They are both sent and received during a single *time slot* by an individual Link 16 unit (JU): the interrogation is sent, and the reply is received.
RTT-A (NPG 2)	By definition, the *Network Participation Group* during which specifically addressed *Round-Trip Timing* messages are transmitted during *time slots* that are dedicated to particular Link 16 units (JUs).
RTT-B (NPG 3)	By definition, the *Network Participation Group* during which *Round-Trip Timing messages* are transmitted during *time slots* that are shared among units and which are accessed by contention.
Secondary Navigation Controller (SNC)	A *network role*, assigned when a relative grid is to be used by units of a Link 16 network, to a single unit that can be either stationary or mobile, but which must be in relative motion with respect to the *Navigation Controller*, and must be in synchronization and *line of sight* of it.
Secondary User (SU)	A *network role* taken by any Link 16 unit (JU) that enters a Link 16 network under restricted conditions, during which they remain either radio silent or *data silent*.
Serial Interface	A computer interface in which single bits are transferred serially, one after the other, along one line.
Serial J	Legacy point-to-point (as opposed to netted) communications protocols that use J-series messages.
Set	In Link 16 *time division multiple access* (TDMA) architecture, one-third the total number of *time slots* in one *epoch*. The three sets of time slots are designated Set A, Set B, and Set C. The epoch consists of the interleaved time slots of these three sets.
Selective Identification Feature (SIF)	A capability that, when added to the basic *Identification Friend or Foe* (IFF) system, provides the means to transmit, receive, and display selected coded replies which uniquely identify a platform.

SIMPLE	Standard Interface for Multiple Platform Link Evaluation, a data link exchange protocol.
Single Pulse	A Link 16 transmission format employing one pulse symbol packet to convey messages.
Socket J	An unofficial term used to characterize the moving of compatible data over a TCP/IP network.
Spread Spectrum	A modulation/demodulation technique in which the transmission bandwidth is much greater than the minimum bandwidth that would be required to transmit the digital information, and which results in a performance improvement. In Link 16, five bits of digital information are transmitted with each pulse by associating each 5-bit message with a different phase of the 32-bit direct-sequence spreading code.
Stacked Nets	The principle of Link 16 TDMA architecture by which the time slots of a single NPG may be simultaneously allocated to 127 different nets, transmitting on different frequency-hopping patterns. The Voice and the Air Control NPGs are the most common examples of stacked nets..
Standard (STD) Format	A transmission format consisting of three words that are transmitted A message consisting of three words that are transmitted redundantly within a single time slot. Because messages of this format are always transmitted with the double-pulse structure, it is sometimes referred to as Standard Double-Pulse (STD-DP) format.
Strength Change Report	The J7.0 Act. (5) message. Note that Strength Changes are not performed by the CDO.
Statute Mile	A unit of distance that is equal to 5,280 feet.
Subscriber Interface Computer Program (SICP)	A computer program, residing within the JTIDS terminal, which has overall responsibility for communicating with the host platform.

Surveillance	The process of searching for, detecting, locating, identifying, and tracking objects of interest to the force. Surveillance information is exchanged on *Network Participation Group* (NPG 7).
Suspended Relay	A *relay* function of a terminal in suspend mode.
System Time	The time maintained by a designated terminal, the *Network Time Reference* (NTR).
Symbol	A single element of a codeword that corresponds to five Reed-Solomon encoded bits of a 155-bit sequence. This sequence represents a 75-bit data word, to which 80 bits have been added for error detection and correction.
Symbol Interleaving	The intermixing of the *symbols* that constitute the header and data of the message. Its purpose is to render the positions of elements of the message header unpredictable, thus greatly decreasing the possibility that the message transmission can be intercepted, exploited, or jammed.
Synchronization	(1) The acquisition and maintenance of system time by any member of a Link 16 network. (2) The second portion of the time slot, during which a specific sequence of symbols is transmitted.
Tactical Air Navigation (TACAN)	A military navigation system that combines distance and direction measurement to military aircraft, which are specially equipped to reference them.
Terminal Input Messages (TIMs)	Messages that transfer data from a host computer to the JTIDS terminal over the MIL-STD-1553B multiplex data bus
Terminal Output Messages (TOMs)	Messages that transfer data over the MIL-STD-1553B multiplex data bus from the JTIDS terminal to a host computer.
Time Division Multiple Access (TDMA)	The architectural principle by which Link 16 networks are structured and periods of transmission are assigned to every unit.

Time Quality (Q_t) The measure, kept by every Link 16 unit (JU), of its accuracy with respect to a designated *Network Time Reference*. Time Quality (Q_t) is expressed as an integer from 0 to 15 that represents the number of nanoseconds' deviation about the standard reference. The maximum Q_t value is 15, which represents a deviation less than or equal to 50 nanoseconds.

Time Refinement The third portion of the time slot, during which four double-pulse starting sequence number (S0) symbols are transmitted over 104 microseconds.

Time Slice For the Link 16 *time division multiple access* (TDMA) architecture, the designation for a single *time slot* that occurs during the identical period of time for all 127 stacked nets.

Time Slot The allocated period of time during which a netted unit contributes its information over a tactical data link. Also, the period of shortest duration of which the Link 16 TDMA architecture is structured. The time slot is the basic window of access to the network and is the period during which a Link 16 unit (JU) is either transmitting or receiving. The duration of the Link 16 time slot is 7.8125 milliseconds.

Time Slot Block (TSB) A collection of time slots spaced uniformly in time over each *epoch* and belonging to a single time slot *set*. A block is defined by indexing time slot number (0 - 32,767), set (A, B, or C), and a *recurrence rate* number (0-15).

Time Slot Duty Factor (TSDF) A restriction that limits the usage of time slots to a number of pulses per unit of time.

Time Slot Reallocation An access method that establishes a pool of *time slots*, which are periodically reassigned among the participants of a *Network Participation Group* (NPG), based on their transmission needs.

Time Slot Reuse The practice of assigning two or more Link 16 units (JUs) to transmit on the same net during the same time slot.

Time Synchronization Messages The J0.0 (Initial Entry) and J0.2 (Network Time Update) messages.).

Time Uncertainty Setting An Link 16 operator setting that tells the terminal how many seconds of uncertainty to use in listening for the *Network Time Reference* unit's *Initial Entry message* to achieve *coarse synchronization*.

T-messages A designation for *Interim JTIDS Message Specification* (IJMS) messages, except for IJMS Position and Status messages, that are transmitted on the *Network Participation Group* (NPG 31) reserved for this purpose.

Today/Tomorrow Pair A schedule for the use of *cryptovariable* pairs loaded into the *Secure Data Unit* that allows the network to roll over *cryptovariables* from one day to the next without disruption to the link.

Track Number (TN) A number, applied to a located object, which is used to associate information and directives for digital communication over Link 16.

Track Number Association The process of assigning, and consistently using, a low track number for tracks that were originated on Link 16 with a high track number and are being forwarded to Link 11.

Transmission Security (TSEC) A *cryptovariable* that is used by a Link 16 unit (JU) to determine the duration of jitter within the time slot, as well as the *pseudorandom noise* with which the received transmission was masked by the transmitter.

Transmission Symbol A 32-bit sequence that results from the bitwise exclusive-or operation of a 32-bit sequence of *pseudorandom noise* and a 32-bit *chipping sequence* of data.

Unconditional Relay A *relay* mode in which a Link 16 unit (JU) in *fine synchronization* with the network and not in Long-Term Transmit Inhibit (radio silence) always relays messages in accordance with its *time slot* assignments.

Upper Packing Limit An initialization parameter of the Link 16 terminal that constrains its transmissions to a subset of the full range of possible *packing structures*. Its purpose is to establish the minimum amount of *antijam margin* always retained.

Variable Format A Link 16 message format that supports the U. S. Army's Link 16 communications requirements, and which consists of a variable number of 75-bit words.

VHF Omnidirectional Range (VOR) A transmitter that is used by aircraft for measuring range. It can be co-located with *Distance Measuring Equipment* for providing aircraft with both range and distance.

Voice A, Voice B The two channels, *Network Participation Groups* 12 and 13, respectively, that are used by Link 16 units (JUs) for secure digitized voice transmissions.

VORTAC (1) A transmitter that combines the functions of a military *TACAN* system and a civilian *VOR* to provide VOR azimuth, TACAN azimuth, and TACAN distance to an airborne interrogator.

Weapons Coordination The *Network Participation Group* (NPG 18) during which commands are transmitted for employing tactical weapons.

Word For Link 16, a sequence of 75 bits, 70 of which are tactical data and 5 of which are for parity. Data words are Reed-Solomon encoded with the (31, 15) algorithm, in which 15 bits are transformed into coded 31 bits.

Zoom Relay A *relay* type in which selected portions of the *main net* are designated for relay on another net.

NOTE

Since this document is intended for public release, the content of this chapter is limited to overview information concerning tactical data links. For additional information, please contact Northrop Grumman.

Product Sales/Customer Service
877-784-HELP (4357)
cis.productsupport@ngc.com
http://tacticalnetworks-ngc.com