



Link 22 Guidebook

February 2016



Distribution: Distribution limited to the Ministries of Defense (MODs) of France, Germany, Italy, Spain, United Kingdom, National Defence Headquarters of Canada, United States DOD, their respective contractors / industry suppliers, and approved Third Party Sales Nations that are financial contributors in good standing and their respective implementation contractors. Other requests for this document must be referred to the NILE Project Management Office (PMO).

NORTHROP GRUMMAN

Link 22

Guidebook

February 2016

Prepared for:

Contract N00039-13-C-0035
NILE Project Management Office
Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, CA 92110-3127

Distribution: Distribution limited to the Ministries of Defense (MODs) of France, Germany, Italy, Spain, United Kingdom, National Defence Headquarters of Canada, United States DOD, their respective contractors / industry suppliers, and approved Third Party Sales Nations that are financial contributors in good standing and their respective implementation contractors. Other requests for this document must be referred to the NILE Project Management Office (PMO).

Prepared by:

NORTHROP GRUMMAN

Northrop Grumman Systems Corporation
Airborne C4ISR Systems Division
9326 Spectrum Center Boulevard
San Diego, CA 92123-1443

Original Edition for the NILE Project Management Office – July 2009
Second Edition for the NILE Project Management Office – July 2010
Third Edition for the NILE Project Management Office – July 2011
Fourth Edition for the NILE Project Management Office – July 2013
Fifth Edition for the NILE Project Management Office – February 2016

Distributed by NILE Project Management Office
Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, CA 92110-3127

Document number NG 278-A011

Printed by Northrop Grumman

Dedication

Preface

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 dated 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 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 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 – 2015: In-Service Support (ISS) Phase
 - Develop the prototype Modernized Link Level COMSEC (LLC)

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 NILE Reference System (NRS) and an interoperability tester, the Multiple Link System Test and Training Tool (MLST3). These test tools are complete systems, consisting of both hardware and software. The NRS can be used to test whether a nation's system 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

This is the complete version of the Link 22 Guidebook that is releasable only to NILE Nations and their approved contractors/industry suppliers, and to Third Party Sales Nations that are financial contributors, in good standing, and their respective implementation contractors. It is a detailed operational and technical guide for Nations who planto implementLink 22. Third Party Sales Nations must have paid both the one-time levy to the Sponsoring NILE Nation for each platform and the annual maintenance fees to the NILE PMO.

Structure

This guidebook is composed of the following three principal chapters.

- Chapter 1, containing executive-level information, for managers, and procurers
- Chapter 2, containing user-level information, for planners, operators, and technicians
- Chapter 3, containing technical-level information, for implementers, integrators, testers, and software engineers

Additionally Appendices for Integration and Test Tools, Troubleshooting, Minimum Implementation, Abbreviations and Acronyms, a Glossary, and a List of References may be found at the back of the guidebook.

How to use this book

This guidebook has been written in a manner that provides suitable information for Link 22 operators, planners, managers, executives, developers, and testers. Users can skip sections that are not of interest or applicable to them.

Chapter 1 should be read by managers, procurers, and anyone who is new to Link 22.

Chapter 2 should be read by planners, operators, and technicians (those in charge of hardware configurations).

Chapter 3 should be read by implementers, integrators, testers and software engineers.

Contact information

NILE Project Management Office
Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, CA 92110-3127

Acknowledgements

The NILE PMO would like to acknowledge the Subject Matter Experts, Reviewers and guidebook publishers who have made this product possible.

Guidebook Subject Matter Experts and Reviewers

Schwartz, Charles	NILE PMO, Project Manager
Gomez, Manuel	NILE PMO, Project Manager (Former)
Buck, Dr. Kevin	NILE PMO, Project Manager (Former)
Harrison, LCDR Stephen	NILE PMO, Canada
Duffley, LCDR Peter	NILE PMO, Canada (Former)
Richard, LCDR Troy	NILE PMO, Canada (Former)
Fontaine, LT Mickael	NILE PMO, France (Former)
Dhakouani, LT Mehdi	NILE PMO, France (Former)
Koschig, LT Alexander	NILE PMO, Germany
Beutner, LT Andreas	NILE PMO, Germany (Former)
Gatti, LCDR Cristian	NILE PMO, Italy
Capecchi, CDR Alessandro	NILE PMO, Italy (Former)
Battaglia, CDR Alessandro	NILE PMO, Italy (Former)
Nieto, CDR Juan	NILE PMO, Spain
Aznar, CDR Francisco	NILE PMO, Spain (Former)
Alvarez-Maldonado, CDR Carlos	NILE PMO, Spain (Former)
Nye, Stephen	NILE PMO, United Kingdom
Nuttall, James	NILE PMO, United Kingdom (Former)
Pooley, David	NILE PMO, United Kingdom (Former)

Northrop Grumman Guidebook Production

Williams, Paul	Principal Author
Sidelnikov, Shannon	NILE Project Manager, Author
Sferra, Vincenzo	NILE Project Manager, Author (Former)
Mueller, Debbie	Author
Solorzano, Dora	Publications Department, Editor
Crowell, Karen	Publications Department, Editor

Table of Contents

Chapter 1 - Link 22 Overview

- Section A Introduction
- Section B Features
- Section C Benefits
- Section D Acquisition

Chapter 2 - Link 22 Operations

- Section A Overview
- Section B Planning
- Section C Link 22 Operations
- Section D Tactical Messages
- Section E Link 22 in a Multilink Environment

Chapter 3 - Link 22 Technical

- Section A Architecture
- Section B External Protocols
- Section C Internal Protocols

Appendices

- Appendix A Integration and Test Tools
- Appendix B Troubleshooting
- Appendix C Minimum DLP-SNC Interface Implementation
- Appendix D Initialization Parameter Generation
- Appendix E Acronyms and Abbreviations
- Appendix F Glossary
- Appendix G References

Index

1

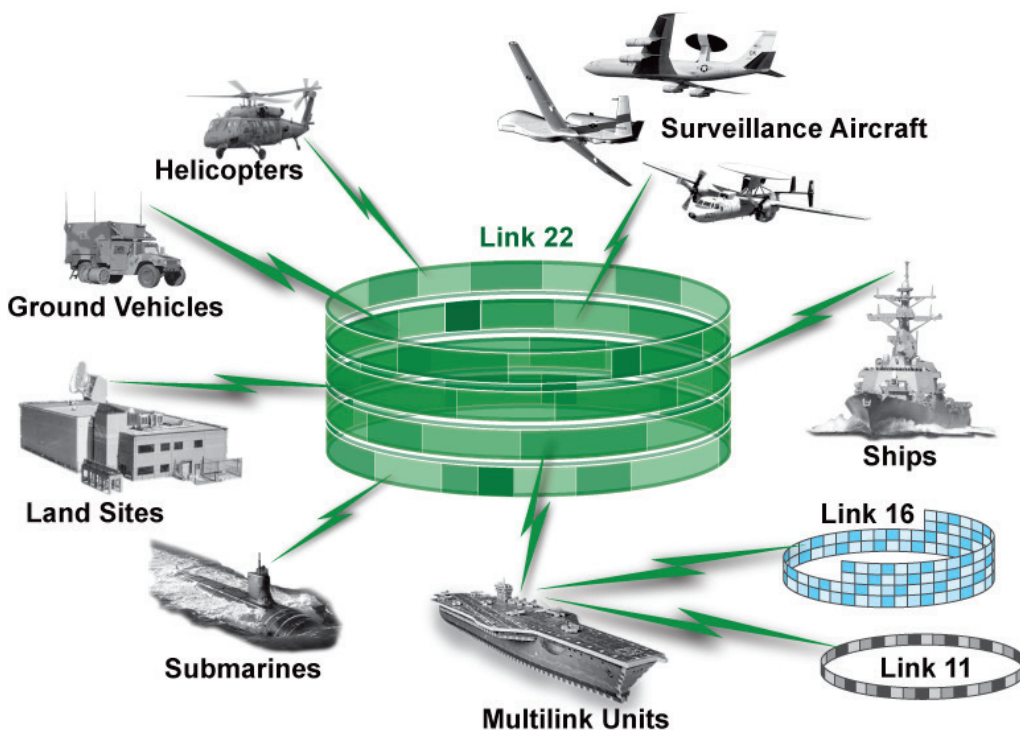
2

3

Chapter 1

Link 22 Overview

Section A Introduction



Link 22 is a North Atlantic Treaty Organization (NATO) secure radio system that provides Beyond Line-Of-Sight (BLOS) communications without the use of satellites. 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.



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.

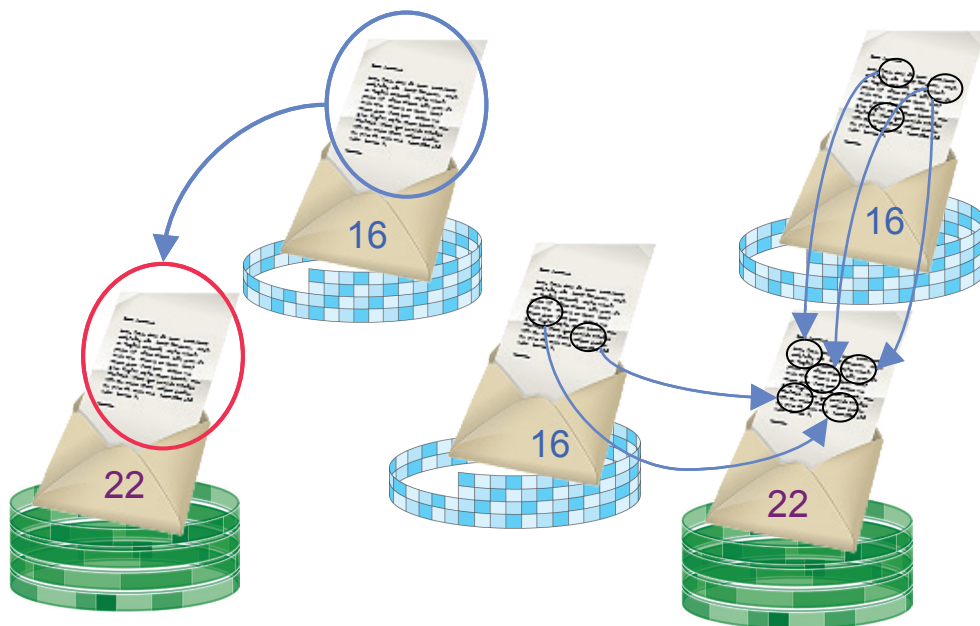


Link 22 was developed to replace and overcome the known deficiencies of Link 11. Link 22 was also designed to complement and interoperate easily with Link 16. It was designed with automated and simple management to ensure that it is easier to manage than both Link 11 and Link 16. This program is called “**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 COMMunications SECurity (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 **Link Level COMSEC (LLC)**. The LLC also provides detection of attempts to disrupt the network. The LLC is based on the existing KIV-7M and is designated the LLC throughout all NILE documentation. It is a programmable crypto that complies 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



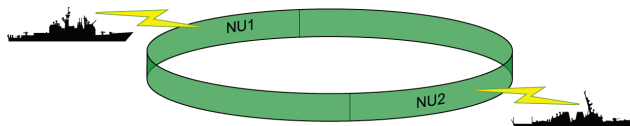
A Link 22 message can contain
a complete Link 16 message

OR

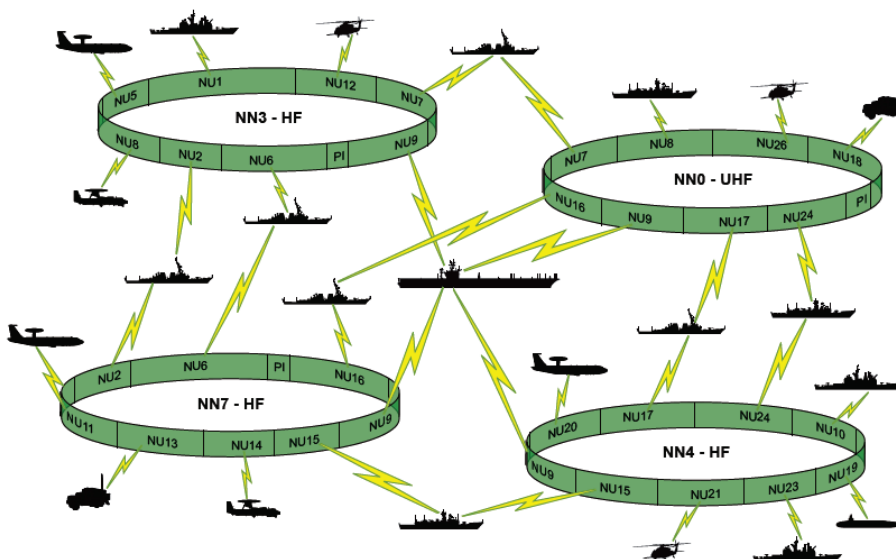
A Link 22 message can contain
parts of Link 16 messages

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.

Link 22 Super Network

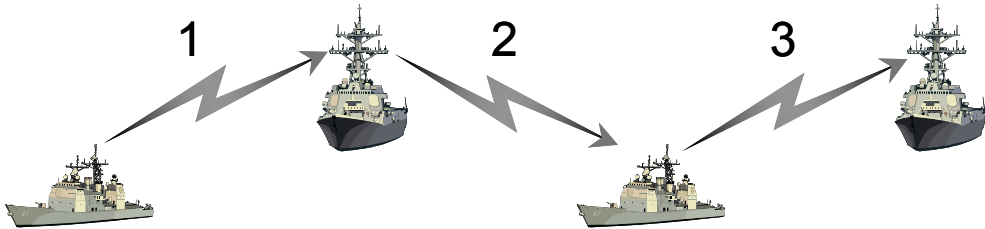


An operational Link 22 system is called a Link 22 **Super Network**. In its simplest form, a Link 22 Super Network consists of just two units communicating with each other in a single NILE Network. The most complex Link 22 Super Network would consist of the maximum number of units (125), with eight NILE 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 below.



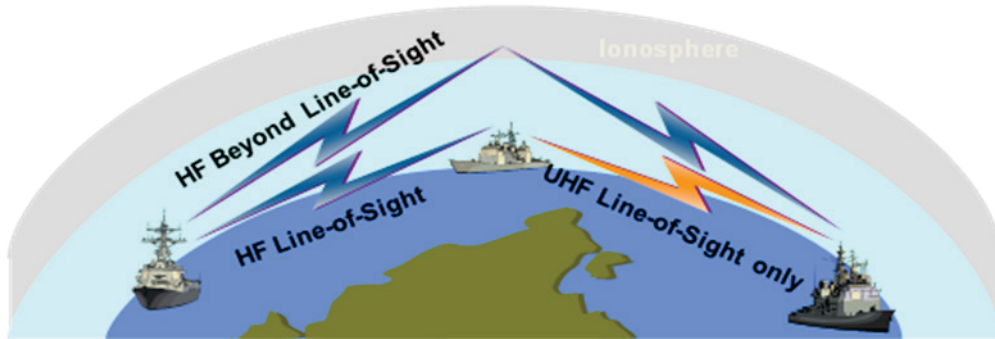
A Super Network enables seamless communication between units using different media to satisfy operational requirements within prevailing media propagation conditions. In a Super Network, any NILE unit can communicate with all other NILE units without regard to the NILE Network in which they are participating, 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 System Network Controller (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.

Beyond Line-Of-Sight Communication



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

HF communications are in the 2-30 MHz band, which provides Beyond Line-Of-Sight (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.

UHF communications are in the 225-400 MHz band (which is within the military 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



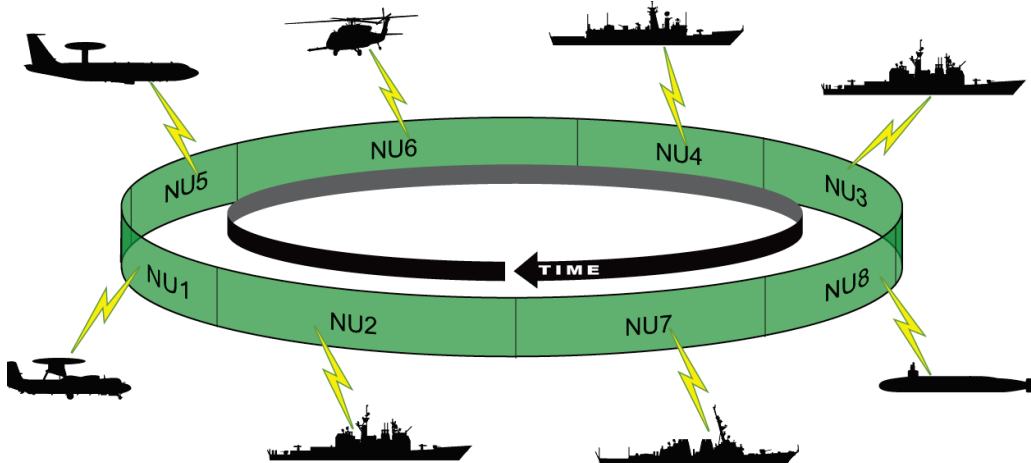
Link 22 has better tactical data throughput than Link 11, and it can even work in conditions where Link 11 will not. When conditions are bad, Link 22 can use more robust media parameters and maintain communication, although at a lower data rate than usual. When conditions are good, Link 22 can optimize 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.

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.

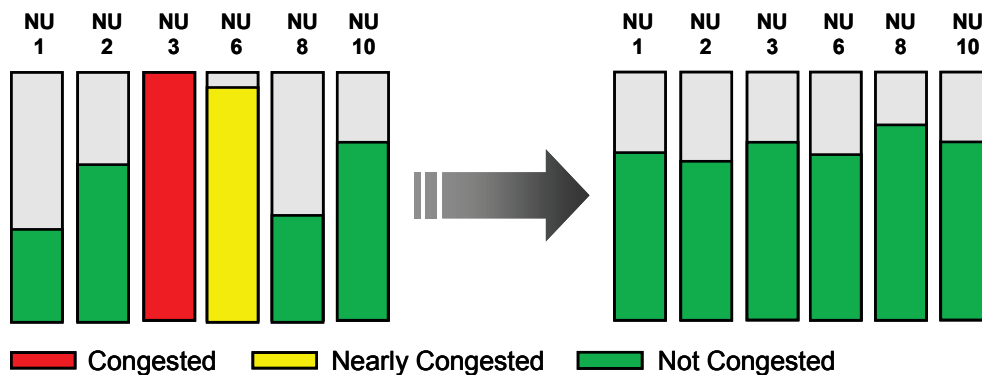
Time Division Multiple Access



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.

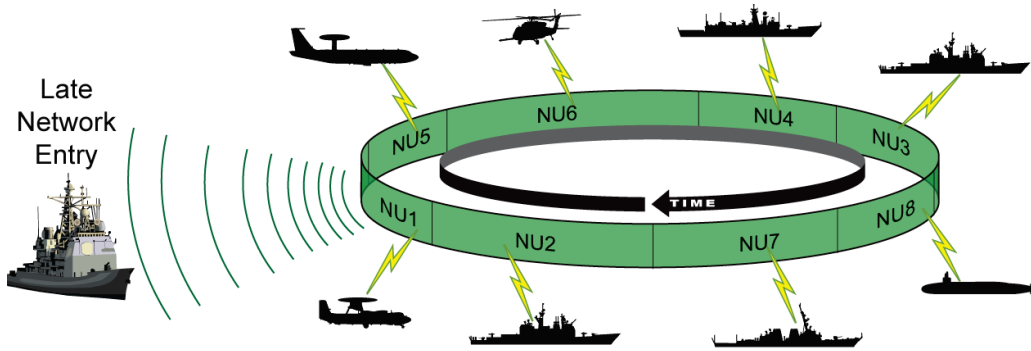
Automated Congestion Management

Congestion Management Can Reallocate Unused Capacity



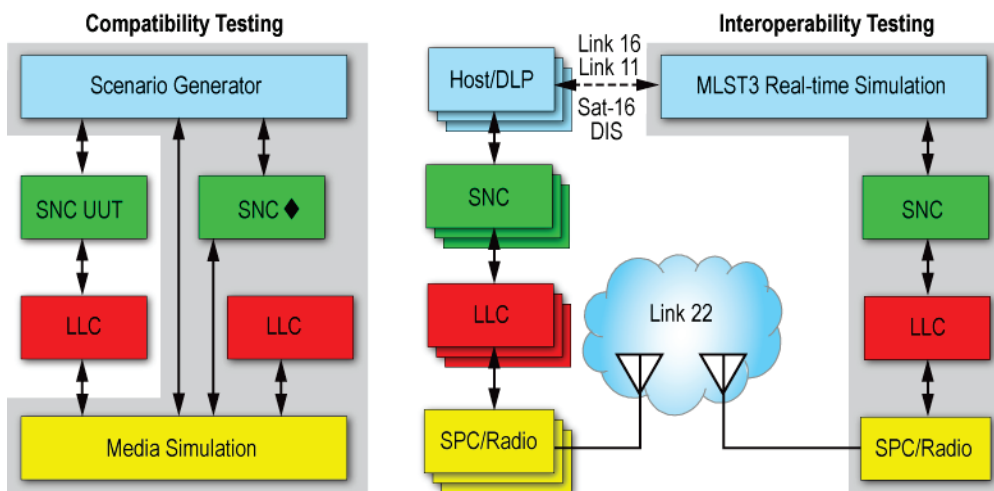
At the tactical level, when a unit is congested, it can reduce the local traffic that it generates based on the provided congestion information. In addition, Link 22 automates Congestion Management in a number of different ways. The routing of messages takes congestion into account and will route messages 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.

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).

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 guidebook. Nations may develop their own Link 22 test systems, but they are not included in this guidebook.

The compatibility test system is called the NILE Reference System (NRS), which was developed to test the System Network Controller (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 Multi- Link System Test & Training Tool (MLST3). This is an existing system which has been extended to incorporate the Link 22 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.

Test Tool details are in Appendix A.



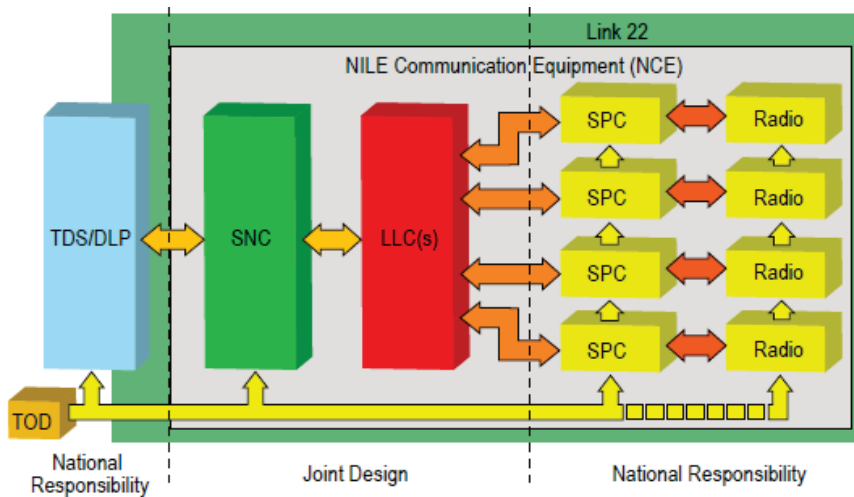
This page is intentionally left blank.

Section B 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. 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 **Data Link Processor (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. 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 Communications Security (COMSEC). It was designed to be mountable in a 1/2 Air Transport Rack (ATR) Long enclosure, and is shown in the picture.

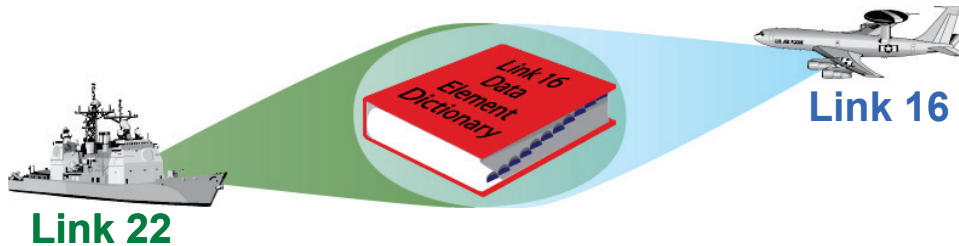


The LLC uses a weekly key to encrypt and decrypt the data traffic that passes through it. The LLC can store 64 keys for each of the 8 NILE networks, enabling it when fully loaded, to operate for more than a year without any operator intervention. New keys can be loaded at any time, except for any of the keys currently being used. 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.

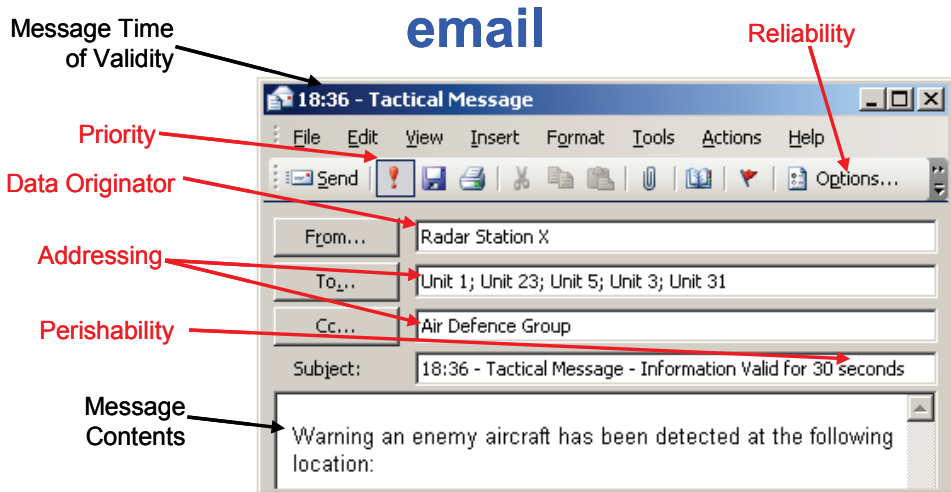
Link 22 messages are called F-Series messages and are part of the J-Family of messages. The F-Series consists of two types of messages, the Unique F messages and the FJ messages. The Unique F-Series messages are more compact versions of Link 16's messages, or messages that do not exist in Link 16. The 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 Quality of Service (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

□ **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 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.

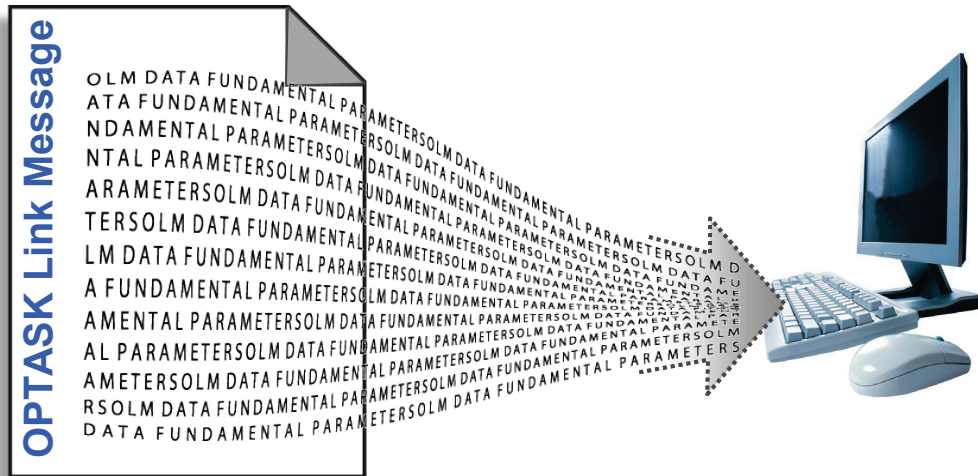
- The Priority Injection Indicator flag is used to enable priority 1 messages to be injected in **Priority Injection (PI)** timeslots, which are timeslots that are not allocated to any specific unit
- The **Radio Silence Override Indicator** flag enables the message to be transmitted when the unit is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

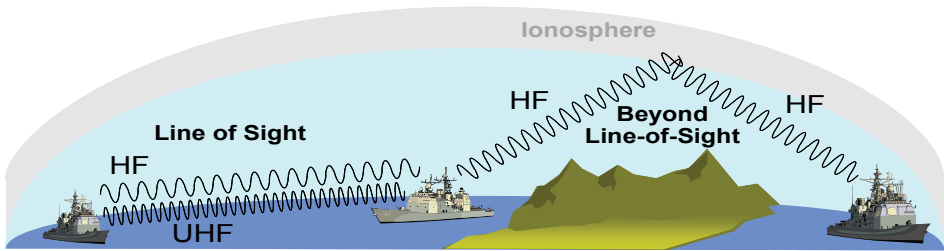
Fundamental Parameters



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.

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, and the expected tactical message throughput of each unit. 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



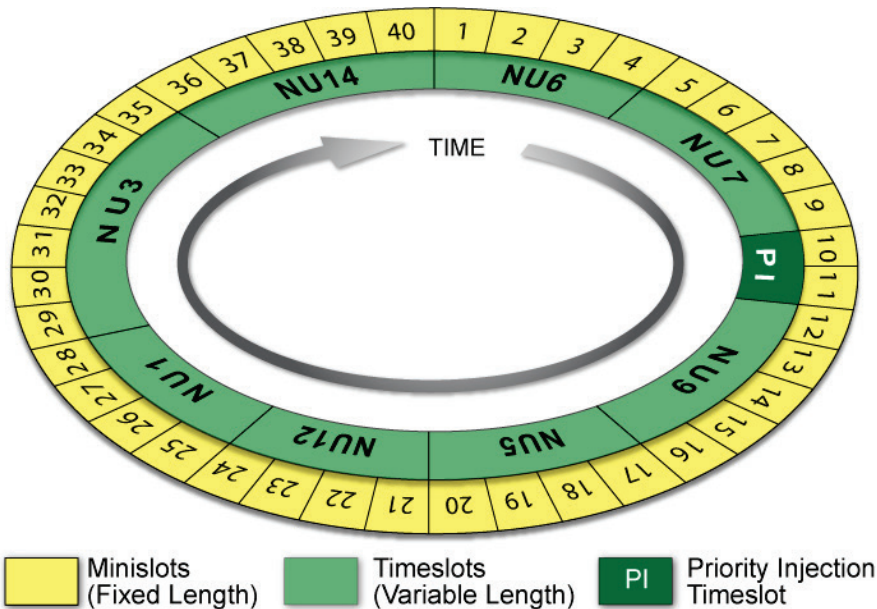
Media using High Frequency (HF) in the 2-30 MHz band provides Beyond Line-of-Sight (BLOS) communications, optimized for (but not limited to) transmission up to 300 nautical miles. Media using Ultra High Frequency (UHF) in the 225-400 MHz band provides Line-of-Sight communications only. Within both bands,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

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

There are four additional unused media types which are available for future use. Each media has one or more different settings (max 255), which use different modulation and encoding schemes. The currently defined Media Settings along with the fragmentation rate, 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. Eleven new HF Fixed Frequency Waveforms to provide extended range and higher capacity have been approved for implementation (these are not shown in the table below). 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

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 Priority Injection 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).

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.

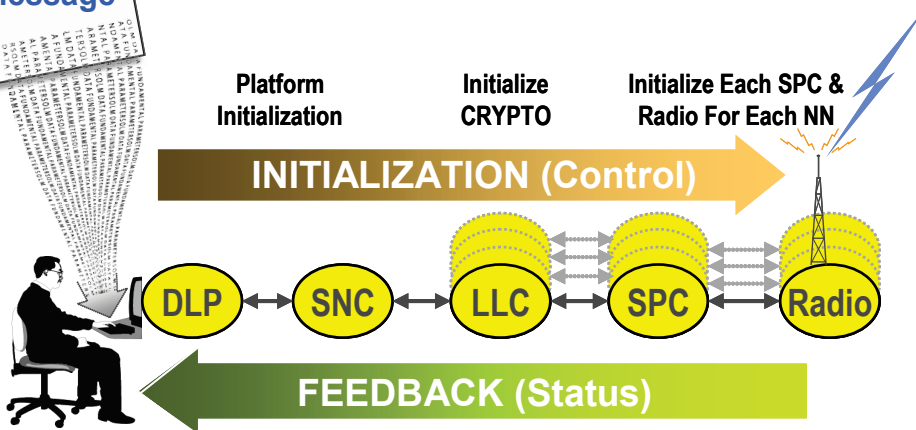
Initialization



PLANNING (Fundamental Parameters)
Production of the OPTASK Link Message



OPTASK Link Message distribution



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

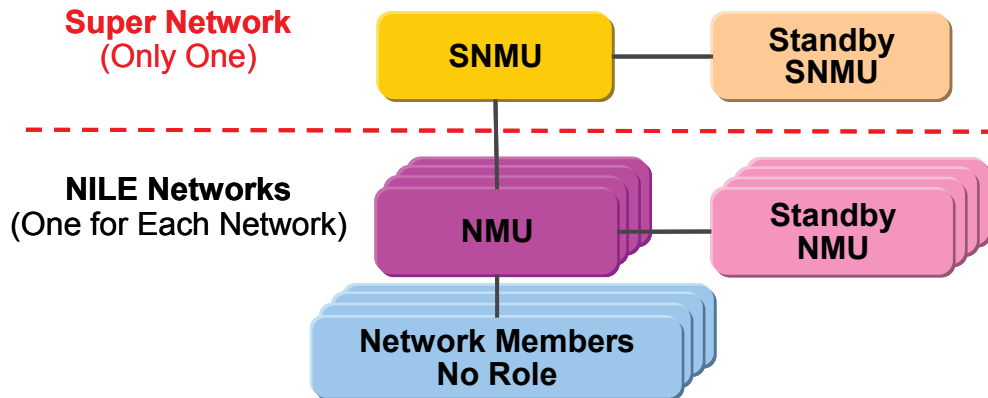
The Link 22 unit's subsystems must be initialized first, before any networks are initialized. Hardware configuration information must be supplied to the SNC by the

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.

If the unit has missed the start time for the network initialization, it should join the network by performing the Late Network Entry (LNE) protocol. Late Network Entry (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 learned 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, although a unit may be the NMU of more than one 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.

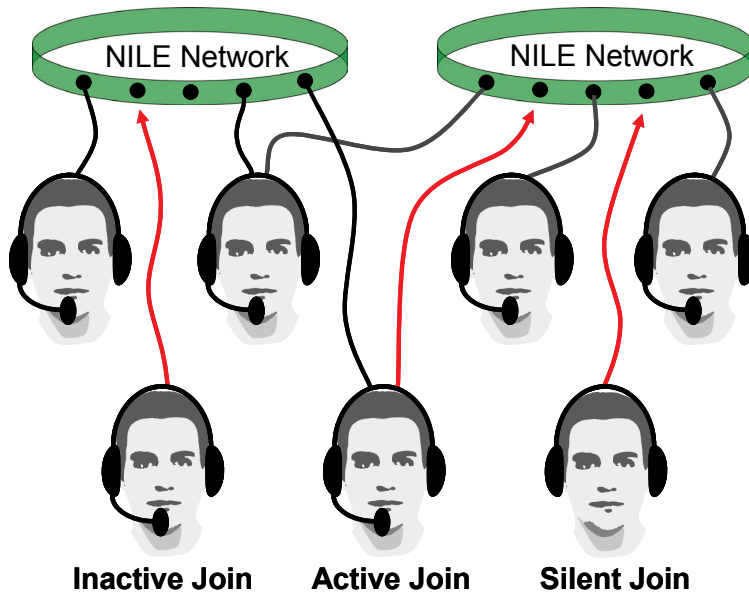
The SNMU and, in some cases the NMU, can order certain management changes to the Link 22 system, including the following.

- 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
- Managing Radio Power

Other management functions, such as those listed below, do not require the use of an order, but do require transmission of a message to initiate the change.

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

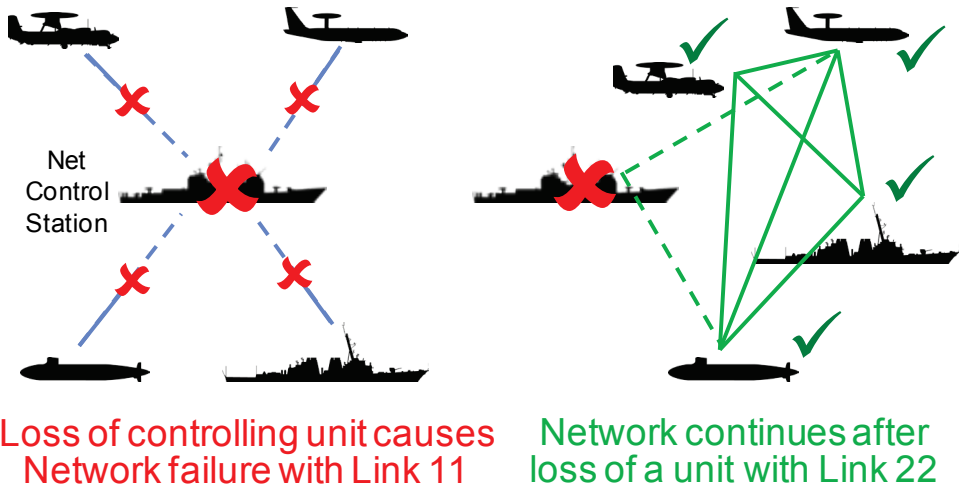
Joining a Network



A unit that arrives after the Super Network has been started can still join by initiating the Late Network Entry (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

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.

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.

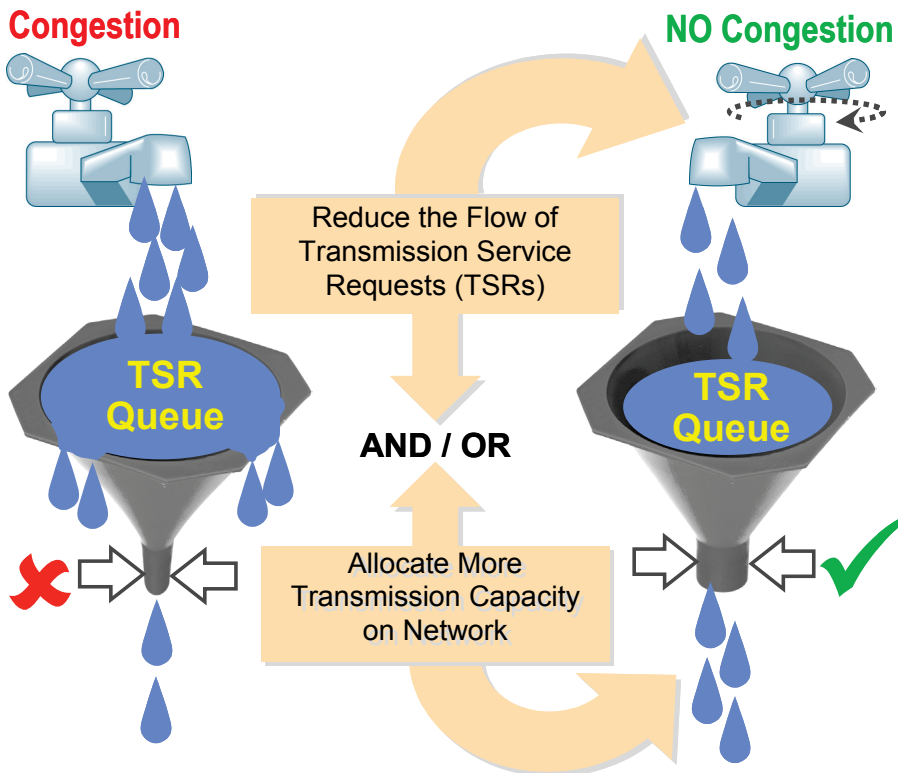
The transmission on the NILE Networks is controlled by the TDMA structure, which is known to each unit, so the loss of any unit does not affect the ability of the remaining units to continue operation. Virtually all functions work in this manner (called distributed protocols), so there is no single point 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 NMU or Standby SNMU that takes over the primary 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 Dynamic TDMA (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 within the SNC, 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.

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 C 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 requires extensive planning and complex management.

Link 22 offers the latest technology and was designed in a layered architecture with each layer using COTS products whenever possible. The DLP software, SNC software, and the LLC are not COTS. The DLP computer and operating system, the SNC computer and operating system, the SPCs and radios are all COTS. 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.

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

Link 11	Link 22
The encryption level is not sufficient for the processing power of modern computers	Crypto technology has been updated to meet future requirements
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

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 which is not dependent on airborne relay units being available. It remains operable when an airborne/satellite relay is not available
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 which can increase the bandwidth

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 JTIDS	Link 22 HF (fixed frequency)	Link 22 UHF (fixed frequency)
1090 or 1800	26,880-107,520	1,493 – 4,053	12,666

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

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

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



This page is intentionally left blank.

Section D 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 Data Link Processor (DLP) is connected to, or is part of, the Tactical Data System (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 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 1GHz processor with one GByte 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 four networks of any of the current types 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. Associated with the LLC and its key loading are two recommended key loading devices, a Data Terminal Device (DTD) and a Simple Key Loader (SKL) AN/PYQ-10 (C). These devices or another compatible device are used to load the keys into the LLC, and would need to be acquired from the national crypto agency. 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 or SKL.

The current LLC is mountable in a 1/2 Air Transport Rack (ATR) Long enclosure. The manufacturer based the LLC on an existing KIV-7M and so the LLC model number was designated as the LLC7M.

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" rack mountable chassis, with two of them containing VME cards which 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 original goals of the NILE Project was to be able to reuse existing modern Link 11 radios and antennas equipment. If they are available this would reduce 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 TOD input to the SPCs is the Extended Have Quick format as defined in [STANAG 4430].

The SNC is delivered with a separate application (TOD) to receive the Extended Have Quick format input in compliance with [STANAG 4430] and supply the actual current UTC information to the SNC. Currently this is supplied by a Universal PCIe Time Card manufactured by Brandywine. The NRS uses a different application called Read TOD that can be controlled by the NRS to supply the SNC with either the actual UTC time or a simulated time for the test scenario being run, as detailed in section 3 of the [NRS 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 installation in single or multiple enclosures is required 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.



This page is intentionally left blank.

Chapter 2

Link 22 Operations

Based on the technical aspects defined in [[STANAG 5522](#)] and on the basis of operational procedures as defined in Allied Data Publication [[ADatP-33](#)] this chapter is intended as a generic guideline for planners, operators and technicians utilizing Link 22 in a single or a multiple link environment. National or platform specific procedures and operator actions are not covered in this guidebook.

Section A Overview

The overview consists of a description of the overall architecture, and the key parameters that affect the system.

2A.1 Architecture

The layers of the Link 22 Architecture and the user interaction with each of the layers are shown in [Figure 2A.1-1](#).

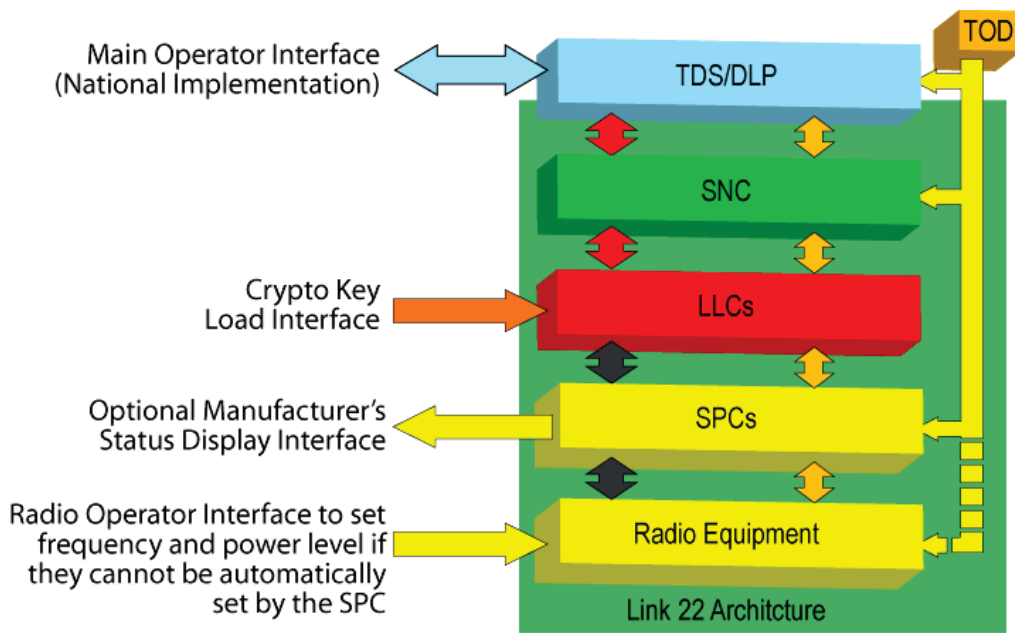


Figure 2A.1-1 Link 22 Architecture

The components of the Link 22 layered system architecture shown in Figure 2A.1-1 are the following.

- Data Link Processor (DLP)
- System Network Controller (SNC)
- Link-Level COMSEC (LLC)
- Signal Processing Controller (SPC)
- Radio Equipment
- Time of Day (TOD) Distribution

Each of these components are detailed in the following subsections.

2A.1.1 Data Link Processor (DLP)

The DLP is connected to, or is part of, the Tactical Data System (TDS), which is also known as the Host System. A Host System processes the received tactical messages and generates tactical messages for transmission in accordance with a unit's national requirements. The Link 22 portion of the DLP includes the interface to the SNC, and the tactical messages that it transmits on the data link. Most user input to the system is via the Host system, and these implementations are the responsibility of member nations. This Guidebook discusses only general functionality, without going into the specifics of any national implementation.

2A.1.2 System Network Controller (SNC)

The SNC is a standard software application that must be used by all national implementations, thus providing compatibility between units. The SNC was developed to be easily portable between different platforms. Official versions are available for Microsoft Windows and for the Linux operating systems running on PC platforms.

The SNC's interface to the DLP uses the TCP/IP socket based communications protocol. For an external DLP this can be via any physical interface on the SNC platform which supports TCP/IP (e.g. Ethernet). When the DLP and SNC are collocated on the same processor this is via the TCP/IP protocol stack within the operating system, without any physical interface. The SNC interfaces to the media via one or more (maximum four) LLC devices. The physical interface is via Ethernet, using TCP/IP communications. The SNC must also be supplied with the TOD, which it obtains from a platform hardware-independent interface. The SNC does not have any direct user input.

2A.1.3 Link-Level COMSEC (LLC)

The LLC provides the communications security of the data transmitted on Link 22. It interfaces with the SNC using Ethernet and TCP/IP communications.

The LLC encrypts the data that the SNC sends, and delivers the encrypted data to the SPC for transmission. The interface to the SPC is via individual serial lines, one for each network. The LLC has four serial ports for the connection of the SPCs. The SNC can be connected to a maximum of four separate LLCs, however only one LLC is required to handle 4 networks with maximum bandwidth.

The data received by the SPC is sent to the LLC, which decrypts it, and delivers it to the SNC. The LLC does not have a TOD input. The LLC provides a standard connector on its front panel for loading of the encryption keys. Crypto key loading is performed by the user, by means of a Simple Key Loader (SKL) device or Data Transfer Device (DTD).

2A.1.4 Signal Processing Controller (SPC)

Link 22 has four different media types and four additional currently undefined media types which are available for future use. An SPC implementation may support more than one type of media, and have the ability to select or configure the media to be used. Additionally, more than one SPC may be implemented on the same physical board or device. Direct user input to the SPC is not required for the operation of Link 22, although the manufacturer may provide a proprietary Human Machine Interface (HMI) for monitoring and diagnostic use. SPC HMIs are not within the scope of Link 22. A manufacturer's HMI may be able to display the selected frequency of the Fixed Frequency (FF) media as well as the selected radio power, so that if manual radio tuning and power control is required, the necessary settings are shown.

2A.1.5 Radio Equipment

The radios include the associated power amplifiers and aerials. Link 22 was designed to be able to reuse the Link 11 fixed frequency HF and UHF radios. To provide additional transmission security, it was also designed to use newer technology frequency hopping radios. These HF and UHF frequency hopping radios (also referred to as Electronic Protection Measures (EPM) Radios) require a TOD input to synchronize their hopping.

The UHF EPM radio's random frequency selection is controlled by the frequency hopset provided to the radio by the SPC.

For the HF EPM, the frequency hopset information has to be supplied to the SPC/radio combination.

When a fixed frequency radio does not provide frequency selection by the SPC, the user has to manually tune the radio to the selected frequency.

If the radio does not provide power-level control by the SPC, the user manually sets the power level of the radio to the requested level. This input should only be required for legacy equipment that does not provide the capability for the SPC to set the frequency or adjust the power level. It should not be needed with more modern equipment that provides the necessary control.

2A.1.6 Time of Day (TOD) Distribution

The TOD is input to the following components.

- DLP
- SNC
- Each SPC
- Frequency Hopping radios

The TOD is used to control the timing of transmissions and receptions. The time is not required by the crypto, even though time is used as part of the encryption. Time is supplied by the SNC with the data to be encrypted, and by the SPC with the data to be decrypted. Note that the TOD supplied to each of the different components of a Link 22 system (DLP, SNC, SPCs and/or radio) does not have to be supplied by the same source. Each component can have a different TOD input, as long as it meets the required accuracy (see Section [3A.2](#)). There is no user input to the TOD system, other than to ensure that it is powered up and operational.

2A.2 Key Parameters

The Link 22 Key Parameters are in three categories.

- Super Network Parameters
 - Start Date/Time
 - Roles (SNMU & Standby)
 - Crypto
- NILE Network Parameters
 - Media Type
 - Media Setting Number
 - Frequency
 - Fragmentation Rate
 - LLC Integrity
 - Network Start Date/Time
 - Initialization Type
 - Network Members
 - Roles (NMU & Standby)
 - DTDMA Enabled/Disabled
 - Network Cycle Structure
- NILE Unit Parameters
 - Unit Identification
 - Link 22 Address
 - Track Number Blocks
 - Role Takeover

2A.2.1 Super Network Parameters

□ Start Date/Time

The starting date and time of the Link 22 Super Network is used to define the first Day Of Week (DOW = 1). For example, if the starting date is on a Thursday, then Thursday = DOW 1. The Day of Week is used during encryption and decryption.

□ Roles (SNMU & Standby)

Certain units within the Super Network have special duties, which are called Roles. The initial allocation of these Roles is defined during network planning, but the Roles can be changed automatically or manually while the system is operating. The special Roles at the Super Network level are as follows.

- Super Network Management Unit (SNMU)
- Standby SNMU

The SNMU is responsible for managing the entire Super Network, which it does by issuing orders to other units and authorizing units to change their network membership, as appropriate. The SNMU is also responsible for ensuring that a Standby SNMU is always allocated and active in the Super Network.

The Standby SNMU monitors the presence of the SNMU and can take over if connectivity with the SNMU is lost.

□ Crypto

Crypto key identifications must be obtained from each nation's crypto key distribution agency. Crypto keys are used in the encryption and decryption processes. Crypto keys last for one week; therefore, multiple keys may be needed for the operation or exercise depending on its timeframe. The LLC-7M can store 64 keys for each of the 8 NILE Networks.

2A.2.2 NILE Network Parameters

A NILE Network is a collection of NILE units exchanging information in accordance with [STANAG 5522], using a single medium and a unique set of network parameters.

□ **Media Type**

Link 22 can support eight different media types, of which currently only four types of RF media (HF FF, UHF FF, HF EPM, and UHF EPM) are defined. The possible eight NILE networks in a Super Network can each use any of the 4 currently defined media types. The remaining four unused media types are reserved for future expansion.

□ **Media Setting Number**

The Media Setting Number (MSN) is a number that defines the waveform, repetition rate, coding and modulation schemes of a media type. MSN values range from 0 to 255. However, the currently defined MSN range is from 1 to 6 depending on the media type, with additional values reserved for future expansion. Short network initialization will use one MSN. Probing network initialization may try up to fifteen MSNs, and then select the best one.

□ **Frequency**

An HF FF network requires the allocation of a frequency between 2-30 MHz. UHF FF requires the allocation of a frequency between 225-400 MHz. The HF EPM and UHF EPM media use frequency hopping within the same frequency ranges, where the hopping frequencies are defined by hopsets.

□ **Fragmentation Rate**

A HF FF or UHF FF network has a defined fragmentation rate in the range one to three, and is the number of transmitted blocks of data that form a Network Packet. The Fragmentation Rate defines how many fragments a Network Packet is split into for transmission; these fragments are transmitted in sequence within the same time slot. The fragmentation rate of a network affects its throughput and robustness. The fragmentation rate for HF EPM and UHF EPM is set to one.

□ **LLC Integrity**

LLC Integrity is a function that when enabled causes the LLC to perform additional checking. LLC Integrity can be enabled or disabled independently for each network.

□ **Network Start Date/Time**

The starting date and time of each NILE Network must be defined.

□ ***Initialization Type***

Networks can be initialized in one of two ways.

- Short - used when communication conditions are likely to be good
- Probing - used when conditions are likely to be unknown

The selection may be different for each network. Probing initialization takes longer because it tries different media settings in order to determine the best setting.

□ ***Network Members***

The members of each NILE Network must be identified. Each unit can be placed in up to four networks, based on the unit's capabilities.

□ ***Roles (NMU & Standby)***

Two special Roles within each Network must be specified.

- Network Management Unit (NMU)
- Standby NMU

The NMU is responsible for managing its NILE Network without requiring authorization of the SNMU. However, if the SNMU requires a change to the network, the SNMU can order the NMU to perform the change. The NMU is also responsible for ensuring that there is always a Standby NMU allocated and active in the network.

Each Standby NMU monitors the presence of the network's NMU and can take over if connectivity with the NMU is lost.

□ ***DTDMA Enabled/Disabled***

DTDMA can be either enabled or disabled for each network. Enabling DTDMA allows the ONCS to be changed automatically, providing dynamic control of the TDMA structure.

□ Network Cycle Structure

A Link 22 NILE Network has a defined Operational Network Cycle Structure (ONCS) to provide Time Division Multiple Access (TDMA). TDMA is used to dedicate periods of time, called timeslots, for each unit in the network to transmit. The total time occupied by all the timeslots in the ONCS is called the Network Cycle Time (NCT). When the end of the cycle is reached, the cycle is repeated. Each NILE network within a Link 22 Super Network can have a different ONCS.

Figure 2A.2-1 shows a simple ONCS for a NILE Network in which eight NILE Units participate.

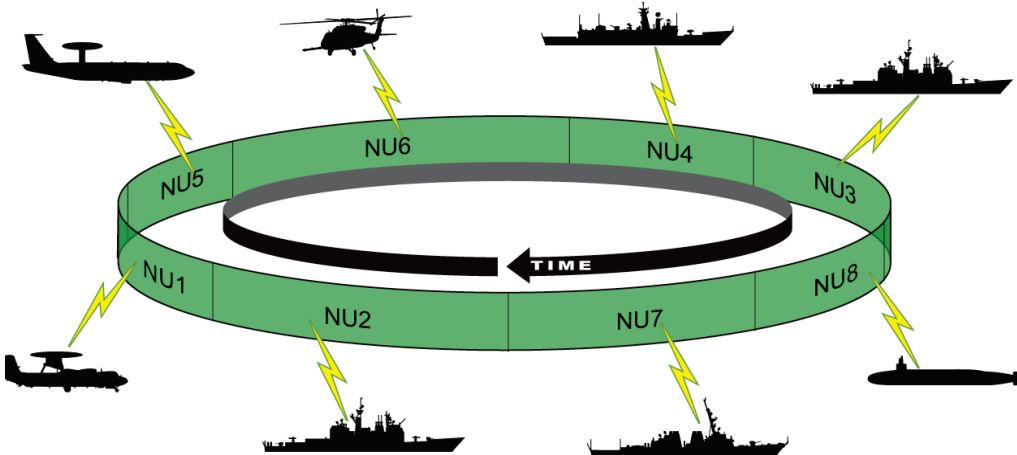


Figure 2A.2-1 Operational Network Cycle Structure

An NCS can be defined by the planner, or the SNC can calculate the NCS, based on the capacity needs and access delays supplied for each unit in the network. Once the network is operational using the NCS it is called an ONCS.

2A.2.3 NILE Unit Parameters

□ Unit Identification

Every unit has a unique designator, for example, a ship's name. Operators use this to identify their unit from the list of all the units in the Super Network.

□ Link 22 Address

Every unit in the Super Network has a unique, 15-bit (five-digit octal) Link 22 Address. This is the same structure as used for Link 16 unit addresses. Internally within Link 22 this address is represented using only 7-bits so that the transmission of address information uses less bandwidth. This 7-bit representation is called a NILE Address (valid values 1-125).


A unit operating on both Link 22 and Link 16 must use the same address on both links, and therefore the Link 22 Address will be the same as the address used on Link 16.

□ Track Number Blocks

Each unit must be assigned a unique range of 19-bit Track Numbers (TNs) to use in reporting tracks. The TNs have the same format as used in Link 16.

□ Role Takeover

The amount of time that elapses before a role is declared lost must be defined. Takeover of the lost role by the Standby unit can be set to occur either automatically or manually.



This page is intentionally left blank.

Section B Planning

Link 22 requires only a small degree of planning, which is negligible when compared to the complexity of the planning necessary for Link 16. Link 22 planning can be as simple as identifying the participating Link 22 units and their available radio types. As Link 22 provides the capability to either manually or automatically adapt the parameters during the operation of the system, the level of the planning is not critical to the performance of Link 22. Note that the term “planner” throughout this section refers to any planner or planners.

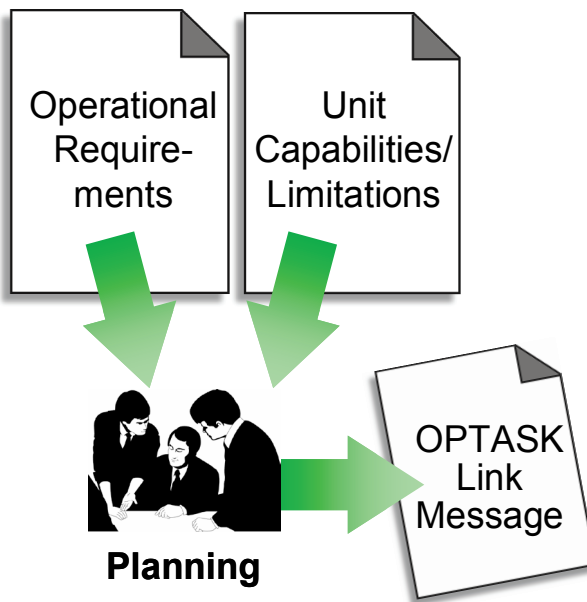


Figure 2B-1 Link 22 Planning

are available. The numbers and types of data links to be used must be determined, along with which units will participate on which data links, and which units will provide forwarding between them. The planner has to attempt to provide the required communications using the available resources. The output of the process is the Operational Tasking (OPTASK) Link Message (OLM).

The inputs and outputs of the data link communications planning process are shown in [Figure 2B-1](#). The planner is supplied with the operational requirements for the data link communications, plus the capabilities and limitations of the units that are to be deployed to perform the operation. The planner performs the communications network planning/design function to define the required data link configuration. The operational requirements include the connectivity requirements, which must be addressed to ensure that the required communications between units

When Link 22 is to be used, the Key Parameters listed in the overview must be derived. These are output as the Link 22 segment of the OLM. For each operation or exercise, an OLM must be distributed to all intended participants. The OLM must include, at a minimum, those Link 22 parameters required to be preloaded by each participant. Where a given Link 22 operation involves multiple networks, they should all be addressed by the same OLM. It is mandatory that all participants receive the same OLM.

Ensure that all participants receive the same OLM version by timely means!

The planning function can be broken down into three phases.

- Analyzing the Input Information
- Determining the Key Parameters
- Generating the OLM

This section considers only the planning functions related to Link 22.

2B.1 Analyzing the Input Information

The capabilities and limitations of each unit that will be involved in the data link must be analyzed. These are used to limit the generation of Key Parameters. For example, a unit cannot be assigned to two different NILE networks of media type HF FF at the same time when the unit has only one HF FF radio available. With only one HF FF radio available, the unit only has the capability to operate on one HF FF network at a time. The operational requirements detail what the units will be doing, and the analysis can therefore derive parameters, such as the expected network capacity and access delay.

2B.1.1 Capabilities and Limitations

The principal capabilities and limitations that need to be known or assessed by the planner are in the following list.

- Whether the unit can perform the SNMU role
- Whether the unit can perform the NMU role
- Whether the unit has functional limitations (for example, does not implement probing)
- The quantity of the unit's available Link 22 HF FF radios
- The quantity of the unit's available Link 22 UHF FF radios
- The quantity of the unit's available Link 22 HF EPM radios
- The quantity of the unit's available Link 22 UHF EPM radios
- Whether the unit is a land, sea, air, or subsurface unit type
- Whether the unit can perform as a Forwarder to/from Link 22

2B.1.2 Operational Requirements

From the operational requirements, the planner must assess the following.

- Which units are involved in the operation
- Each unit's required tactical traffic load (capacity need)
- Each unit's required Access Delay
- The Frequency constraints and/or clearance
- The Start Date/Time of the operation
- The Start Date/Time of the Link 22 data link
- The Start Date/Time of each individual NILE Network
- The starting location and expected movements of the involved units - for example, will each unit be available at exercise or operation start?
- Expected propagation conditions for the network's waveforms

After the basic list of units and mission requirements are identified, the data link planner may need to request additional units to ensure that the required operational connectivity among all participants is met, operating either as a single Link 22 Super Network or in a wider, multilink environment.

2B.2 Determining the Key Parameters

The Key Parameters of Link 22 discussed in section A must be determined when planning an operation or exercise. Many parameters have recommended default values. The required parameters are in three categories.

- Super Network Parameters
- NILE Network Parameters
- NILE Unit Parameters

Figure 2B.2-1 presents a checklist of required planning parameters and their recommended values. Note, however, that most Link 22 parameters can be modified during operations, so their initial settings are not critical.

Parameters	Recommendation
Super Network	
Start Date/Time	
Roles (SNMU & Standby)	
Crypto	
NILE Network	
Media Type	
Media Setting Number	HFFF: 4 All others: 1
Frequency	N/A
Fragmentation Rate	1
LLC Integrity	Disabled
Network Start Date/Time	N/A
Initialization Type	Short
Network Members	
Roles (NMU & Standby)	
DTDMA Enabled/Disabled	Enabled
Network Cycle Structure	
NILE Unit	
Unit Identification	
Link 22 Address	00001
Track Number Blocks	
Role Takeover	Not Automatic, 2 minute timeout

Figure 2B.2-1 Link 22 Parameters Checklist

2B.2.1 Super Network Parameters

□ Start Date/Time

The planner must define a date and time at which the Link 22 Super Network is planned to start. The day is used to define the first DOW: that is DOW = 1 on this date. The date on which a Link 22 network starts can be later than the Super Network Start Time, in which case the DOW will be calculated as an offset from the Super Network Start Time. The DOW value ranges from 1 to 7, and then rolls over back to 1. The DOW is used during encryption and decryption.

□ Roles (SNMU & Standby)

The planner must select the units that will perform the special Super Network roles: the SNMU and its Standby.

It is recommended that the SNMU has the following characteristics.

- It is planned to be present at the start of the Super Network
- Its DLP is capable of performing the SNMU role
- It is planned to be located at the geographic center of the Task Force

It is recommended that the Standby SNMU has the following characteristics.

- It is planned to be an RF Neighbor of the SNMU, to minimize communications and provide easier loss detection
- It is planned to be present at the start of the Super Network
- Its DLP is capable of performing the SNMU role

The presence of the SNMU and its Standby is not mandatory for the initialization of the Super Network. The special DLP capabilities required to perform the SNMU role are indicated in the Minimum Implementation Note column of [Figure C.1-2 Control and Status Interface Message Minimum Implementation \(DLP to SNC\)](#) in [Appendix C](#).

□ Crypto

The planner must obtain the identification information for the crypto keys that are valid for this timeframe from the participating NILE units' national crypto key distribution agency. These procedures may vary depending on the country, and they are detailed in the LLC Key Management Plan [[LLC KMP](#)]. Each key will have a "Key Use and Circuit Identification," which is referred to as the crypto key's Short

Title. If the key is encrypted, a Short Title for its encryption key is also needed. Each key is further identified by a Crypto Variable Logical Label (CVLL), which is an integer value in the range 1-127. Multiple keys may be needed to cover the timeframe of the operation or exercise.

2B.2.2 NILE Network Parameters

Link 22 supports eight different types of media, of which four are currently defined as follows.

- HF FF (3KHz as defined in [\[STANAG 4539\]](#))
- UHF FF (3KHz as defined in [\[STANAG 4444\]](#))
- HF EPM (25KHz as defined in [\[STANAG 4205\]](#))
- UHF EPM (25KHz as defined in [\[STANAG 4372\]](#))

It supports up to eight networks in a Super Network. The planner should define a minimum of one network per media type that will be used in the operation or exercise.

□ Media Type

Each network is defined to use one currently defined media type. The planner must select the media type for each network currently (HF or UHF), and currently whether it is fixed frequency or frequency hopping. UHF is used only for Line-of-Sight connectivity, whereas HF is used for Beyond Line-of-Sight (BLOS) communications. Frequency hopping can be selected when a greater degree of TRANsmission SEcurity (TRANSEC) is desired.

□ Media Setting Number

The planner selects a Media Setting Number (MSN) for each network, based on the network's media type. The MSN defines the waveform, coding, modulation scheme, and repetition rate used for a network. The degree of throughput varies inversely with the robustness of the MSN. Current MSN selections are described in [Figure 2B.2-2](#).

For HF media, the choice of MSN will be influenced by the operation's geodetic location, with the more robust waveforms selected for Polar Regions.

Media Type	Media Setting Number	Meaning
HF FF	1	Lowest throughput and highest robustness
	2	Low/medium throughput and high to medium robustness
	3	Low/medium throughput and medium robustness
	4	Medium throughput and low/medium robustness
	5	Medium/high throughput and medium robustness
	6	Highest throughput and lowest robustness
HF EPM	1	Highest throughput and lowest robustness
	2	High throughput and medium/low robustness
	3	Medium throughput and medium robustness
	4	Lowest throughput and highest robustness
UHF FF	1	No choice – must be 1
UHF EPM	1	Highest throughput and lowest robustness
	2	High throughput and low/medium robustness
	3	Medium throughput and medium robustness
	4	Lowest throughput and highest robustness

Figure 2B.2-2 Media Setting Numbers

□ **Frequency**

Link 22 HF and UHF Fixed Frequency media may use the same radios as used by Link 11, and EPM radios use the same frequency bands as Link 11. This means that the use of frequencies for Link 22 is no different than the already established practices used for Link 11. There are no frequency clearance problems as there are with Link 16. The planner selects which of the Link 11/22 designated frequencies to use for each HF FF or UHF FF network initialization. For each HF EPM or UHF EPM network initialization, the planner must select a frequency hopset. For HF networks, certain frequencies are better at different times of day, and this affects the choice of frequency if more than one frequency is available. [Figure 2B.2-3](#) lists the frequency ranges for HF and UHF media. For the fixed frequency media the actual frequency has to be specified. For the EPM media, a hopset has to be defined which controls the selection of the frequencies used within the specified range.

Media	Frequency
HF	2–30 MHz
UHF	225–400 MHz

Figure 2B.2-3 Media Frequency Range

A hopset is defined by a channel code, a net number, and a frequency plan. A hopset has the format CNNNFF (6 hexadecimal digits (0-F)), where C is the Channel Code, NNN is the Net Number and FF is the Frequency Plan. The Channel code is either 0 (Full-band) or 1 (Sub-band), with 2-F not used. The Net number is 000-3E7 hex (0-999 decimal), with 3E8-FFF not used. The Frequency Plan is 00-FF hex. For Example the hopset “123E0A” means channel code = sub-band, net number = 23E hex or 574 decimal, and the frequency plan is 0A hex or 10 decimal.

□ **Fragmentation Rate**

The planner must select a fragmentation rate for each network, based on the network’s media type. These selections are described in [Figure 2B.2-4](#).

Media Type	Fragmentation Rate	Meaning
HF FF and UHF FF	1	Low throughput and high robustness
	2	Medium throughput and medium robustness
	3	High throughput and low robustness
HF EPM and UHF EPM	1	No choice – must be 1

Figure 2B.2-4 Fragmentation Rate

Normally, the planner would select a fragmentation rate of one. Higher fragmentation rates are used only under optimal RF conditions, so their use typically cannot be foreseen during the planning phase of an exercise or operation. The fragmentation rate can be changed during operations by performing a Network Re-Initialization.

□ **LLC Integrity**

LLC Integrity is a function that enables extra checking within the LLC. This function reduces the number of bits available for tactical traffic, but can increase system robustness when propagation conditions are unknown or enemy disruption activities are expected. The planner must choose whether to enable or disable LLC Integrity for each defined network.

□ **Network Start Date/Time**

The OLM includes the Super Network Start Date/Time. The planner must also indicate a start date and time for each individual network.

□ **Initialization Type**

The planner can select from one of two methods to initialize each network.

- Short initialization
- Probing initialization

If communication conditions are likely to be good, short initialization will usually be selected. If conditions are likely to be unknown, probing initialization can be selected, enabling different MSNs to be used to determine the most successful MSN value. Probing should not be selected if either of the following two conditions exists.

- When there are time constraints on initiating network operations, because probing takes longer than short initialization
- Some units in the network do not have the advanced capability to perform probing

If a unit requires an operator to manually control a radio's frequency setting, and multiple frequencies may be probed (by using reprobe), the operator may not be able to correctly change the frequency at the required times and so the Probing results for that unit may not be valid. The decision of which settings to use are based on the Probing results from all units, and invalid results could affect the decision, and so it is recommended that when using multiple frequencies, units without frequency control should not be included in the probing.

The initialization type may be different for each network. If probing initialization is selected, the planner must specify the initial list of MSNs to be probed. The MSNs should be ordered so that the final MSN to be probed is expected to be the most robust, as it uses the last probing configuration to distribute the selected configuration. This also minimizes the number of media reconfigurations.

□ **Network Members**

Each unit can be placed in up to four networks, based on its radio capabilities. The planner uses information on each platform's capabilities and limitations to ensure that the network members have the selected media type capability.

When more than one network is defined, at least one unit must be placed in multiple networks, so that this unit can relay data between the networks. A minimum of two units in both networks is recommended, so that no single point of failure is introduced into the system. [Figure 2B.2-5](#) shows two defined networks, one HF FF and one UHF FF. Two units, addresses 100 and 101, are participating in both networks.

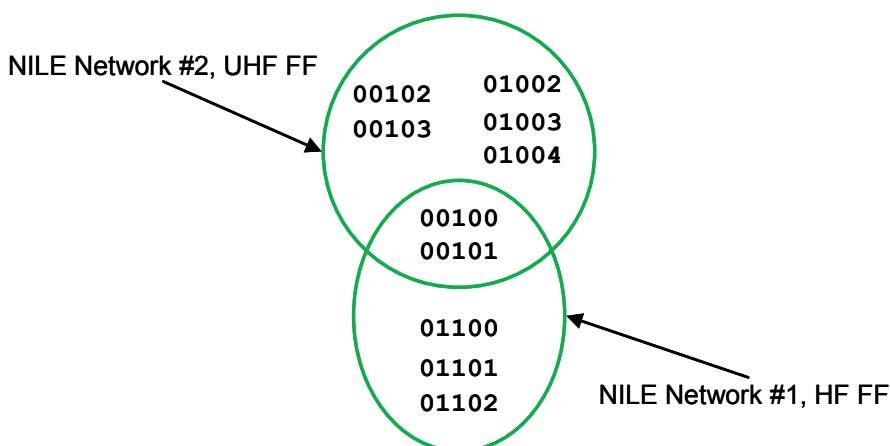


Figure 2B.2-5 Network Membership

□ **Roles (NMU & Standby)**

The planner must select for each network the units that will perform the two special NILE network roles: the Network Management Unit (NMU) and its Standby.

It is recommended that each network's NMU has the following characteristics.

- It is planned to be located at the geographic center of the network
- It is planned to be present at the start of the network
- Its DLP is capable of performing the NMU role
- It is preferably the SNMU, if the SNMU is a member of this network

It is recommended that each network's Standby NMU has the following characteristics.

- It is planned to be an RF Neighbor of the NMU, to minimize communications and provide easier loss detection
- It is planned to be present at the start of the network
- Its DLP is capable of performing the NMU role

The presence of the NMU and its Standby is not mandatory to initialize the network, except when initialization with probing is performed. The special DLP capabilities required to perform the NMU role are indicated in the Minimum Implementation Note column of [Figure C.1-2 Control and Status Interface Message Minimum Implementation \(DLP to SNC\)](#) in Appendix C.

□ ***DTDMA Enabled/Disabled***

If the traffic requirements in a network are expected to change during the operation or exercise, the planner may want to enable Dynamic TDMA (DTDMA) for the network. This allows units with unused capacity to automatically donate some of their extra capacity, either temporarily or permanently, to units that request additional capacity. This capability helps to relieve message traffic congestion.

□ ***Network Cycle Structure***

After the networks and the units in each network have been determined, the Network Cycle Structure (NCS) of each network can be defined. The planner has to choose from the following two options.

- [Planner Defines the NCS Manually](#)
- [The SNC will calculate the NCS](#)

■ ***Planner Defines the NCS Manually***

When planners define the NCS, the size and owner of each timeslot must be specified. This may be as simple as defining that all units will have the same number and duration of timeslots. Or it may involve the planner manually computing a more complex solution. There could also be an external planning tool available into which the planner enters the traffic load prediction, and the tool generates an NCS. Possibly the planner has available pre-defined NCS for specific mission profiles and just needs to select one that matches the mission being planned. Whatever the method, the result is that the planner has an NCS that they want to be used.

Long timeslots generate a more efficient NCS, but also a potentially longer wait between transmission opportunities. Short timeslots allow more access opportunities, but reduce the overall assigned capacity and efficiency.

An example NCS is shown in [Figure 2B.2-6](#). Units can be assigned more than one timeslot in an NCS, as shown for units 100, 101, 102, and 103. This decreases the unit's access delay. Priority injection slots are short timeslots with no owner (owner = 0). The insertion of priority injection slots is discussed further in subsection [2B.4 Additional Planning Topics](#).

Owner	100	101	1002	0	1003	1004	102	103	100	101	102	103
Size (minislots)	8	8	6	4	6	6	8	8	8	8	8	8

Figure 2B.2-6 Example NCS

A timeslot's size is specified as a number of minislots. A minislot has a defined length of time, based on the media type. Subsection [2B.4 Additional Planning Topics](#) provides details on the parameters involved.

■ **The SNC will calculate the NCS**

The SNC calculated NCS is expected to be the normal selection for planning when traffic load prediction is available. If the planner selects that the SNC will calculate the NCS, then the following information for each network must also be supplied. The values supplied may be based on historical data derived from the NU Performance information, as detailed in subsection [2B.4 Additional Planning Topics](#). For each unit, the following two parameters must be defined.

- [Capacity Need](#)
- [Access Delay](#)

◇ **Capacity Need**

Knowledge of the number and types of tracks that each unit is expected to report can be used to determine the approximate number of Tactical Message Words (TMW) per second that each unit is expected to transmit. [Figure 2B.2-7](#) lists the average TMW per second for the most frequent messages, which can be used as a guide. These values are calculated from the track repetition rate and the average number of words transmitted for the track (message) type, as defined in [\[STANAG 5522\]](#).

Message Type	Average TMW Per Second
Air Participant Location and Identification (PLI)	0.115
Surface (SUR) PLI	0.018
Subsurface (SUB) PLI	0.045
Air Surveillance	0.109
Surface Surveillance	0.014
Subsurface Surveillance	0.014
Land Track Surveillance	0.021

Figure 2B.2-7 Typical Real Time TMW per second

The possible capacity need values are defined in Figure 2B.2-8. The planner needs to include possible relay traffic in the calculation of Tactical Message Words per second.

For contingency, allocate an additional 15% – 20% more than the calculated amount for the predicted tactical traffic.

TMW/sec	Capacity Need
0.25	Ultra Low
0.5	Very Low
1	Low
1.5	Medium Low

TMW/sec	Capacity Need
2	Medium
3	Medium High
4	High
8	Very High

Figure 2B.2-8 Capacity Need

◇ Access Delay

Access Delay is the maximum time between transmissions required by the unit. This value depends mostly on the types of tracks that the unit is expected to report, as shown by the update rates for different types of tracks in [Figure 2B.2-9](#). Other tactical message transmission requirements also need to be taken into account, such as for commands and track management messages.

Track Category	Seconds	Track Category	Seconds
Air, Real Time	12	Subsurface, Real Time + HUR	24
Air, Real Time + HUR	**	Subsurface, Non Real Time	N/A
Air, Non Real Time	48	Land, Real Time	96
Air, SLURP	24	Land, Real Time + HUR	24
Surface, Real Time	96	Land, Non Real Time	140
Surface, Real Time + HUR	24	Ballistic Missile, Real Time	12
Surface, Non Real Time	140	Ballistic Missile, Real Time + HUR	**
Subsurface, Real Time	96	Ballistic Missile, Non Real Time	48

** Air/Ballistic Missile tracks designated High Update Rate (HUR) shall be reported on the interface following every sensor update, but no more often than every 6 seconds for air tracks, and as requested in the FJ7.1 message for Ballistic Missile tracks.

Figure 2B.2-9 Update Rates for Tracks

The unit's access delay can be approximated by using the value for the track type with the highest update rate that the unit is expected to report. The access delay values that must be supplied are defined in [Figure 2B.2-10](#). "Unlimited" indicates that the unit's access delay is not considered to be operationally significant.

When the SNC calculates the NCS, it is possible that all requested parameters cannot be met. Therefore, the planner must select values for the following two parameters, which are progressively applied to the overall NCS calculation.

- Access Delay Tolerance
- Efficiency

Access Delay	Seconds
Unlimited	—
Long	≤ 48
Medium Long	≤ 24
Medium Short	≤ 12
Short	≤ 8
High Update	≤ 4

Figure 2B.2-10 Access Delay

◇ **Access Delay Tolerance**

The access delay tolerance value defines how closely the NCS calculated by the SNC must meet the access delay parameters of each of the units in the NCS. This value is defined in [Figure 2B.2-11](#).

Delay Tolerance Level	Percent
No Tolerance	0%
Low Tolerance	5%
Medium Tolerance	15%
High Tolerance	30%

Figure 2B.2-11 Access Delay Tolerance

◇ **Efficiency**

The Efficiency is defined as the percentage of the NCS that is available for the transmission of data. The preamble at the beginning of a timeslot or the last minislot in HF EPM reduces the amount of user throughput available in the timeslot. Efficiency affects the number and duration of timeslots. Higher efficiency values will generate longer timeslots, so that the preamble is a smaller percentage of the timeslot, which may produce longer access delays. Efficiency is specified in the range 75–100 percent.

2B.2.3 NILE Unit Parameters

The following data must be defined for each unit.

- Unit Identification
- Link 22 Address
- Track Number Blocks
- Role Takeover

Other optional unit parameters are discussed in section [2B.4 Additional Planning Topics](#) below.

□ **Unit Identification**

Each Link 22 unit’s unique designator must be supplied, so that the operators can determine which unit they are. A call sign may optionally be included.

□ **Link 22 Address**

Each Link 22 unit must be assigned a unique address. In a multilink environment, this is referred to as the Interface Unit (IU) address. An IU address must be unique across

all of Link 22, Link 11, Link 11B, and Link 16. [Figure 2B.2-12](#) summarizes the preferred assignment of Link 22 addresses. Note that all IU addresses are octal. The IU type abbreviations are described in [Figure 2B.2-13](#). It should be noted that addresses 00000, 00077, 00176, 00177, 07777 and 77777 octal are not valid, and when an address range is defined it does not include these values.

IU Type/Function	Legal Range(Octal)	Preferred Range (Octal)
NU	00001–77776	00001–00175
FNUA/FNUAB	01–76	01–76
FNUB	100–175	100–175
Link 11 capable NU	00001–77776	01–76
Link 11B capable NU	00001–77776	100–175

Figure 2B.2-12 Link 22 IU Addresses

Abbreviation	Meaning	Description
FNUA	Forwarding NILE Unit to/from TDL A (Link 11)	Performs data forwarding between Link 22 and Link 11
FNUB	Forwarding NILE Unit to/from TDL B (Link 11B)	Performs data forwarding between Link 22 and Link 11B
FNUAB	Forwarding NILE Unit to/from TDLs A and B	Performs data forwarding between Link 22 and Link 11, and Link 22 and Link 11B

Figure 2B.2-13 Interface Unit Definitions

Link 22 and Link 16 use the same IU address range, so in a multilink environment that does not include Link 11 or Link 11B, the entire range of addresses can be used.

In a multilink environment that includes Link 22 and Link 11 or Link 11B, every effort should be made to assign Link 22 addresses in the Link 11/11B range: 01–76 (Link 11) or 100–175 (Link 11B), octal. This will enable NILE Units (NUs) to properly exchange addressed messages with Participating Units (PUs) on Link 11 and Reporting Units (RUs) on Link 11B. Addresses in these ranges are termed “low IU addresses”.

If it is not possible to assign only low IU addresses, addresses greater than 177 octal should be assigned only to the NUs that are least likely to exchange addressed messages with PUs and RUs. Those NUs with command authority, or that are likely to originate handover requests or orders addressed to PU/RUs, should be assigned low

IU addresses; that is, addresses below 176 octal. Orders and requests cannot be forwarded directly to Link 11/11B when the source TN is 00200 octal or greater.

A forwarder from Link 22 to Link 11 is to be assigned a single address in the range of 01–76 octal, because it participates actively as a PU and an NU and uses a single address on both links and for data forwarding. For a similar reason, a forwarder from Link 22 to Link 11B should be assigned a single address in the range of 100–175 octal. In addition, Standby forwarders should be assigned addresses as described here.

An NU capable of Link 11 should be assigned a Link 22 address in the range of 01–76 octal, even if it plans to operate only on Link 22. This expedites the unit’s activation of Link 11 and prevents confusion if the unit ceases using its Link 22 capability. For similar reasons, an NU capable of Link 11B operation should be assigned a Link 22 address in the range of 100–175 octal.

For multilink-capable IUs, it is recommended that a unit be assigned the same IU address on Link 22, Link 16, and Link 11

□ **Track Number Blocks**

Each NU must be assigned a unique range of Track Numbers (TNs) to use in reporting tracks. Track numbers are 19-bit values, which are represented as two 5-bit fields followed by three 3-bit fields. The 5-bit fields are represented using characters 0-7 and A-Z, excluding characters I and O. The 3-bit fields are represented as octal (0-7). These numbers must be unique across all of Link 22, Link 11, and Link 16. TNs can be categorized as Low TNs and High TNs, as shown in [Figure 2B.2-14](#). Link 11/11B uses only Low TNs. Link 16 and Link 22 can use any TNs.

	Low TNs	High TNs
Value	00000 – 07776 (Both Octal or Track Number Format) (uses only the least significant 12 bits)	10000–1777777 (Octal) 0A000–ZZ777 (Track Number Format) (uses more than 12 bits)
Purpose	Track origination on Link 16, Link 22, or Link 11/11B (with leading zero omitted) Data forwarding of High TNs to Link 11/11B – referred to as Data Forwarding TNs	Track origination on Link 16 and Link 22

Figure 2B.2-14 Track Numbers

TN blocks should be at least 50% larger than the maximum number of simultaneous tracks a NU may be expected to originate.

High TNs normally should be allocated only when there are not enough Low TN blocks.

A High TN block must be composed entirely of numeric TNs, or entirely of alphanumeric TNs, not a combination of both.

For multilink-capable NUs, that may operate in either the Data Forwarding or Concurrent mode, the same Low TN block is used on all links.

□ Role Takeover

During an operation or exercise, if the SNMU or an NMU is lost, the Standby SNMU or the Standby NMU should take over the role of the lost SNMU or NMU. The planner can define the time that must elapse before the Standby decides that the SNMU or NMU is lost (in the range of 2–15 minutes). The planner can also define whether the SNC of the Standby will or will not automatically take over the role. By default, the SNC does not automatically take over the role. Instead, the SNC informs the DLP, and it is the responsibility of the DLP/Operator to decide whether or not to take over the lost role.

2B.3 Generating the OLM

After the planner has selected all required Link 22 parameters for the operation or exercise, the OLM can be generated. This message contains the operational details required by each unit participating in the operation or exercise.

The OLM has been modified in order to include the Link 22 segment. This modified version of the OLM has been initially incorporated into the AXP-5 (Experimental Tactics Document) as [EXTAC 779] Annex C. The final OPTASK LINK message will be defined in ADatP-3 and also potentially in the US in MIL–STD–6040.

The two simple examples below illustrate the OLM generation process. The first example demonstrates the simplicity of Link 22 planning. The second example is slightly more detailed. Both examples were based on the OLM definition that was current at the time of publication.

2B.3.1 Example #1

This example illustrates the simplicity of Link 22 planning. It provides only the Link 22 portion of the OLM, and contains only its required sets and fields. The Super Network in this example has the following requirements.

- The Super Network is composed of 1 HF FF Network
- Two units; Link 22 addresses 00100 (SNMU and NMU) and 00101 (Standby SNMU and Standby NMU)
- Short initialization with NCS computation by the SNC
- DTDMA and LLC Integrity are enabled

The Link 22 portion of the OLM for this example is given in [Figure 2B.3-1](#). This is the only Link 22 information required to produce a fully functioning Link 22 operation or exercise.

1	LNKXXII/LINK 22 SEGMENT//
2	NSNET/NATO0000B/00100/00101/011400ZJUL2007/1/2//
3	JCRYPDAT/1/AKAK123-A//
4	NNET/1/00176/00100/00101/SNC/DTDMA:ENABLE/DIVS:ENABLE//
5	NNETPART/00100/00101//
6	NNMEPARS/HFFF4539/1/4.5MHZ/-/-/-/SHORT/NST:011400ZJUL2007/-/HFFF1//
7	NUBWR/85/2/00100/5/3/00101/5/3//
8	NCRYPLST/1/011400ZJUL2007//
9	NUDATA/SHIP:PACDG/-/00100/00200-00777/-/-/ENABLE/2//
10	NUDATA/SHIP:NIMITZ/-/00101/01000-01377/-/-/ENABLE/2//

Figure 2B.3-1 Link 22 Segment of OLM for Example #1

Explanations of each of the sets and fields of an OLM are included in the more detailed second example.

2B.3.2 Example #2

This example is slightly more detailed to illustrate the use of additional OLM Link 22 sets and fields. Figure 2B.3-2 represents the architecture for this second example.

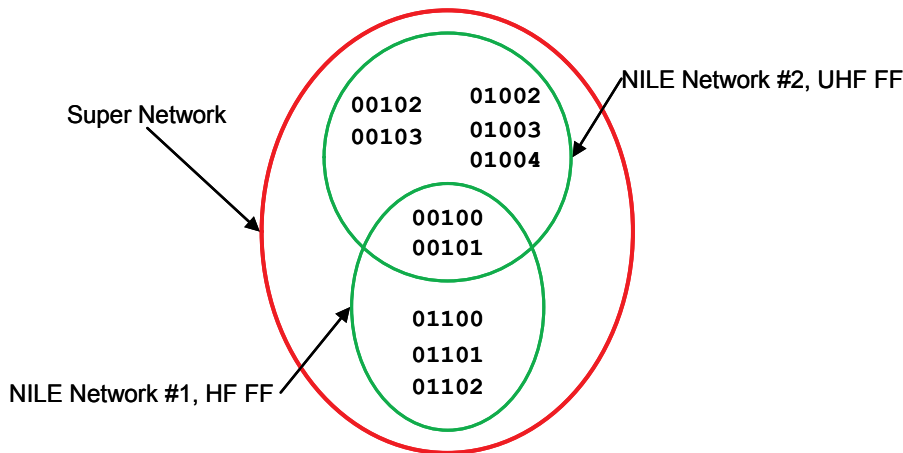


Figure 2B.3-2 Example #2 Architecture

The requirements for the Link 22 Super Network in this example are as follows.

- The Super Network is composed of one HF FF NILE Network and one UHF FF NILE Network. It includes 10 Link 22 units. The radio and SPC equipment available on each unit are as follows
 - Three units are HF FF capable only
 - Five units are UHF FF capable only
 - Two units are HF FF and UHF FF capable simultaneously
- The Super Network starts on 1 July, 2006, at 1400Z, and is expected to remain operational for one week
- HF conditions are unknown. Initialization with probing, secondary HF FF frequencies, and integrity verification service are selected for the HF Network. The HF network must be initialized sooner than the UHF network because probing initialization takes longer
- Two NUs (00100 and 00101) serve as relays between the HF FF and UHF FF networks. These Link 22 relaying NUs require extra bandwidth

- Data forwarding units (for forwarding data to/from Link 11 and/or Link 16) must be given extra transmission capability and lower access delay. These NUs are the addresses 00100, 00101, 00102 and 00103
- Dynamic TDMA Management is used for both networks. Automatic NCS computation by the SNC is used for the HF FF network. OLM-defined NCS is to be used for the UHF FF network

The Figure 2B.3-3 shows the OPTASK LINK message for this example.

1	EXER/LINK 22 GUIDEBOOK//
2	MSGID/OPTASK LINK 22 2007/NILE PMO//
3	REF/A/DESC:ADATP-33 (WORKING DRAFT)/NATO/YMD:20060201//
4	REF/B/DESC:OPTASK LINK MESSAGE (LINK 22) ANALYSIS AND DEFINITION /LINK OIWG/YMD:20050713//
5	POCLINK/TACTICAL COMMANDER/SMITH/CIV/SHIP:NIMITZ/TEL:619-555-1234//
6	PERIOD/0114000ZJUL/072359ZJUL//
7	IVCCN/DCN/P/WIN:5234.5KHZ//
8	CORRDEC/AUTO DEFAULT//
	•
	•
	•
9	LNKXXII/LINK 22 SEGMENT//
10	NSNET/NATO0000A/00100/00101/011400ZJUL2006/2/10/-//
11	JCRYPDAT/1/AKAK123-A/AKAT2345-A/1//
12	NNET/1/00176/00100/00101/SNC/DTDMA:ENABLE/DIVS:ENABLE//
13	NNETPART/01101/01102/00100/00101/01100//
14	NNMEPARS/HFFF4539/1/4.5MHZ/14.5MHZ/-/-/PROBE/- /PST:011330ZJUL2006/HFFF1/HFFF2/HFFF3/HFFF4/HFFF5/HFFF6//
15	NUBWR/85/2/01101/4/1/01102/4/1/00100/5/4/00101/5/4//
16	NCRYPLST/1/011300ZJUL2006//
17	NNET/2/00175/00100/00101/DLP/DTDMA:ENABLE/DIVS:DISABLE//
18	NNETPART/00100/00101/01002/01003/01004/00102/00103//
19	NNMEPARS/UHFFF4205/3/240.5MHZ/-/-/SHORT /NST:011350ZJUL2006/-/UHFFF1//
20	NNCS/12/00100/8/00101/8/01002/6/00000/4/01003/6/01004/6 /00102/8/00103/8/00100/8/00101/8/00102/8/00103/8//
21	NCRYPLST/1/011300ZJUL2006//
22	NUDATA/SHIP:HAMBURG/-/00100/00200-00777/-/-/ENABLE/2/00200-00777//
23	NUDATA/SHIP:NIMITZ/-/00101/01000-01377/-/-/ENABLE/2/01000-01377//
24	NUDATA/SHIP:GUISEPPE/-/00102/02000-02377/-/-/ENABLE/2/02000-02377//
25	NUDATA/SHIP:CASTILLA/-/00103/02400-02777/-/-/ENABLE/2/02400-02777//
26	NUDATA/SHIP:WINNIPEG/-/01002/A0000-A3776/-/-/ENABLE/2/-//
27	NUDATA/SHIP:FREMM1/-/01003/A4000-A7776/-/-/ENABLE/2/-//
28	NUDATA/AC:E3/-/01004/90000-93776/-/-/ENABLE/2/-//
29	NUDATA/SHIP:ARKROYAL/-/01100/94000-97776/-/-/DISABLE/15/-//
30	NUDATA/AC:PATMAR1/-/01101/9A000-9G776/-/-/ENABLE/2/-//
31	NUDATA/SHIP:FREMM2/-/01102/9H000-9Z776/-/-/ENABLE/2/-//

Figure 2B.3-3 OLM with Link 22 Segment for Example #2

2B.3.3 OPTASK LINK Message

The OLM structures the information into Sets and Fields. Fields are the smallest divisible part of the message, where each field contains the value of a particular parameter. A set is a group of related fields, with the first field of the set being the Set Identifier. Fields are separated by a single “/”, while sets are separated by double “/” (//). In this way, the last field of a set is followed by “//”. This section identifies the fields in the sets. The packing of fields that require special consideration is also discussed.

□ Link 22 Super Network Information Set

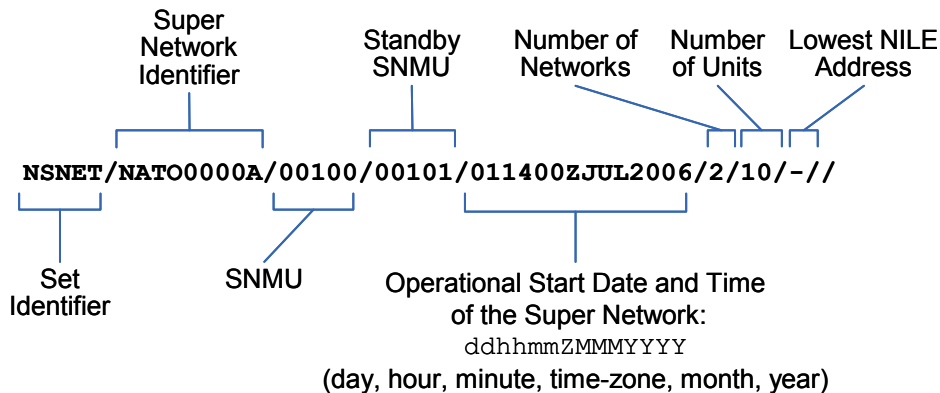


Figure 2B.3-4 NSNET

One NSNET set is required which defines the Super Network. The format of the NSNET set is shown in Figure 2B.3-4. NILE Units (NUs), such as the SNMU and Standby SNMU, are identified by their Link 22 Addresses throughout the Link 22 Segment of the OLM. The operational start date and time of the Super Network is specified in the format as shown in Figure 2B.3-4, which is the format used for all date times within the Link 22 sets in the OLM. The Lowest NILE Address field is optional. When optional field values are not specified, a dash “-” is used for the field’s value. NILE addresses default to start at 1. The sum of the number of units plus the lowest NILE address cannot exceed 126 (because the highest NILE address is 125).

□ **Link 16 and Link 22 Cryptographic Data Set**

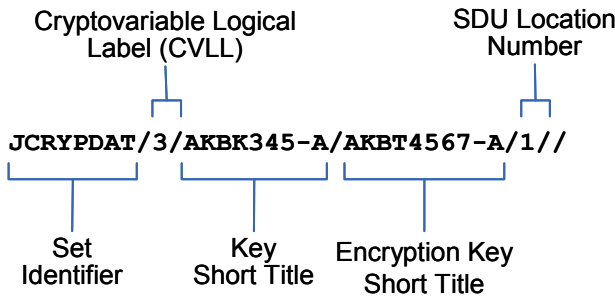


Figure 2B.3-5 JCRYPDAT

One JCRYPDAT set is included for each key that will be used during the lifetime of the Super Network. The format of the JCRYPDAT set is shown in Figure 2B.3-5. The CVLL, Key Short Title, and Encryption Key Short Title values are obtained from a nation’s crypto key distribution agency. The Secure Data Unit (SDU) Location Number (0–63) is optional in this set and may be repeated. Each unit can load the keys into any available LLC key position.

□ **Link 22 Network Information Set**

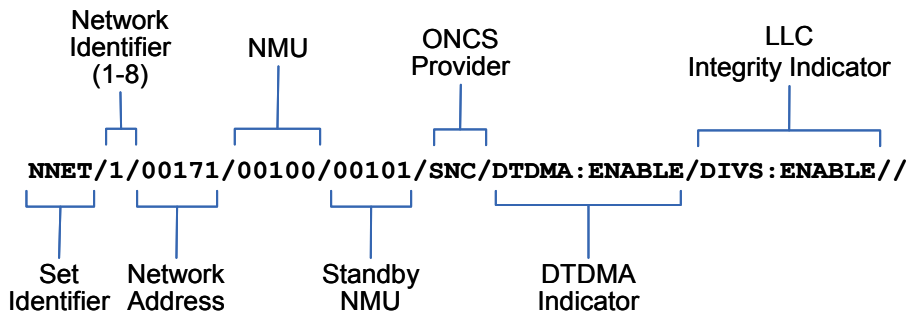


Figure 2B.3-6 NNET

One NNET set is required for each defined network. The format of the NNET set is shown in Figure 2B.3-6. The Network Identifier in the OLM is 1–8, which corresponds to Network ID 0–7, the values that are internal to the DLP and SNC.

□ **Link 22 Network Participants Set**

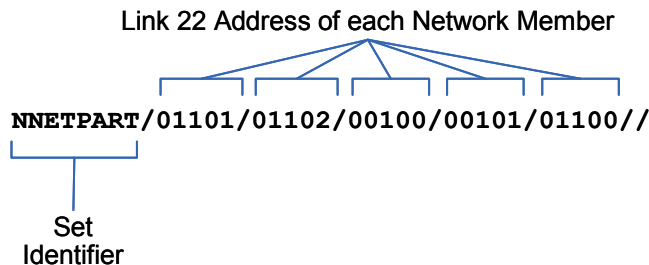


Figure 2B.3-7 NNETPART

The NNETPART set lists the Link 22 Addresses of all NUs that are part of the network identified in the previous NNET set. The format of the NNETPART set is shown in Figure 2B.3-7. This includes Active, Inactive, Receive-Only, and Radio Silent units.

□ **Link 22 Network Media Parameter Settings Set**

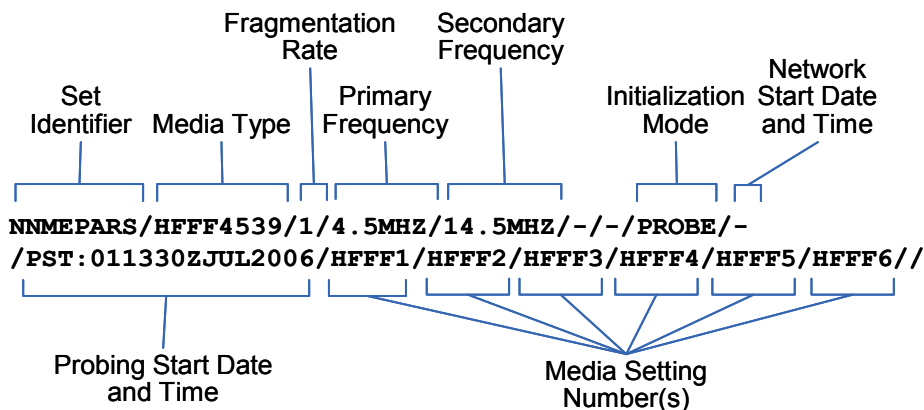


Figure 2B.3-8 NNMEPARS

The format of the NNMEPARS set is shown in Figure 2B.3-8. The secondary frequency may be used by the NMU in subsequent probing sequences if the first frequency is not deemed feasible. The fifth field is used to define the HF Hopset for HF EPM networks. The sixth field is used to define the UHF Hopset for UHF EPM networks. A dash (“-”) is used as a placeholder if a field is not defined. In this example, the Network Start Date and Time field is not defined, because probing

initialization uses the Probing Start Time field. Short initialization would use the Network Start Time field and place a dash in the Probing Start Time field.

□ **Link 22 Bandwidth Requirement Set**

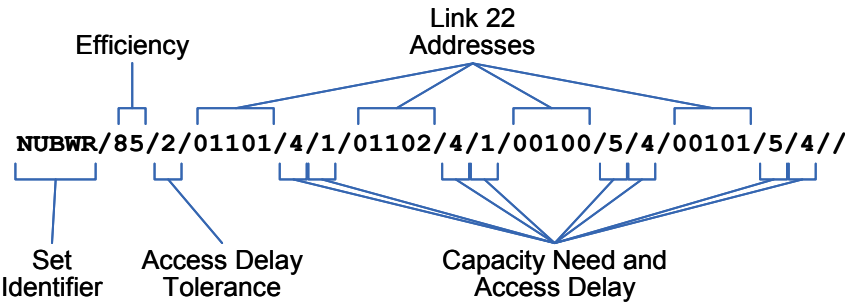


Figure 2B.3-9 NUBWR

The NUBWR set shown in Figure 2B.3-9 is used when the SNC is required to calculate the NCS for the network defined in the previous NNET set. Receive-Only units are not included in the NUBWR set. Access Delay Tolerance, Capacity Need and Access Delay values are defined in Figure 2B.3-10, Figure 2B.3-11, and Figure 2B.3-12 below.

Value	Tolerance Level	%
0	None	0
1	Low	5
2	Medium	15
3	High	30

**Figure 2B.3-10
Access Delay
Tolerance**

Value	Capacity Need	TMW /sec
0	Ultra Low	0.25
1	Very Low	0.5
2	Low	1
3	Medium Low	1.5
4	Medium	2
5	Medium High	3
6	High	4
7	Very High	8

**Figure 2B.3-11
Capacity Need**

Value	Access Delay	Secs
0	Unlimited	—
1	Long	≤ 48
2	Medium Long	≤ 24
3	Medium Short	≤ 12
4	Short	≤ 8
5	High Update	≤ 4

**Figure 2B.3-12
Access Delay**

□ **Link 22 NILE Network Structure Set**

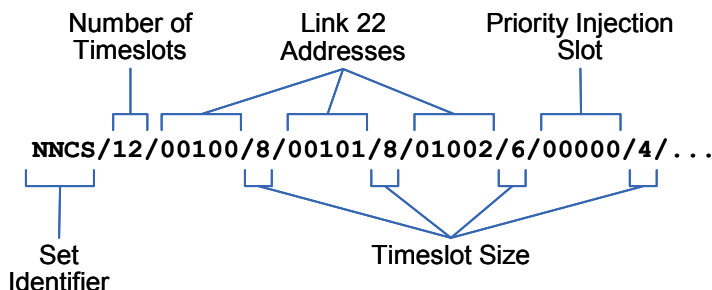


Figure 2B.3-13 NNCS

The NNCS set shown in Figure 2B.3-13 is used when the planner determines the NCS for the network defined in the previous NNET set. Receive-only units are not included in the NNCS set. Priority Injection slots are defined by setting the Link 22 Address of the timeslot (owner) to the value 0.

□ **Network Cryptographic Resource Description Set**

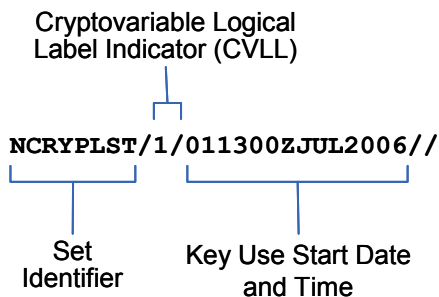


Figure 2B.3-14 NCRYPLST

The NCRYPLST set shown in Figure 2B.3-14, indicates when to use each crypto key defined in the JCRYPDAT set for the network defined in the previous NNET set.

□ **Link 22 Unit Data Set**

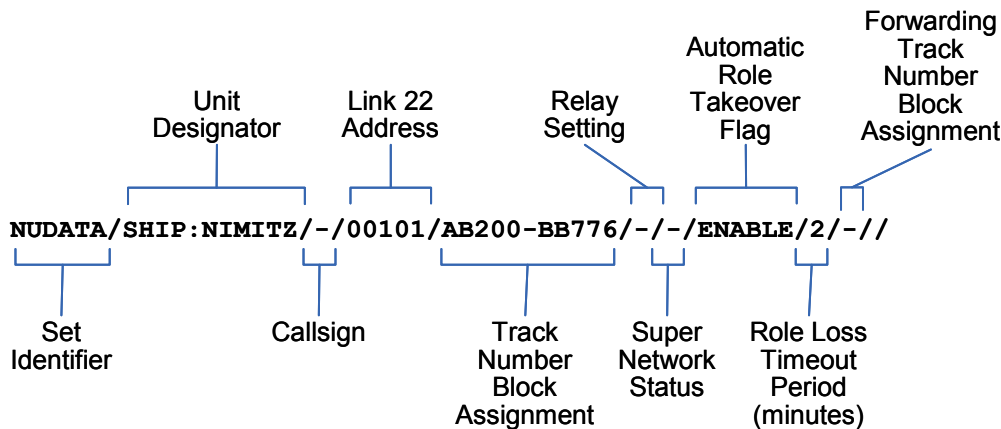


Figure 2B.3-15 NUDATA

One NUDATA set (shown in [Figure 2B.3-15](#)) is required for each NILE Unit, the number of NILE Units being specified in the NSNET set. A dash (“-”) is used as a placeholder for optional fields that the planner does not specify. The order of these sets is important as NILE Addresses are allocated to each unit based on the order they are in the OLM.

There may be NUDATA sets for units that will not participate in the Super Network and even for units that may not be Link 22 capable. This allows the originator of tactical data that is forwarded from another data link to be associated with a NILE Address which saves bandwidth on Link 22. The SNMU can allocate NILE Addresses to other units once the Super Network is initialized.

2B.4 Additional Planning Topics

This section covers details about additional planning activities that may be useful, but are not necessary under most circumstances. The topics covered are as listed below.

- Transmission Needs
- Network Membership Determination
- Planner Defined NCS
- Mission Requirements
- Advanced Unit Parameters
- Advanced OLM Production
- Additional Planning Flowchart

A flowchart of the additional planning process is included at the end of the section in Figure 2B.4-19.

The planner should make provision for Link 22 participants from other regions, including units in transit through areas of operation, as well as for the addition of significant numbers of Link 22 platforms in times of crisis and war. This can be accomplished by giving additional transmission capacity to existing units, so that the extra capacity can be given to new units as they dynamically join the Super Network. Additional transmission capacity is also beneficial for improving reallocation through DTDMA.

2B.4.1 Transmission Needs

The use of a planning tool is recommended, but not required, for advanced calculation of transmission needs. The planner can determine the transmission needs of each unit by considering the following information.

- Numbers and types of tracks the unit is expected to report
- Non-track-anticipated transmission loads
- Connectivity to other NUs
- Role assignments
- Relay needs

□ Tactical Loads

The planner can determine how much (capacity) and how often (access delay) each Link 22 unit will need to transmit. Units needing higher than average capacity include those expecting to have higher than average reporting responsibility, those performing

data forwarding, those in closest proximity to the enemy, etc. It is also necessary to consider that units reporting air tracks transmit their track updates more often than units reporting surface or subsurface tracks. Data forwarding units may also require more frequent opportunities to transmit.

Units with roles (such as a data forwarding unit), and units expected to perform relay, will also require extra transmission capacity. These will be discussed in a separate subsection below.

During an operation or exercise, each unit's average Capacity Need (CN) values are reported every 20 minutes in an NU Performance Data message. This data can be saved for historical purposes. Access Delay (AD) can also be computed based on transmission of tactical traffic. When determining CN and AD values in a future planning session, historical CN and AD data if available can be used to validate the planned values.

□ Connectivity

The two types of connectivity that should be considered when planning a Super Network are as follows.

- Connectivity between networks in the SN
- Connectivity within a single network

Any Super Network containing multiple networks will require that at least one unit participates on multiple networks, so that this unit can relay information between the networks.

Units within the same network may not have direct RF communications due to a number of reasons, such as geographic location and communications conditions. Other units within the same network may have to perform the relay function in these circumstances. Identifying the potential relay units during planning allows assigning extra transmission capacity for the relayed messages.

One example of network connectivity is the case of overlapping networks. In this case, all units belong to more than one network that employs the same media type. This capability potentially doubles the available capacity. The SNC manages the efficient use of the bandwidth, as transmissions are not repeated in the other networks unless retransmission is required to reach the requested reliability.

□ **Bandwidth Calculation**

Planners should calculate the amount of bandwidth in terms of Tactical Message Words (TMW) per second required in the Super Network for each unit. Some typical real-time update rates are provided in [Figure 2B.4-1](#), assuming that all data is available to report but is not changing. If data is changing, it is reported more often. If data is not available, it is not reported at all. Note that not all TMWs are sent for every periodic update. Refer to [STANAG 5522] for details of these transmission rules.

By knowing the numbers and types of tracks that are expected to be reported in the Super Network, an approximation of the track load bandwidth can be calculated, based on the information in [Figure 2B.4-1](#).

Extra bandwidth should be added as necessary for the following.

- Non-track tactical traffic
- Internal Link 22 network management
- Relay
- Data forwarding

The amount of bandwidth required for each unit should also be calculated, using the same information.

Non-track tactical load can be approximated as a percentage of the track load, depending on expected operational requirements of the unit. For example, Data forwarding units may require greater bandwidth than other units.

Internal network management bandwidth requirements for a unit depend on the roles assigned to that unit. All NUs require a small amount of bandwidth for transmitting periodic messages, such as heartbeat technical messages. SNMUs require extra bandwidth for transmitting periodic management updates and periodic information about other NUs. NMUs require extra bandwidth for managing their networks. As a general rule for most NUs, 15–20 percent should be allocated above and beyond tactical traffic requirements.

Message Type	Periodic Rate (sec)	TMW	TMW Periodic Inclusion*	Average TMW per Report	Average TMW per Second
Air PLI	12	PLI POS (F1-1) AIR PLI CAS (F02.2-0) AIR PLI AMC (F02.2-1) PLI IFF (F02.1-0)	1 1/4 1/16 1/16	1.375	0.11458
Surface PLI	96	PLI POS (F1-1) SUR PLI CAS (F02.3-0) PLI IFF (F02.1-0)	1 1/2 1/4	1.75	0.01823
Subsurface PLI	60	PLI POS (F1-1) SUB PLI CAS (F02.4-0) SUB PLI AMC (F02.4-2) PLI IFF (F02.1-0)	1 1 1/3 1/3	2.67	0.0445
Air Surveillance	12	AIR POS (F2) AIR CAS (F5-0) IFF (F01.0-0)	1 1/4 1/16	1.3125	0.10938
Surface Surveillance	96	SUR POS (F3) SUR CAS (F5-1) IFF (F01.0-0) STMIS (F01.0-1)	1 1/4 1/16 1/16	1.375	0.01432
Subsurface Surveillance	96	SUB POS (F4-0) SUB CAS (F4-1) IFF (F01.0-0)	1 1/4 1/16	1.3125	0.01367
Land Track Surveillance	96	INIT (FJ3.5I) EXT (FJ3.5E0) CONT1 (FJ3.5C1) CONT3 (FJ3.5C3)	1 1 1/16 0	2.0625	0.02148

* Indicates how often the TMW is included in a periodic report. For example, 1/4 means that the TMW is included in every fourth periodic report.

Figure 2B.4-1 Typical Real Time TMWs per second

2B.4.2 Network Membership Determination

After the total bandwidth required in the Super Network has been calculated, the planner can determine how many networks are needed to reach the bandwidth requirements. The radio capabilities of the units must be taken into account in order to determine which types of networks can be used. Network bandwidth is primarily based on the following parameters.

- Media type
- MSN
- Timeslot sizes

Small timeslots have a higher percentage of wasted bandwidth because a higher percentage of the timeslot is used for overhead. However, smaller timeslots allow for faster access time, and may be necessary for optimal network operation.

Media	Setting Number	TMW per Sec Range
HF FF	MSN 1	14–15
	MSN 2	20–24
	MSN 3	20–24
	MSN 4	18–32
	MSN 5	33–41
	MSN 6	39–49
UHF FF	MSN 1	124–160

Media	Setting Number	TMW per Sec Range
HF EPM	MSN 1	22–27
	MSN 2	15–17
	MSN 3	15–17
	MSN 4	7
UHF EPM	MSN 1	<CN>
	MSN 2	<CN>/2
	MSN 3	<CN>/3
	MSN 4	<CN>/4

Figure 2B.4-2 Range of TMW per Second per Network

Figure 2B.4-2 shows the range of the number of tactical message words per second that each media type can support. The lower range occurs when the smallest timeslot is used; the upper range occurs when the largest timeslot is used. Each network can have multiple different timeslot sizes, so this table can be used to approximate the bandwidth of a network.

Multiple networks can be used to provide more Super Network bandwidth. Each unit can be assigned to additional networks to give it greater transmission capacity. Placing a unit in multiple networks may improve connectivity, especially when there are units

in the additional network that were not in the networks in which the unit was previously a member.

2B.4.3 Planner Defined NCS

For networks where the planner defines the NCS, the planner or a planning tool defines the owner of each timeslot and the number of minislots contained in each timeslot. A minislot is a defined duration of time that can hold a specific number of tactical message words.

The duration of each minislot for the different types of media is shown in [Figure 2B.4-3](#). The duration of a UHF EPM minislot is a classified number, as shown by the notation “<CN>” in the table. These values are used when determining access delay in an NCS.

Media Type	HF FF	UHF FF	HF EPM	UHF EPM
Minislot Duration (Seconds)	0.1125	0.0480	0.1125	<CN>

Figure 2B.4-3 Minislot Duration

The capacity in TMW of each minislot for different media types and MSNs is given in [Figure 2B.4-4](#).

Media	Setting Number	TMW per Minislot
HF FF	MSN 1	2
	MSN 2	3
	MSN 3	3
	MSN 4	4
	MSN 5	5
	MSN 6	6
UHF FF	MSN 1	8

Media	Setting Number	TMW per Minislot
HF EPM	MSN 1	3 (2)
	MSN 2	2 (1)
	MSN 3	2 (1)
	MSN 4	1 (0)
UHF EPM	MSN 1	6
	MSN 2	3
	MSN 3	2
	MSN 4	1.5

Figure 2B.4-4 Minislot Capacity

Part of each timeslot is used so receiving units can compensate for transmission delays and synchronize with the transmission. For HF FF, UHF FF, and UHF EPM, the

entire first minislot of each timeslot is used; and so cannot contain tactical messages. For HF EPM, only part of the last minislot is used to compensate for transmission delays, and contains one fewer tactical message words than the other minislots of the timeslot, as shown in parentheses in the TMWs per Minislot column of the [Figure 2B.4-4](#). HF EPM uses bits in every minislot for synchronization, and so has less bandwidth available than HF FF. The planner must take into account this lost capacity per timeslot when determining assigned capacity.

Smaller timeslots decrease capacity due to a larger percentage of the timeslot being used for synchronization but may be necessary to meet the access delay requirements.

Up to 256 timeslots can be defined. The size of a timeslot can be between 2 and 32 minislots, with a maximum of 1024 minislots per NCS. There are two types of timeslots: Assignment Slots, which are assigned to a specific unit, and Priority Injection Slots, which are not assigned to any unit. A Priority Injection slot is a small timeslot that can be used by any unit, but only for the early transmission of the most important high priority messages, when the unit's next allocated timeslot is greater than 2.5 seconds after the start of the Priority Injection slot. [STANAG 5522] defines some longer messages that may not be transmitted with some of the low MSNs. To avoid this occurrence, a minimum size of timeslots is recommended. The provided values are the ones used by the SNC. If the expected traffic profile does not include the relevant messages, the operator may define any valid range. In [Figure 2B.4-5](#) the column titled "Frag Rate" is the Fragmentation Rate. For HF EPM MSN 4, if there are more than 78 NUs in the network, then the minimum of 13 cannot be met and the integer value of 1024 divided by the number of NUs is used.

Media	MSN	Frag Rate	Recommended Assignment Slot Sizes	Permitted Priority Injection Slot Sizes
HF FF	1	1	7–16	3–16
		2	7–15 (odd values only)	3–15 (odd values only)
		3	7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	2	1	5–16	3–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	3	1	5–16	3–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	4	1	4–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	5	1	4–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	6	1	4–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
UHF FF	1	1	4–32	2–32
		2	5–31 (odd values only)	3–31 (odd values only)
		3	4,7,10,13,16,19,22,25,28,31(every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
HF EPM	1	1	5–32	2–32
	2	1	7–32	3–32
	3	1	7–32	3–32
	4	1	Min(13,Int(1024/#NUs)) – 32	5–32
UHF EPM	1	1	4–32	2–32
	2	1	5–31 (odd values only)	3–31 (odd values only)
	3	1	7,10,13,16,19,22,25,28,31 (every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
	4	1	9, 13, 17, 21, 25, 29 (every 4 th)	5, 9, 13, 17, 21, 25, 29 (every 4 th)

Figure 2B.4-5 Recommended Timeslot Sizes

The information presented above should be used to design an NCS with recommended timeslot sizes to meet the capacity needs and access delay requirements of each unit, as required. If desired, Priority Injection slots can be included in the NCS design. When a unit operates in multiple networks, the capacity needs of the unit can be spread across them.

Figure 2B.4-6 provides all allowed timeslot sizes when the DLP defines the NCS.

Media	MSN	Frag Rate	Valid Ranges of Assignment Slot Sizes	Valid Ranges of Priority Injection Slot Sizes
HF FF	All	1	4-16 (Valid numbers: 4, 5, ... 16)	2-16 (Valid numbers: 2, 3, 4, 5, ... 16)
		2	5-15 (odd values only)	3-15 (odd values only)
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
UHF FF	1	1	4-32	2-32
		2	5-31 (odd values only)	3-31 (odd values only)
		3	4,7,10,13,16,19,22,25,28,31(every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
HF EPM	All	1	4-32	2-32
UHF EPM	1	1	4-32	2-32
	2	1	5-31 (odd values only)	3-31 (odd values only)
	3	1	4,7,10,13,16,19,22,25,28, 31(every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
	4	1	5, 9, 13, 17, 21, 25, 29 (every 4 th)	5, 9, 13, 17, 21, 25, 29 (every 4 th)

Figure 2B.4-6 Valid Timeslot Sizes

Note that it may be impossible to meet all requirements of all units, and the planner may have to accept a compromise solution. The compromise may be produced by reducing the capacity need and/or increasing the access delay of some of the units.

The following is an example of a planner defined NCS. The media parameter requirements (Figure 2B.4-7) and the capacity need and access delay requirements of each unit (Figure 2B.4-8) are the inputs to the process.

Network #	Media	MSN	Fragmentation Rate	DTDMA	Tolerance	Efficiency
1	UHF FF	1	2	DISABLED	NONE (0%)	75%

Figure 2B.4-7 Media Parameter Requirements

Qty	34 NUs	Access Delay	Capacity Need
1	00001	UNLIMITED	VERY LOW
1	00002	UNLIMITED	MEDIUM LOW
1	00003	UNLIMITED	MEDIUM HIGH
1	00004	UNLIMITED	VERY HIGH
1	00005	UNLIMITED	VERY LOW
1	00006	UNLIMITED	MEDIUM LOW
1	00007	UNLIMITED	MEDIUM HIGH
1	00010	UNLIMITED	VERY HIGH
1	00011	UNLIMITED	VERY LOW
1	00012	UNLIMITED	MEDIUM LOW
1	00013	UNLIMITED	MEDIUM HIGH
1	00014	UNLIMITED	VERY HIGH
1	00015	UNLIMITED	VERY LOW
1	00016	UNLIMITED	MEDIUM LOW
1	00017	UNLIMITED	MEDIUM HIGH
1	00020	UNLIMITED	VERY HIGH
1	00021	MEDIUM LONG	VERY LOW
1	00022	MEDIUM LONG	MEDIUM LOW
1	00023	MEDIUM LONG	MEDIUM HIGH
1	00024	MEDIUM LONG	VERY HIGH
1	00025	SHORT	VERY LOW
1	00026	SHORT	MEDIUM LOW
1	00027	SHORT	MEDIUM HIGH
1	00030	SHORT	VERY HIGH
2	00031 – 00032	UNLIMITED	VERY HIGH
4	00033 – 00036	UNLIMITED	MEDIUM HIGH
4	00037 – 00042	SHORT	VERY HIGH

Figure 2B.4-8 Capacity Need & Access Delay Requirements

Details of the UHF FF media are included in [Figure 2B.4-9](#). The minislot information is used when defining the NCS.

Media Details	Value
Minislot Duration in milliseconds	48
Minislots per Network Packet (Fragmentation Rate)	2
Preamble + Guard Time, in minislots	1
Minimum Timeslot Length, in minislots	3
Minimum Assignment Timeslot Length, in minislots	5
Maximum Assignment Timeslot Length, in minislots	31
Regular Network Packet Capacity, in bits	1216
Short Network Packet Capacity, in bits	1216

Figure 2B.4-9 Media Details

Based on the input requirements, the planner defines an NCS.

- Units with higher capacity needs are assigned larger timeslots
- Units with short access delays are assigned multiple timeslots

An example NCS that could be produced by the planner is shown in [Figure 2B.4-10](#).

#	Timeslot Size (Minislots)	Timeslot Owner	#	Timeslot Size (Minislots)	Timeslot Owner	#	Timeslot Size (Minislots)	Timeslot Owner
1	05	00025	18	05	00025	35	05	00026
2	05	00026	19	05	00026	36	05	00027
3	05	00027	20	05	00027	37	07	00030
4	09	00030	21	09	00030	38	07	00037
5	09	00037	22	09	00037	39	07	00040
6	09	00040	23	09	00040	40	07	00041
7	09	00041	24	09	00041	41	07	00042
8	09	00042	25	09	00042	42	05	00021
9	09	00023	26	23	00024	43	05	00022
10	09	00003	27	09	00007	44	05	00001
11	05	00005	28	05	00011	45	05	00002
12	05	00006	29	09	00013	46	23	00004
13	23	00010	30	05	00015	47	05	00012
14	05	00016	31	09	00017	48	23	00014
15	23	00020	32	23	00031	49	03	00000
16	09	00033	33	09	00034	50	23	00032
17	09	00036	34	05	00025	51	09	00035

Figure 2B.4-10 Example NCS

After a NCS is defined, the planner should determine whether the NCS meets the efficiency, tolerance, capacity need, and access delay requirements. The details of the NCS that are needed for the calculations are shown in [Figure 2B.4-11](#).

Calculated NCS General Details	Value
Network Cycle Time (minislots)	465
Network Cycle Time (seconds)	22.32
Number of timeslots in the NCS	51
Number of Priority Injection timeslots in the NCS	1
Priority Injection timeslot length (minislots)	3

Figure 2B.4-11 Calculated NCS Details

Efficiency is the percentage of minislots that can be used for transmission. Preambles and Priority Injection slots reduce the number of minislots that can be used, and therefore decreases the efficiency. The Efficiency is calculated using the following equation.

$$\text{Efficiency} = \frac{<\text{NCT}_m> - <\text{Preambles}> - <\text{PI}>}{<\text{NCT}_m>}$$

- NCT_m : Network Cycle Time in minislots
- Preambles: Number of Preambles (one per timeslot for UHF FF)
- PI = Number of Priority Injection minislots (excluding their preambles)

With the example NCS above, the calculated Efficiency is (465-51-2)/465 = 0.886, or 88.6%, which satisfies the Efficiency requirement of 75%.

Access Delay is the maximum time between timeslots assigned to a unit. As shown in [Figure 2B.4-12](#), the NCS meets the access delay requirement of all the units.

Tolerance is calculated as the percent that the access delay for each unit exceeds the desired value. Since each unit’s access delay is met, the total tolerance requirement of 0% is also met.

The capacity (bits/second) for a unit is defined by the following equation.

$$\text{Capacity} = \frac{<\text{NPs}> * <\text{Bits per NP}>}{<\text{NCT}_s>}$$

- NPs : number of network packets assigned to a unit
- Bits per NP = number of bits per network packet
- NCT_s = Network Cycle Time in seconds

With the example NCS, there are 1216 bits per network packet, and the NCT is 22.32 seconds. [Figure 2B.4-12](#) shows that the NCS meets the capacity need of all the units.

Qty	34 NUs	Access Delay	Capacity Need	Number of Timeslots	Number of NP	Max Delay	NU Tolerance	Capacity Allocated
1	00001	UNL	36	1	2	22.32	N/A	108
1	00002	UNL	108	1	2	22.32	N/A	108
1	00003	UNL	216	1	4	22.32	N/A	217
1	00004	UNL	576	1	11	22.32	N/A	599
1	00005	UNL	36	1	2	22.32	N/A	108
1	00006	UNL	108	1	2	22.32	N/A	108
1	00007	UNL	216	1	4	22.32	N/A	217
1	00010	UNL	576	1	11	22.32	N/A	599
1	00011	UNL	36	1	2	22.32	N/A	108
1	00012	UNL	108	1	2	22.32	N/A	108
1	00013	UNL	216	1	4	22.32	N/A	217
1	00014	UNL	576	1	11	22.32	N/A	599
1	00015	UNL	36	1	2	22.32	N/A	108
1	00016	UNL	108	1	2	22.32	N/A	108
1	00017	UNL	216	1	4	22.32	N/A	217
1	00020	UNL	576	1	11	22.32	N/A	599
1	00021	24	36	1	2	22.32	0%	108
1	00022	24	108	1	2	22.32	0%	108
1	00023	24	216	1	4	22.32	0%	217
1	00024	24	576	1	11	22.32	0%	599
1	00025	8	36	3	6	7.536	0%	326
1	00026	8	108	3	6	7.536	0%	326
1	00027	8	216	3	6	7.536	0%	326
1	00030	8	576	3	11	7.536	0%	599
2	00031,00032	UNL	576	1	11	22.32	N/A	599
4	00033-00036	UNL	216	1	4	22.32	N/A	217
1	00037	8	576	3	11	7.584	0%	599
1	00040	8	576	3	11	7.680	0%	599
1	00041	8	576	3	11	7.776	0%	599
1	00042	8	576	3	11	7.872	0%	599

Figure 2B.4-12 Calculated NCS Details for Each NU

2B.4.4 Mission Requirements

The planner must be aware of any special mission needs during the operation or exercise. Units participating in the same mission will all likely need to receive the same messages. To address a transmitted message to a group of units on the same mission, a Mission Area Sub Network (MASN) can be defined that contains all of the units required for the specific mission.

MASNs for each network (1–8) are automatically defined, so that a message can be addressed to all units in a network. The planner can create MASNs 0 and 9–31. Each MASN includes the MASN Identifier (0, 9–31), a name, and the list of Link 22 Addresses of the units included in the MASN. Note that MASN 0 cannot currently be defined in an OLM; however, it can be generated by the DLP.

2B.4.5 Advanced Unit Parameters

The planner can define the following advanced parameters for any unit.

- NU Status
- NU Link Reception Quality
- Relay Settings
- Late Network Entry
- Data Forwarding

The planner can also identify units that are expected to perform Late Network Entry.

□ **NU Status**

The NU Status of a unit within the Super Network is listed in [Figure 2B.4-13](#), in order of precedence from highest to lowest.

NU Status	Definition
Active	A NU that has a timeslot assigned on at least one network. It is able to receive, send, and acknowledge messages
Radio Silence	A NU that has a timeslot assigned on at least one network, but by choice or order, is not allowed to transmit on any network. It is able to receive, but not send and acknowledge messages. It may break the 'Radio Silence' status and inject messages upon request of its own DLP
Receive Only	A NU that has NO timeslots assigned on any network. It is able to receive
Inactive	A NU currently not part of the (Super) Network (Failure, Maintenance, etc.), with or without a timeslot assigned

Figure 2B.4-13 NU Status Values, Highest to Lowest Precedence

A NILE Unit may have a different status on different networks. However, its highest precedence status, as listed in [Figure 2B.4-13](#), is reported as its NU Status.

The NU Status is the overall status of the unit within the entire Super Network.

The initial NU Status of a unit in the Super Network can be set during planning. If no value is set, the NU Status of the unit defaults to Active. An incorrectly set NU Status is only a temporary condition, because the status will be corrected automatically during operation by the SNMU.

The planner may identify units expected to be initially Receive-Only or Radio Silent, and may also specify whether other units are expected to be initially active or inactive. A unit should be set to Inactive only if it is known that the unit will not be available at the start of the operation. Inactive units will be changed to active automatically as soon as the SNMU receives data from them.

□ **NU Link Reception Quality**

Link Reception Quality (LRQ) represents how well a unit receives transmissions from another unit. This information is transmitted periodically or upon change. When a unit receives the LRQ from another unit, this is called the CLRQ. The CLRQ represents how well the other unit is receiving this unit's transmissions. The LRQ and CLRQ define the connectivity between units, which is used for routing.

If a unit is to be radio silent or receive only in any network, the planner can identify a neighbor unit to relay traffic to the unit. The planner does this by setting the Complementary Link Reception Quality (CLRQ) between the unit and its neighbor unit so that the neighbor unit knows there is a connection to the unit and so will perform the required relay.

This is needed only if the planner must ensure that traffic can be routed to the passive unit. This is not needed when the unit will be in a position where it will be able to receive all relevant traffic without relay.

□ **Relay Settings**

Each unit can be set for automatic relay (the default), inhibited from performing relay, or selected as a preferred relayer. Setting a unit to have a relay setting of Inhibited or Preferred allows the planner to influence traffic flow in the Super Network. An inhibited relayer will not relay messages at all.

A relay setting of inhibited should only be used when there are alternative paths available, as disabling the unit's relay capability can cause connectivity problems, such as fragmentation of the Super Network.

If a unit is set as a Preferred Relayer, and if there are multiple paths to the destination addressees and all other factors are equal, the unit will be selected in preference to any of the others that are not preferred. However, using any value other than the default Automatic relay setting is not recommended. If other values are used, the planner must fully understand that changing this setting affects the routing algorithm, which is described in detail in Chapter 3 [Section C](#).

□ ***Late Network Entry***

If it is known in advance that a unit will be joining a network late, the planner can shorten the LNE protocol by doing the following.

- Include the LNE unit in the OLM at the Super Network level — include a NUDATA set for the unit, which will cause the LNE unit to already have a NILE address when it joins
- Include the LNE unit in the OLM at the Network level — include the LNE unit in the NNETPART set of the network the unit is expected to join, so that it is already a member of the network MASN when it joins
- Mark the LNE unit as inactive in the OLM — set the NU Status field of the NUDATA set to INACTIVE. This will prevent other units from trying to communicate with the LNE unit before it is present, which conserves bandwidth

This information helps to identify the units that are expected to perform LNE. A LNE Slot should be inserted into the ONCS before any unit is expected to perform LNE. The NMU can do this, or the SNMU can order the NMU to do it.

□ ***Data Forwarding***

In a multilink environment, one or multiple data forwarding capable units should be identified, depending on the other data links involved, and the connectivity between them. For each data forwarding unit, one or more standby units should also be identified. Data forwarding units must be assigned an extra block of Low TNs to use for forwarding High TNs onto Link 11/11B.

2B.4.6 Advanced OLM Production

The following advanced Link 22 OLM sets were not covered earlier.

- Link 22 Mission Area Sub Network Set
- Link 22 Unit Data Set
- Link 22 Unit Reception Quality Set

□ Link 22 Mission Area Sub Network Set

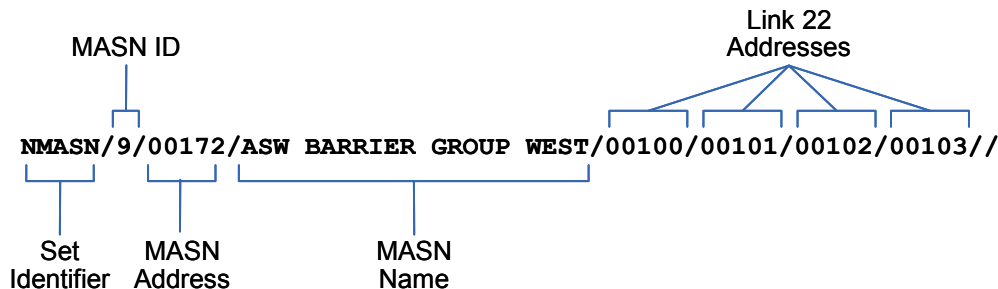


Figure 2B.4-14 NMASN

The NMASN sets shown in Figure 2B.4-14 are used to define any non-network MASNs (9–31). The MASN must be given a name. The use of MASNs is not currently specified in [STANAG 5522].

□ Link 22 Unit Data Set

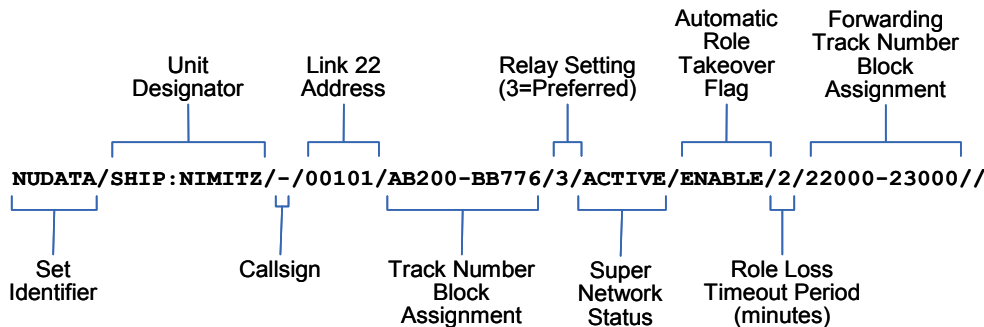


Figure 2B.4-15 NUDATA

The NUDATA set shown in [Figure 2B.4-15](#) is used to assign Forwarding Track Number Blocks to data forwarding units and to define the unit's Relay Setting. Relay Setting values are defined in [Figure 2B.4-16](#).

Relay Setting Value	Relay Setting
1	Automatic
2	Inhibited
3	Preferred

Figure 2B.4-16 Relay Setting Values

□ **Link 22 Unit Reception Quality Set**

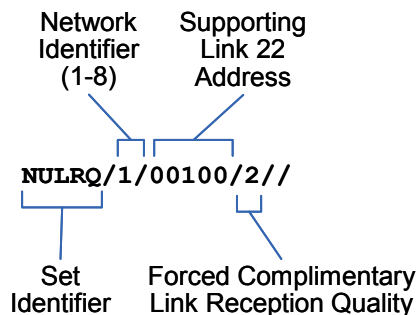


Figure 2B.4-17 NULRQ

The NULRQ set shown in [Figure 2B.4-17](#), if used, immediately follows the NUDATA set of the radio silent NU for which it applies. The forced Complementary Link Reception Quality (CLRQ) between the radio silent NU and its supporting unit can be one of the values given in [Figure 2B.4-18](#).

CLRQ Value	Meaning
0	No Link
1	Poor – some missing data
2	Good – some corrected errors
3	Excellent – no errors

Figure 2B.4-18 CLRQ

2B.4.7 Additional Planning Flowchart

The flowchart provided in [Figure 2B.4-19](#) shows the iterative steps that a planner may need to take before an acceptable plan is finalized. Note that minor deficiencies in a plan should not be a problem, since the Link 22 system can automatically adjust to actual conditions during operations. Red flowchart processes are expanded in [Figure 2B.4-20](#) and [Figure 2B.4-21](#).

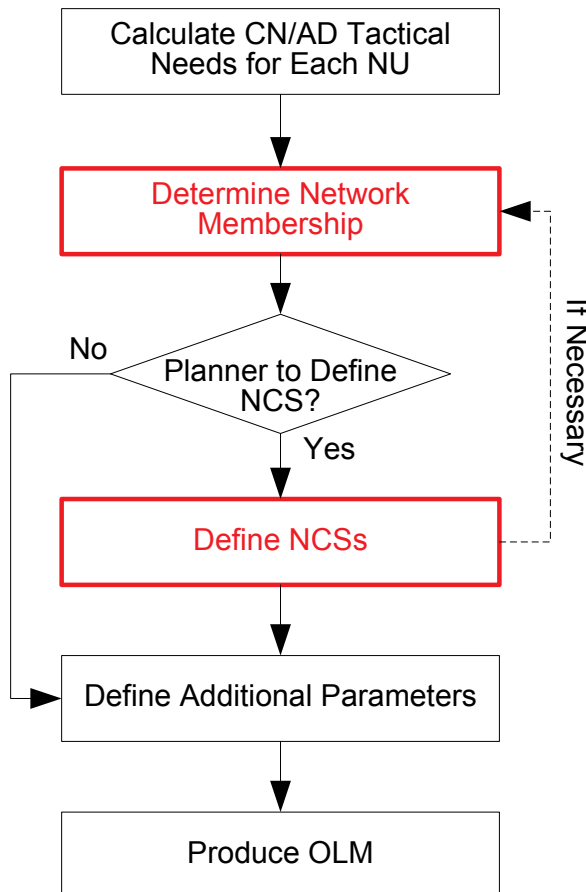


Figure 2B.4-19 Top Level Additional Planning Flowchart

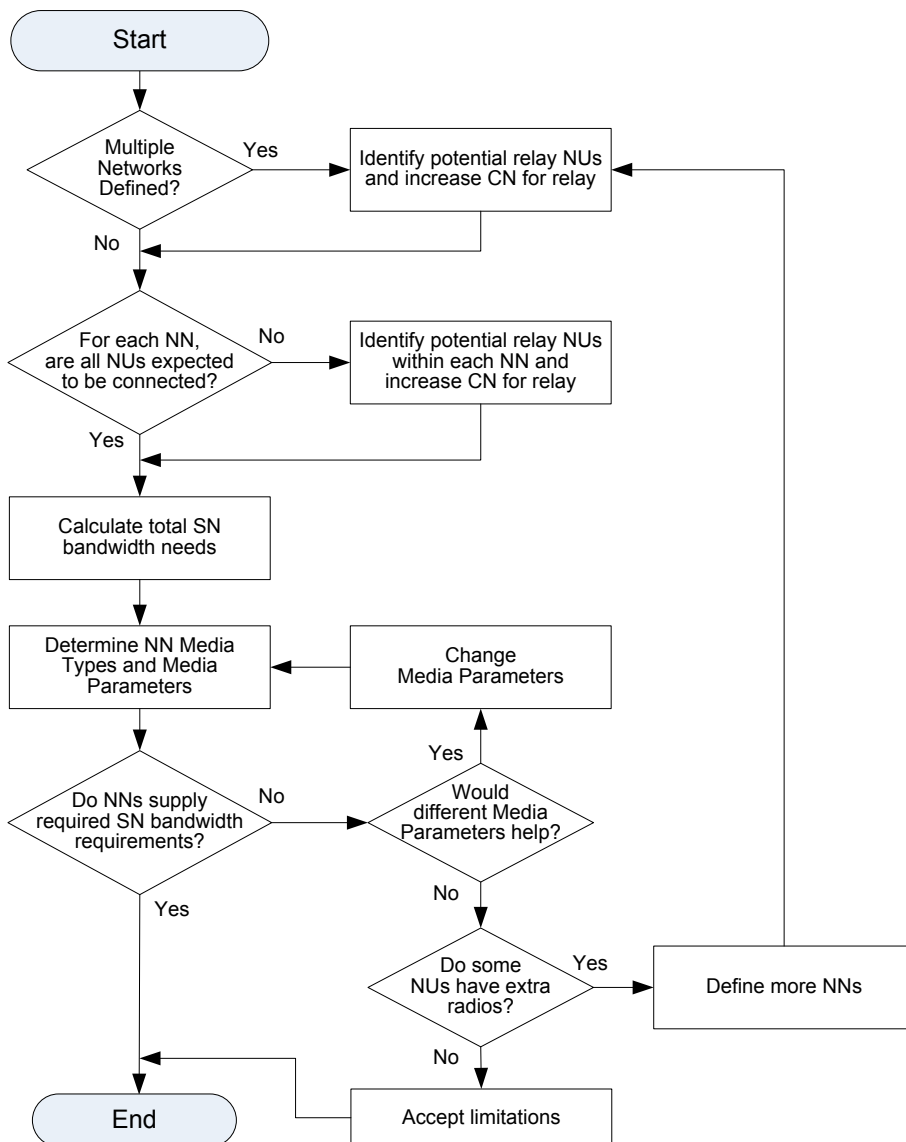


Figure 2B.4-20 Determine Network Membership Flowchart

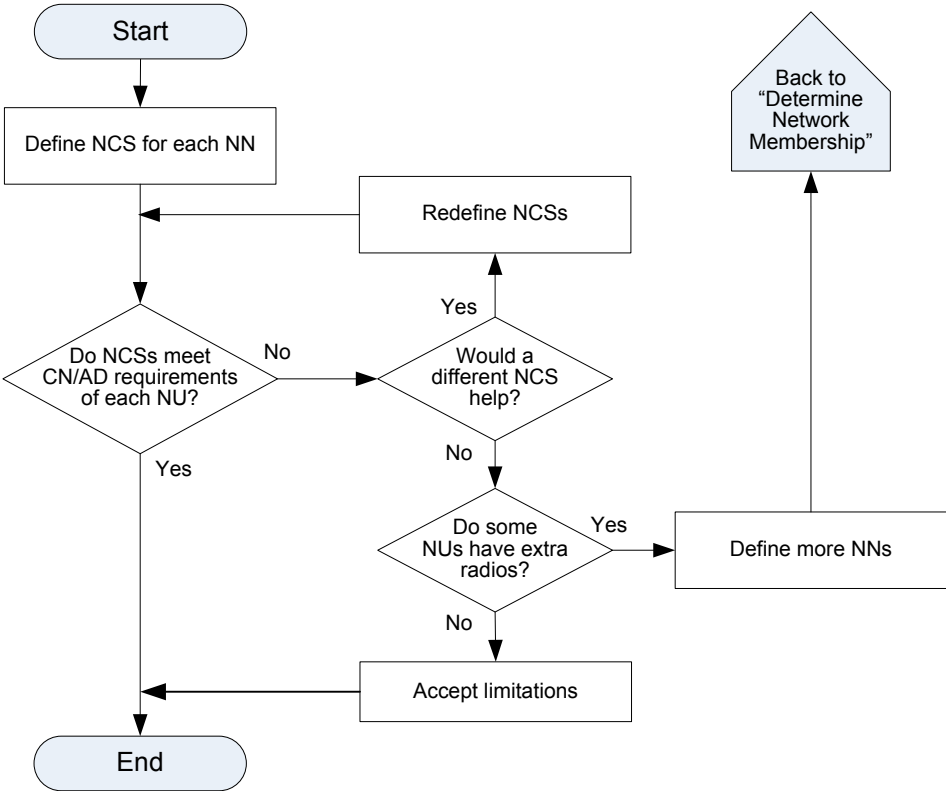


Figure 2B.4-21 Define NCSs Flowchart



This page is intentionally left blank

Section C Link 22 Operations

The operation of Link 22 may involve a number of different operators, possibly tactical display operators, data link management operators, radio operators, crypto key operators etc. or there may be very little if any operator interaction. The amount of interaction depends on the platform configuration and its role in the system. It can also be affected by national or allied doctrine. As it is not possible to be specific this section refers to a generic Operator. Link 22 Operations consist of the following three main phases.

- Initialization
- Operation
- Termination

A summary of management operations is provided in section [2C.4 Operator Actions Summary](#).

Within this section, there are many operator interaction figures which show how the operator interacts with the Link 22 system of their unit and how the unit communicates with other Link 22 units. The figures use the following color and symbol conventions as shown in [Figure 2C-1](#).

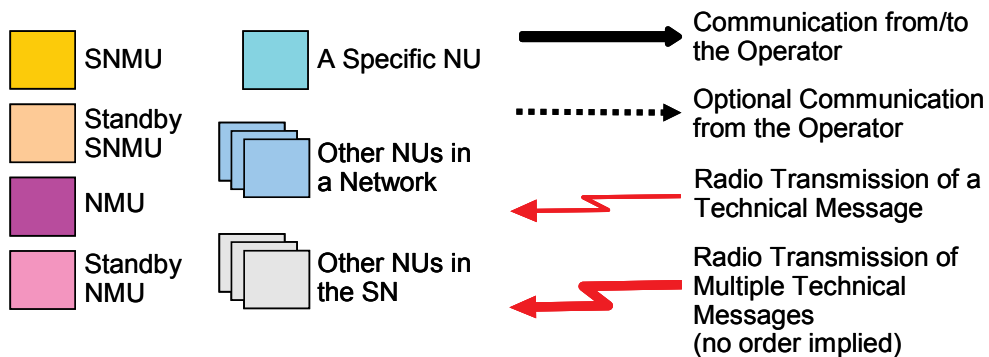


Figure 2C-1 Color and Symbol Conventions

2C.1 Initialization

Initialization of a Link 22 unit consists of the following steps.

- Initialization Data Input
- Hardware Initialization
- System Initialization
- Network Initialization

2C.1.1 Initialization Data Input

The operator is responsible for supplying the DLP with the information contained in the OPTASK Link Message (OLM), which is necessary for the initialization of the Link 22 system. Successful initialization requires that all NUs are provided with the same OLM.

In addition to the information in the OLM, the following unit specific information is required.

- Own Unit Link 22 Address
- LLC/SPC selection for each Network that the own unit will participate in
- Crypto Day of Week, and Key Location Information
- Non-OLM related initialization data

Figure 2C.1-1 illustrates one unit that has two LLCs. Each LLC has two SPCs/Radios. If the OLM indicates that this unit is to participate in one HF FF network, an LLC and SPC must be selected for the network. In the figure, there are two choices: LLC 1 / SPC 0, or LLC 2 / SPC 0. In this illustration, LLC 2 / SPC 0 have been selected.

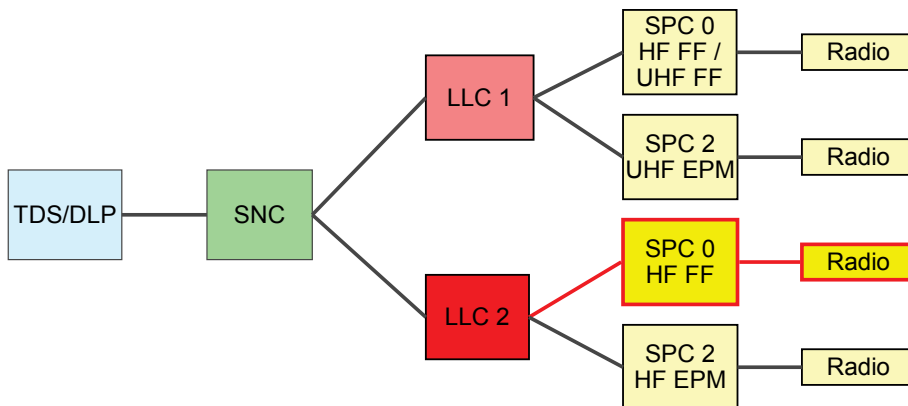


Figure 2C.1-1 LLC and SPC Selection

If the system does not automatically supply the unit specific information, the operator may need to supply it manually. A detailed explanation of how the OLM is used in determining unit specific information is included in the [Troubleshooting Appendix B](#). Further details of non-OLM data can be found in [Appendix D](#).

2C.1.2 Hardware Initialization

The operator should ensure that all necessary hardware is powered up, and all necessary software is executing, prior to starting system initialization. This includes the TDS/DLP, the SNC, the necessary LLCs, SPCs, and radios, and any necessary TOD equipment and software. For an embedded system, this is likely to involve just powering on the system, which would automatically start all required software.

□ Crypto Management

The operator will need to load crypto keys into the LLCs, at least one for each network that will be used prior to starting System Initialization. All crypto keys for an operation extended beyond a single week could be loaded into the designated crypto key locations before starting the operation, eliminating the need for future key loads. The default starting key location used is recommended to be either zero (relative to the SN Start date), or the week number of the year (relative to the calendar). However, any key locations can be used as long as the DLP is made aware of the location to be used for initializing a network. After 7 crypto days, the LLC performs a key rollover switching the crypto keys for all configured networks to the next locations ((current location + 1) modulus 64), during this process the old crypto key is deleted. The

operator must have loaded a new crypto key into the next location for each configured network before the key rollover occurs.

The SNC ensures that each LLC's Day of Week (DOW) is initialized with the Super Network's current DOW. The SNC when initializing an LLC, configures the LLC with no ports, and checks that there are none currently configured. Then the SNC configures the LLC to the required configuration, setting the reset DOW flag to true and providing the current SN DOW. This ensures that the LLC's DOW is the same as the SN DOW. This same DOW procedure is used if an LLC is added, replaced, or restarted while the system is running.

Further details about crypto keys and DOW can be found in [Appendix B Troubleshooting](#), [Appendix D](#), and in the LLC Operator's Manual [LLC OPM].

□ **SPC/Radio Management**

For HF and UHF fixed frequency media types, if the SPC does not control the radio frequency, the operator needs to ensure the radio is tuned to the correct frequency.

For HF and UHF frequency hopping (HF EPM & UHF EPM) media types, the frequency hop set and a TRANSEC key must be loaded into the system. The key controls the selection of the frequency from the hop set for each frequency hop and the selection of data used as known system overheads.

For UHF EPM, the key is loaded directly into the radio, and the frequency hopset has to be supplied to the radio either by the SPC or via the operator.

For HF EPM, the TRANSEC functionality may be implemented in the SPC, in the radio or split across both. Therefore, the key may have to be loaded into the radio or the SPC or possibly both, depending on the media implementation. If the radio requires the frequency hop set and the SPC does not supply it to the radio, then the frequency hopset may have to be loaded directly into the radio.

The TRANSEC key is loaded via the standard key-fill connector on the device using the associated fill-gun for the device.

If the SPC does not control the radio power then the power setting has to be adjusted manually.

2C.1.3 System Initialization

After the operator has supplied all necessary information to the system, the operator can start Link 22 system initialization. Exact details of how to perform this operation are system dependent.

The TDS will instruct the DLP to start Link 22 system initialization, which will start to initialize the SNC and the media segment. During the initialization process, the SNC will report successes and failures back to the DLP/TDS for display to the operator. The operator should monitor the status of the SNC initialization. Failures during SNC Initialization will cause the SNC Initialization process to stop. Further recovery details are supplied in [Appendix B, Troubleshooting](#).

After SNC initialization is complete, Network Initialization as specified in the OLM will automatically begin just before each network's start time.

If a unit is being initialized later than the network initialization start date and time specified in the OLM, or if it is not specified as a member of a network it wants to participate in, the operator can start the Late Network Entry process, as described in the next section.

2C.1.4 Network Initialization

The OLM indicates the start date and time of each network. The Operational Start Time (OST) supplied by the DLP to the SNC for each network does not contain a date, only a 24 hour time (represented as the number of seconds (0-86400) since midnight). This 24 hour time is considered to be divided into 12 hours before the current time, and 12 hours after the current time. The system assumes the following.

- If OST is before the current time, start immediately
- If OST is after the current time, start in the future at the indicated OST

These two cases are shown in [Figure 2C.1-2](#) and [Figure 2C.1-3](#).

- OST = 0500 hours
- Current time = 1100 hours.

OST is before the current time. The network will start immediately, i.e. it is assumed that the unit is starting late.

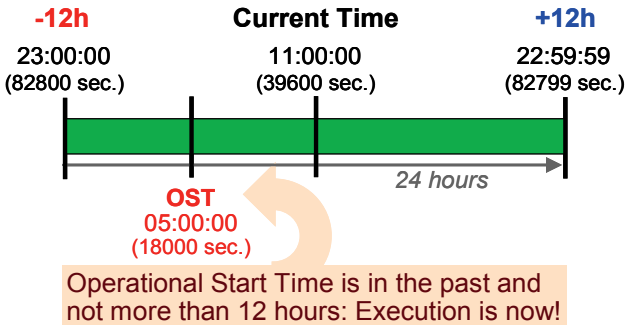


Figure 2C.1-2 OST Before Current Time

- OST = 1700 hours
- Current time = 1100 hours.

OST is after the current time. The unit will wait 6 hours until OST before starting the network.

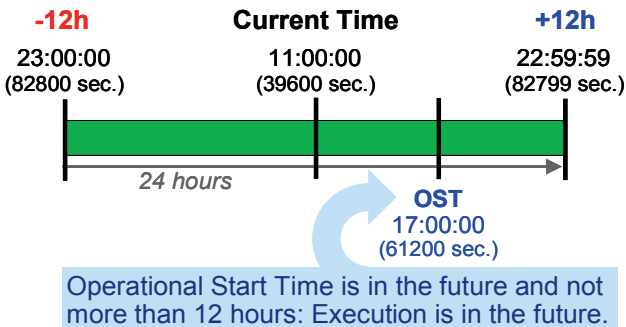


Figure 2C.1-3 OST After Current Time

Due to the DLP-to-SNC system time constraints described above, a TDS/DLP will only start to initialize a network within the 12 hours before OST. If the initialization is after the OST but within 12 hours, the OST can still be used. If the unit is initializing on the network more than 12 hours late, then the OST included in the OLM is no longer valid, and the system will replace the OST with the current time. Network initialization after OST should only be performed if the operator is certain that there have been no changes to the OLM information for the network since the network was started (needs external confirmation). Otherwise, the unit must join the network by performing LNE as described later in this chapter.

There are three types of network initialization.

- Short Network Initialization
- Probing Network Initialization
- Late Network Initialization

The SNC notifies the DLP/TDS (which may inform the operator) of the successful completion of network initialization.

□ **Short Network Initialization**

The Short Network Initialization procedure implies that the set of initial parameters have been chosen with enough confidence that no optimization of the Network and Media parameters is necessary (that is, Channel Probing is not performed).

Either the NCS is defined in the OLM, or the SNC will calculate the NCS based on parameters defined in the OLM. When the SNC calculates the NCS, the calculated NCS is provided to the DLP/TDS for acceptance.

□ **Probing Network Initialization**

Network Initialization with Channel Probing implies that low confidence is given to some of the media parameters and therefore the successful functionality of the network. Therefore, the SNC is requested to probe the channel to identify the best set of parameters and optimize the Operational NCS (ONCS) taking into account connectivity information.

The results of probing of each waveform are provided to the DLP/TDS. Only the NMU operator will receive all the results and is responsible for making the final decisions. The results include a connectivity matrix (known as Probing Reception Quality (PRQ)) and an indication of the amount of received correct data (known as throughput). The connectivity matrix covers NUs up to three legs away.

After all probing has been completed, the NMU operator can decide to probe more sets of data, in which case the NMU operator must supply the following network parameters for the Reprobe.

- Media Type
- Frequency/Hopset
- Up to fifteen Media Setting Numbers
- List of units
- Reprobe Start Time

After the NMU operator is satisfied with the probing results, the NMU operator must select which media parameters are to be used. The NMU operator must also decide how to provide the NCS for the network, either request an NCS from the SNC or provide the NCS.

The NMU operator can request that the SNC calculates a new NCS for the network, and the NMU operator has to supplying the following information.

- Capacity Need per unit
- Access Delay per unit
- Access Delay Tolerance
- Efficiency

Refer to [2B.2.2 The SNC will calculate the NCS](#) for details about these values.

The calculated NCS will be displayed to the NMU operator. The NMU operator can accept the NCS, send a different set of information for the SNC to use to recalculate a different NCS, or the operator may decide to provide an NCS.

The operator/TDS/DLP can provide an NCS for the SNC to use as the Operational NCS for the network. The NMU operator may be able to specify an NCS by assigning timeslots to units, based on the needs of each unit, or the NMU operator may use a tool to produce an NCS. Refer to subsection [2B.2.2 Planner Defines the NCS Manually](#) of section 2B.2.2 for considerations when creating an NCS.

The selected Media Parameters and the NCS will be transmitted to all the NUs in the network, using the last probed network configuration. The SNC of the receiving NUs will provide the selected configuration to its DLP/TDS for possible display to the operator. The NMU operator should verify that all expected units complete the probing. If they don't, the NMU should include an LNE slot in the ONCS so that it is possible for those NUs that may not have received the selected configuration to join the network.

[Figure 2C.1-4](#) shows an example of probing (no reprobe) with the SNC calculating the NCS. In this case, it is assumed that the probing started automatically at the Operational Start Time for the network, so no operator command is shown to start the probing.

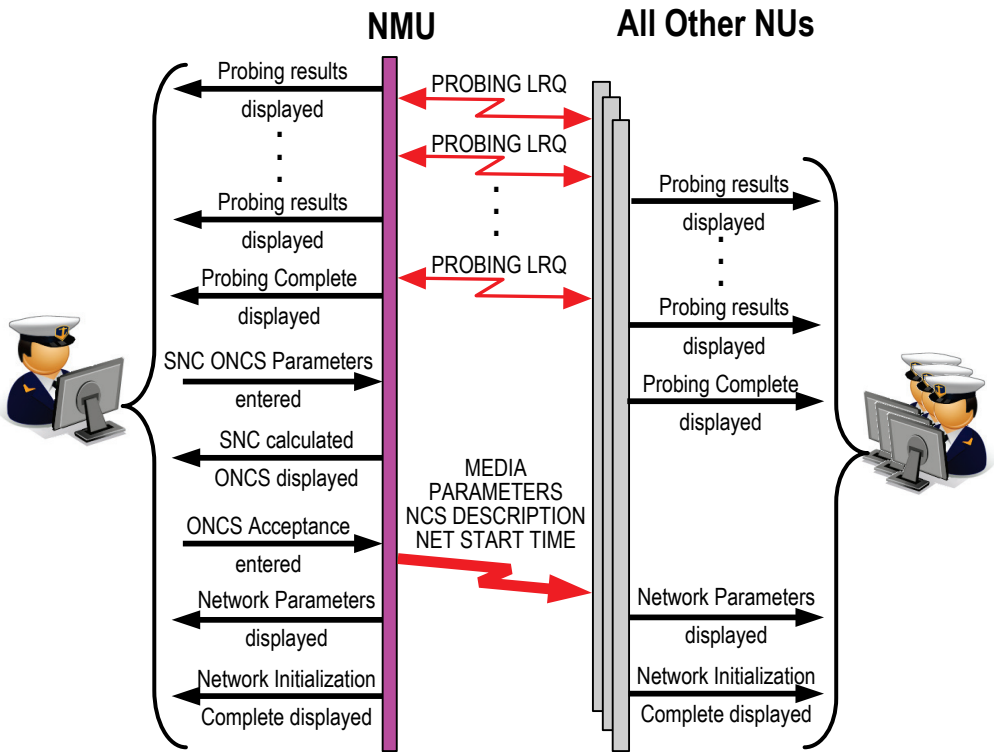


Figure 2C.1-4 Probing Network Initialization

□ **Late Network Initialization**

After the network has been started, units that have not yet initialized on the network can join the network by initiating a protocol called Late Network Entry (LNE). LNE supports the following.

- Units not yet initialized on any network
- Units already initialized on another network
- Units joining only to listen – no transmission capacity requested during LNE, receive-only after LNE is complete
- Units silently joining, without making any transmissions

■ **Start of the LNE Protocol**

The LNE operator has two methods to perform LNE.

- Silent Join – the operator only wants to listen to the network, and does not want to make any transmissions while performing LNE. The unit is not a member of and does not want to become a member of the Super Network
- Non-Silent Join – the operator wants to use transmissions to join the network

The LNE operator must select an LLC and SPC to use for the network it is joining. The operator must ensure that the correct crypto keys are loaded for the network. The operator must supply which LLC port the SPC is attached to and the location of the crypto key for the network to be configured on the port. .

The LNE operator must supply the correct media type and frequency/hopset for the network it is joining, if it is not a member of any other network. If known, the operator can also supply the other media parameters: LLC Integrity, Fragmentation Rate, Media Setting Number, and the Network Cycle Time. If the operator does not know some of the parameters, the SNC will attempt to acquire them during the LNE protocol.

Depending on the implementation of the DLP, once the LNE process has been started, it may either be automatically completed without operator intervention, or operator actions may need to be performed. During a Non-Silent Join, the operators at three different NUs may need to take action during LNE. These operators are the LNE unit's operator, the NMU operator, and the SNMU operator, as shown in [Figure 2C.1-5](#). The actions of the Supporting Unit (SU) are performed automatically by its SNC.

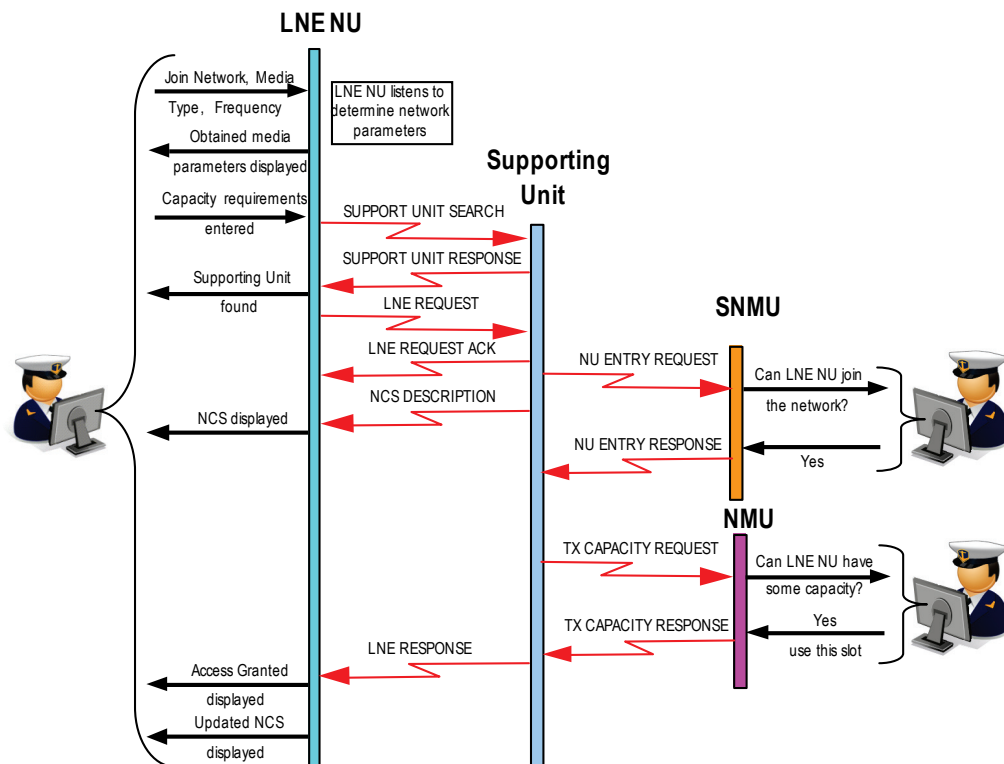


Figure 2C.1-5 Successful Non-Silent Join Late Network Entry

The operator needs to determine when to use Late Network Entry. A Short network initialization can only be used if the OLM used Short initialization and verbal confirmation that no changes have occurred is obtained from the SNMU or NMU. Otherwise Late Network Entry should be used as default, and must be used when any of the following conditions exist.

- OLM used Probing initialization
- OLM used Short initialization and changes may have occurred
- Unknown current Network settings

For the case of a Non-Silent Join, if the LNE unit is not already active on another network, the NMU must have activated the insertion of an LNE slot for the LNE to proceed. If the SNMU and NMU are aware of the planned entry, the following steps will speed up the process.

- Addition of the LNE unit to the Super Network
- Addition of the LNE unit to the Network membership MASN
- Reconfiguration of the Network to allow capacity for the LNE unit, before inserting the LNE slot (if not a receive only NU)

■ ***LNE Status***

The status of the LNE is reported to the LNE NU operator as the LNE protocol progresses. At various points during the LNE protocol, the LNE operator may need to decide to continue with the LNE protocol or terminate it, as detailed below.

■ ***Request Network Parameters***

The LNE operator starts the LNE protocol by supplying the known network parameters, which at a minimum must include the media type and the frequency/hopset, if the LNE unit is not active on any other network. The unit's SNC determines the remaining network parameters, which are reported to the operator. If the SNC cannot determine the network parameters, LNE Failure will be reported to the operator.

If Silent Join was used, no other operator actions are required. The unit simply starts receiving on the network if the network parameters are successfully obtained.

■ ***Request Access***

For non-silent join, based on the obtained network parameters and the available hardware, the LNE operator must decide whether to continue or not. If the operator wants to continue to join the network, the operator must supply its transmission

capacity need and access delay requirements, or indicate that the unit does not need any transmission capacity.

The LNE operator will be informed of the result, which will be either that the unit was granted or denied access to the requested network or granted access on an alternate network.

■ ***Access Granted***

The LNE unit may be granted access to the requested network, or an alternate network. If access was granted on an alternate network, the LNE operator may want to terminate LNE if the necessary hardware is not available. The LNE protocol is completed using the original hardware configuration, even if access was granted on an alternate network. After the LNE protocol is completed and if access was granted on an alternate network, the LNE operator may need to reconfigure the hardware for the alternate network, and then notify the DLP that it is ready to use that network. The LNE unit will have to wait for capacity, until the NMU has performed a network reconfiguration, if capacity was requested and no capacity was allocated.

■ ***Access Denied, or other Failure***

If LNE fails, the LNE operator may want to try LNE again with different parameters, or on a different network, or may contact the SNMU or NMU for direction using a secure voice support circuit.

2C.2 Operation

This section details cases that may require operator intervention. During operations, changes can be made to unit, network, and Super Network parameters. The SNMU operator can manage changes involving individual units, the networks, and the Super Network. The NMU operators can manage their networks. All NU operators can manage their own units. An implementation of a DLP could perform many of these functions automatically; however, this section will provide the fundamental descriptions of all management functions. This section consists of the following subsections.

- [NU Management](#)
- [Advanced NU Management](#)
- [Network Management](#)
- [Super Network Management](#)

Information provided by the SNC to the DLP/TDS may be displayed to the operator. However, the amount or types of information displayed is an implementation decision and may vary on different systems. A specific implementation may fully or partially notify or alert the operator. This section focuses on flow and information relevant to the operator to ensure proper understanding and effective management of the protocols. When the DLP/TDS is provided with the information, it may or may not be displayed to the operator, depending on the DLP/TDS implementation. The figures in this section show the data that could be displayed to the operator if fully implemented.

2C.2.1 NU Management

During normal operations, there are very few actions that a NU operator normally performs. The NU operator has the ability to perform some changes locally, normally under the supervision of the operational command, including the SNMU and NMU. After initialization, typical NU operator functions may consist of the following.

- [Change Radio Power](#)
- [Change Radio Silence](#)
- [Monitor Statistics](#)
- [Fault Management](#)

The NU operator may also need to respond to orders from the SNMU or NMU, or perform other more advanced functions, as discussed in the [2C.2.2 Advanced NU Management](#) section.

□ **Change Radio Power**

The operator may want to adjust its own transmission power used on a network. The operator instructs the DLP to request the SNC to request the network's SPC to change its radio power, as shown in [Figure 2C.2-1](#). The results of the radio power change are shown to the operator.

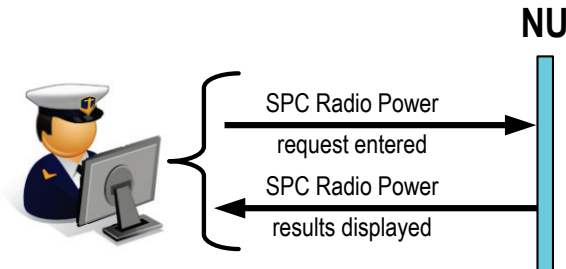


Figure 2C.2-1 Change Radio Power

The SNMU or NMU can order a single unit or all units in a network to change their radio power. This can be done independently, or applied to all units in a network as part of a network parameter change.

Some implementations or systems may not allow the change of radio power automatically through the SNC and SPC. In this case, the value stored inside the SNC is for reference only, as the Operator needs to ensure externally that the power level is at the required value.

□ **Change Radio Silence**

Rules for entering and exiting Radio Silence are part of the Emission Control (EMCON) policy. The impact on the Super Network connectivity has to be taken into consideration, because if the unit is a critical link in the connectivity, the change to Radio Silence may fragment the Super Network, causing loss of connectivity between units.

The operator can direct the unit to go to Radio Silence on a specific network, or in the entire Super Network, at a specified time, or immediately, in case of an emergency. All other NUs are informed that the NU is going to Radio Silence, if there is time before the NU becomes Radio Silent, as shown in [Figure 2C.2-2](#). In certain circumstances, some tactical messages may be transmitted while in Radio Silence, depending on the EMCON plan. [STANAG 5522] specifies which tactical messages

have the highest priority and are eligible for priority injection; these most important messages are the ones that may possibly be allowed to be transmitted while in radio silence. The operator can later direct the unit to terminate the Radio Silence condition on the network or Super Network, either at a specified time or immediately.

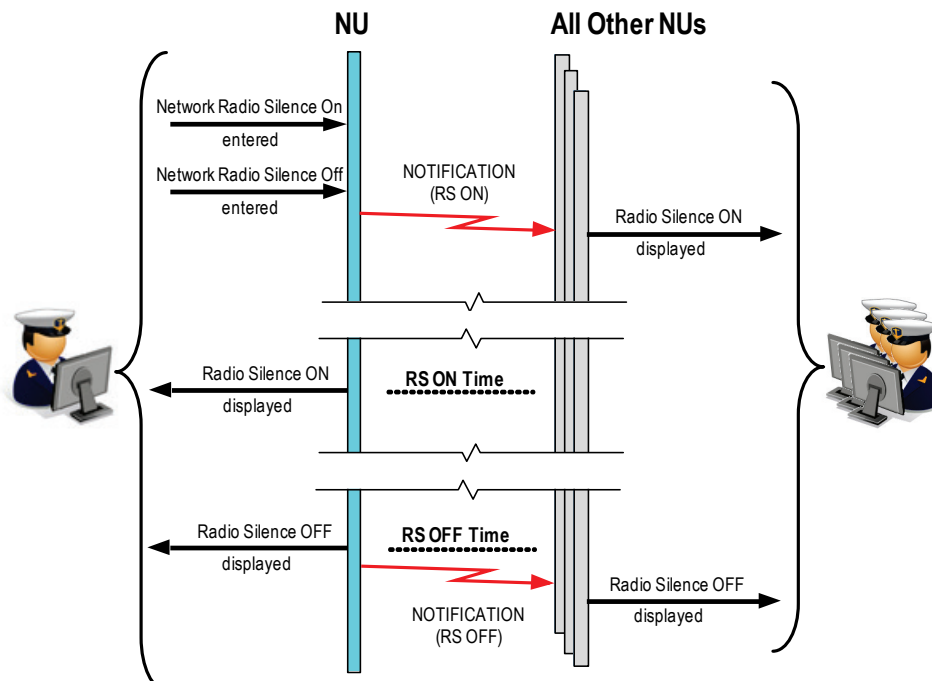


Figure 2C.2-2 Change Radio Silence

The system allows any combination of Radio Silence ON or OFF, which may be initiated locally or remotely ordered by the NMU or SNMU, which are processed based on the indicated time included in each request. The SNC will go into radio silence whenever it receives a message to do so from any of the three valid sources. The SNC will maintain radio silence until radio silence off is received from all the originators of the radio silence on messages or the NU overrides radio silence to turn it off. The precedence of the radio silence off messages is detailed in [Chapter 3](#).

[[STANAG 5522](#)] requires that a unit transmits a PLI with the Network Participation Status Indicator set to Conditional Radio Silence before entering Radio Silence in the Super Network. This ensures that the other NUs are aware that it is going into Radio Silence and reporting responsibility can be reassigned based on the applicable rules.

The SNMU or NMU can also order a unit to change its Radio Silence status in the network. The SNMU can also order a unit to change its Radio Silence in the entire Super Network (that is, on all of its networks). A Radio Silence ON order can optionally also include the time to turn off radio silence. Following a Radio Silence ON period transmissions will resume. It will take time to re-establish the connectivity between units, which will affect relay determination and therefore optimal traffic exchange.

□ **Monitor Statistics**

All units receive statistical information from their SNC that may be displayed to the operator. Some of the data is sent automatically on a periodic basis while other data is only sent on request from the DLP. The SNMU and NMU operators may use this information in deciding whether to make changes to the networks. The following statistical information may be provided to all units.

- Channel Utilization
- Connectivity
- Congestion
- Error Rates
- DTDMA Participation
- NU Reception
- Tactical Transmission/Reception Statistics
- Fault Management

Every NU operator should monitor statistics, errors and alarms to determine if there are any actions that the operator may need to take to correct any identified issues. If the NU operator wants to contact the NMU or SNMU operator to discuss any issues or possibly request changes, an external circuit needs to be used.

A brief description of each of the different types of statistical information is included below.

■ **Channel Utilization**

For each network, the SNC reports the percent of the unit's assigned timeslots that were used for transmitting its own tactical messages, and the percent used for relaying tactical messages. The percentages are reported for each of the four different priorities. This information is reported following the use of each transmission timeslot. If a unit is not congested, channel utilization information indicates how much of the channel capacity the unit is using.

■ **Connectivity**

The Link Reception Quality (LRQ) data represents the quality of the connection between two NUs, in one direction, up to two legs away. The connectivity of all NU pairs in both directions in the Super Network is included in the report. The LRQ has four levels: No connection, Poor, Good and Excellent. The Link Connectivity Data (LCD) represents the connectivity, “at least good connectivity” or “not connected,” between two NILE Units bi-directionally up to three legs away. The combination of LRQ and LCD provides knowledge of the connectivity between a unit and other units up to three legs away.

The DLP can either request the connectivity when it needs the information, or can request that the SNC report it periodically once every specified reporting period.

■ **Congestion**

The Congestion information indicates how backed up the SNC transmissions are for each of the four priorities, and is related to Channel Utilization. When Channel Utilization becomes high, the Congestion Values indicate how much remains to be transmitted. Since the SNC transmits messages based on priority, high priority traffic will always have precedence. The SNC has a significantly larger queue than transmission will allow. If the queue’s limit is reached, the SNC will automatically delete lower priority requests, when a higher priority request is received.

Congestion may be temporary or sustained. The system automatically attempts to alleviate conditions that have contributed to the congestion. The congestion may also be relieved by reducing tactical traffic. Channel Utilization and Congestion information can be used to determine what type of tactical messages, local or relay, and what priority of tactical messages are causing the congestion. Congestion can affect reporting responsibility. As permitted by operational rules and under appropriate command, the NU operator may need to modify reporting responsibility, change reporting filters, or modify the quality of service of the tactical messages.

■ **Error Rates**

For each network, at the end of each Network Cycle Time (NCT), the SNC reports the percent of Network Packets (NPs) received without errors, the percent of NPs received with various types of errors, and the percent of NPs that were not received. [Appendix B, Troubleshooting](#), discusses this data further.

■ ***DTDMA Participation***

Every 10 Network Cycle Times (NCTs), a unit's participation in DTDMA is reported for each network that has DTDMA activated. It includes information such as the number of times this unit offered some of its own capacity to other units, and the number of times this unit accepted capacity from other units. If the unit is donating capacity, this indicates that other units are more congested than this unit, whereas if this unit is receiving capacity it is more congested than the neighboring units that have donated capacity.

■ ***NU Reception***

Once each minute, each SNC reports if and when it last received a message from the active NUs in the Super Network, and how many units have to transmit (transmission legs) to reach each NU. A transmission leg value of 0 indicates that the connectivity is not known because it is more than three legs away.

If the NU is not receiving from units as expected, it may indicate a problem with that unit. Refer to [Appendix B, Troubleshooting](#) for potential recovery actions.

■ ***Tactical Transmission/Reception Statistics***

The system may provide the operator with statistics on the number of transmitted and received tactical messages over time (rate). The system may also provide the change of rate over time (trend). The statistics may include the following data.

- STANAG Repetition Rate Variance
- Transmission Success Rate
- Message Time of Validity to Transmission Complete Timing
- Received Message Delay
- Received Tactical Errors

◇ **STANAG Repetition Rate Variance**

The system may compute the difference between the expected repetition rate of tactical messages based on the STANAG rules and the actual rate of received messages. In Figure 2C.2-3 the black intervals represent the STANAG expected repetition rate of 12 seconds, and the red interval markers the actual reception of the repeated message. From the intervals between receptions, it can be seen that on average the transmitting unit is more than 2 seconds late. Significant variance may imply that congestion is present and the network is not optimized.

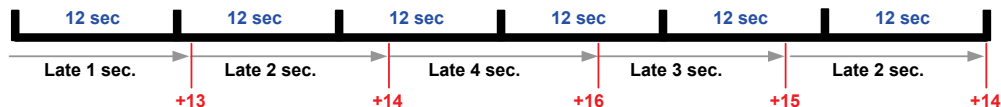


Figure 2C.2-3 Tactical Repetition Rate Monitoring

◇ **Transmission Success Rate**

The percentage of the required networks on which the messages were successfully transmitted may be provided. A value less than 100% means that all required network transmissions were not completed due to timeout and some of the addressed units may not receive the message. This may indicate possible problems of connectivity and/or congestion.

◇ **Message Time of Validity to Transmission Complete Timing**

The difference between the time the data was generated for transmission and the completion of all transmissions may be provided. A significant difference when multiple transmissions are required indicates congestion.

◇ **Received Message Delay**

The difference between the time the data was generated for transmission and the time the message was received may be provided. When longer than expected delays occur, this may indicate possible problems in the network.

◇ **Received Tactical Errors**

Tactical messages consist of 1–8 words. A message may be received with errors in some of the words, but not others. This can only happen when fragmentation is used to transmit the message. An indication of the amount of word errors may be provided.

This may help to identify problems with reception by this unit, or a problem with transmission by the transmitting unit. The system is expected to verify compliance of the received tactical messages and the tactical implication in accordance with [STANAG 5522], [STANAG 5616 Volume II], [STANAG 5616 Volume III], and [ADatP].

□ **Fault Management**

Problems that may occur in the Link 22 system typically fall into one of the following categories.

- Initialization Problems
- Hardware Problems
- Software Problems
- Operator Errors
- Operational System Level Problems

Some problems in the Link 22 system are automatically recoverable. Others may require manual operator actions. [Appendix B](#) discusses troubleshooting issues in detail.

2C.2.2 Advanced NU Management

Occasionally, an NU operator may need to perform some of the following functions.

- Request Management Information
- Crypto Key Management
- Order Automation
- New Network Initialization
- Role Takeover Control
- Relay Flow Control Decisions

□ Request Management Information

Figure 2C.2-4 shows the flow of a management information request to the SNC. The set of response messages depends on the values in the request. The request specifies whether the information is provided once per request or whether it should be provided periodically.

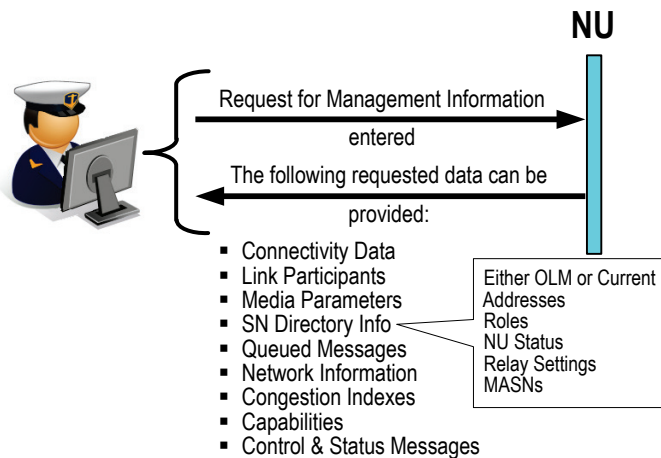


Figure 2C.2-4 Request Management Information

A description of each type of data follows.

■ **Connectivity Data**

The Link Reception Quality (LRQ) and connectivity data represents the quality of the connection between two NILE Units that are up to two legs apart. The Link Connectivity Data (LCD) represents the connectivity between two NILE Units that are three Legs apart. If there is at least a good connection in both directions, LCD is 1; if the connection is less than good, LCD is 0. As indicated above, the combination of LRQ and LCD provides knowledge of the connectivity between a unit and other units up to three legs away.

■ **Link Participants**

A list of the Link 22 addresses of all Super Network members and a list of the Link 22 addresses of each NILE Network's members is returned.

■ **Media Parameters**

The following data is returned for each network.

- Media Type
- Frequency/Hopset
- SPC Radio Power
- Media Setting Number
- Fragmentation Rate
- LLC Integrity Flag
- Dynamic TDMA Flag
- Network Start Time

■ **SN Directory Info** see [Appendix B Troubleshooting](#).

■ **Queued Messages**

The SNC queues all messages associated with commands it receives from the DLP, which are to be processed in the future to allow the operator the ability to cancel relevant commands, if the operational situation changes. Upon request, all commands which have not yet started to be processed are returned. The operator can use this list to cancel any of the commands which are no longer desired. The SNC removes a queued command and transmits it 20 minutes before its scheduled time, at which time the command can no longer be cancelled.

■ **Network Information**

The following data is returned for each network on which the NU is operational.

- Media Parameters
- NU Status in the network

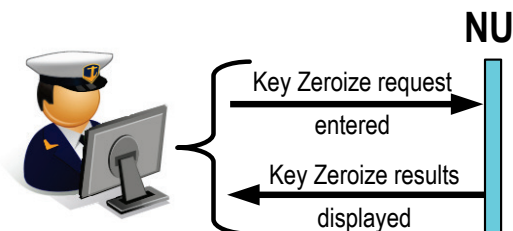
- ONCS
- Whether there is an LNE slot inserted in the network
- **Congestion Indexes**
The congestion indexes for each operational network are returned. This provides a quantized value for the congestion of each NU in the network at each message priority level.
- **Capabilities**
The SNC version and whether the NU is capable of performing the SNMU and/or the NMU role. This information is returned for itself and for all other NUs that it has received the information from.
- **Control & Status Messages**
The information provided by the DLP in some Control & Status messages can be returned to the DLP; where the information is not provided by any other option.

□ **Crypto Key Management**

In rare instances, the operator may need to zeroize the keys.

■ **Key Zeroize - Local**

Key zeroization is to be used locally if there is a risk that the unit may be compromised and the crypto keys in the LLC need to be destroyed. This can be done manually on the LLC front panel, or by an operator command, if the system is currently operational. If applicable, the operator instructs the system to request the SNC to zeroize the LLC keys, as shown in [Figure 2C.2-5](#). After the zeroization process is completed, the status of the zeroization is sent back to the operator, so that the operator will know if there was a failure to perform the key zeroization. The recommended method is to physically zeroize the LLC from the front panel. Note that an LLC front panel reset does not affect the current value of the DOW.



The SNMU can also order a specific unit to zeroize its keys, as discussed later in this section, when it considers that the unit is compromised.

Figure 2C.2-5 Key Zeroization - Local

□ **Order Automation**

A unit can receive orders from the SNMU or NMU. Some orders can be automatically accepted and/or executed by the system without operator intervention. The ability to do so is an implementation decision. This section provides information about SNC settings for automation and also the steps involved when receiving an order.

When a unit receives an order, there are two possible steps.

- Respond to the order (WILCO or CANTCO)
- If WILCO then perform the function specified in the order

The system can be set to either of the following for each type of order.

- Automatically respond with a WILCO to an order
- Allow the operator to decide whether or not to comply with the order

Similarly, the system can be set to either of the following for each type of order.

- Automatically perform the function specified in the order
- Allow the operator to decide when to perform the function

These two settings for each type of order will be preset by the system implementation. Some implementations may allow the operator to select these settings or even to modify these setting during operation.

Figure 2C.2-6 lists all orders and shows the default settings within the SNC for the Automatic Compliance Switch (ACS) and the Automatic Perform Function Switch (APFS), for each order. It also indicates whether the DLP can modify the setting.

When an ACS switch is set to OFF, either the DLP/TDS will automatically decide whether to comply or not, or in some implementations the decision may be presented to the operator. Similarly, when an APFS switch is set to OFF, either the DLP/TDS will automatically tell the SNC to perform the function, or in some implementations the operator may have to initiate the function. When the ACS switch is OFF, the APFS switch is ON, and the operator/TDS/DLP WILCOs the order, the SNC will automatically perform the function. This combination of switch settings is commonly used as the default.

Name	ACS	APFS	Modifiable
SN Closedown	OFF	OFF	Yes
NN Closedown	OFF	ON	Yes
Leave Super Network	OFF	OFF	Yes
Leave Network	OFF	ON	Yes
Join an existing Network	OFF	ON	Yes
Assume SNMU Role	OFF	ON	Yes
Assume Standby SNMU Role	ON	ON	Yes
Assume NMU Role	OFF	ON	Yes
Assume Standby NMU Role	ON	ON	Yes
Insert LNE Slot	ON	ON	Yes
Remove LNE Slot	ON	ON	Yes
Radio Silence ON - Super Network - Single NU	OFF	ON	Yes
Radio Silence ON - NILE Network - Single NU	OFF	ON	Yes
Radio Silence ON - Super Network	OFF	ON	Yes
Radio Silence ON - NILE Network	OFF	ON	Yes
Radio Silence OFF - Super Network - Single NU	OFF	ON	Yes
Radio Silence OFF - NILE Network - Single NU	OFF	ON	Yes
Radio Silence OFF - Super Network	OFF	ON	Yes
Radio Silence OFF - NILE Network	OFF	ON	Yes
Initialize New Network (DLP NCS)	OFF	OFF	No
Initialize New Network (SNC NCS)	OFF	OFF	No
Initialize New Network (Probing)	OFF	OFF	No
Re-initialization (DLP NCS)	ON	ON	Yes
Re-initialization (SNC NCS)	ON	ON	Yes
Re-initialization (Media only)	ON	ON	Yes
Re-initialization (Probing)	ON	ON	Yes
Reconfiguration (DLP NCS)	ON	ON	Yes
Reconfiguration (SNC NCS)	ON	ON	Yes
Reconfiguration (DTDMA ON)	ON	ON	Yes
Reconfiguration (DTDMA OFF)	ON	ON	Yes
Key Management – Zeroize	ON	ON	No
Key Management – Load	OFF	OFF	No
Key Management – Rollover	OFF	OFF	Yes
Radio Power Management	OFF	OFF	Yes

Figure 2C.2-6 SNC Default Function Management Switch Settings

When both switches are set to ON for an order, the processing of the received order is fully automatic and no operator action is required. Key zeroization always occurs automatically for security reasons, which is why its switches are always set to ON, and cannot be modified. Initialization of a new network and key loads are always manually performed because these require manual hardware procedures, which is why its switches are always set to OFF, and cannot be modified. Operator actions for the initialization of a new network are discussed below in the [New Network Initialization](#) section.

The figures in this Link 22 Operations section indicate the required operator actions if manual actions are used instead of automatic actions.

□ *New Network Initialization*

The SNMU may order the start of a new network. If the unit does not have the necessary hardware to join the new network, the operator should reply with a CANTCO. If the unit has the necessary hardware, but it is being used on a different network, the operator should reply with a WILCO, and then closedown the active network prior to the time of activation of the new network.

SN Closedown changes the status of the unit within the SN to be Inactive, while NN Closedown of the last (or only) active network indicates that the unit is still considered active within the SN, as it is going to restart in the same or new network as required.

The operators of all units in the new network must select an LLC and SPC for the new network. The new network hardware must be prepared, such as setting of the radio to the new frequency, and loading crypto keys if necessary. The operator informs the system when the hardware is ready, which will then start the new network initialization at the network start time.

Figure 2C.2-7 shows a case that does not require shutdown on an existing network. The exact operator actions required may differ for each implementation.

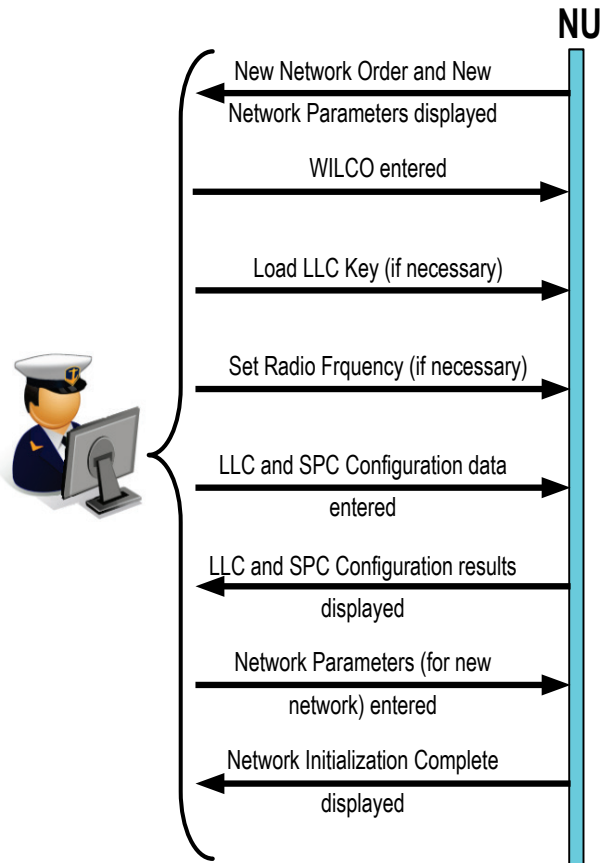


Figure 2C.2-7 New Network Initialization

□ **Role Takeover Control**

Each NU operator can specify whether role takeover is to occur automatically, or whether the operator must take action to take over a lost role. The operator can also specify the role loss timeout period which is the period used to detect the loss of a role, whether or not takeover is enabled. These values may be in the OLM; therefore, using a different set should be authorized by the operational command or by standard operating procedures. These controls may be able to be set even if the NU is not currently a Standby, as shown in [Figure 2C.2-8](#).

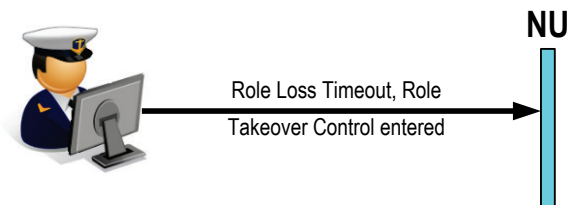


Figure 2C.2-8 Role Takeover Control

□ **Relay Flow Control Decisions**

In the rare case that automatic flow control is not able to relieve congestion, the SNC will send to the DLP all relay messages that have been received and are pending retransmission. The Operator may then have the ability to delete any of the presented messages, as shown in [Figure 2C.2-9](#). The decision to delete a relayed tactical message is based on the content of the tactical message.

The operator can also attempt to relieve some of the congestion, as detailed in section [2C.2.3 Network Management](#).

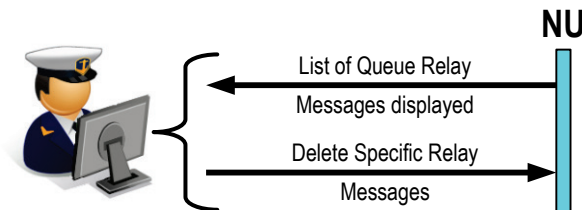


Figure 2C.2-9 Relay Flow Control

2C.2.3 Network Management

The NMU operator has control over its network. The SNMU operator can order the NMU to make changes to the network. Operational Network Management includes management of the network's parameters, and each unit's network specific settings, and consists of the following areas.

- Monitoring
- NMU Role Management
- Network Parameters Management
- LNE Support
- Radio Power Management
- Network Radio Silence

□ Monitoring

The operators of the SNMU and NMU should monitor the Link 22 system to look for trends that may require changes to the networks to improve performance.

The statistics messages can indicate potential problems in the following areas.

- NUs are disconnected in the Super Network
- Distance between NUs is greater than anticipated
- NU needs more timeslots
- NU does not need most of its timeslots
- ONCS needs improving
- Some NUs may have the wrong ONCS
- Radio power level of individual NU
- Radio interference between multiple radios of an individual NU

Operators should take actions based on trend data, not just on the current values, as these may only be valid for a short period of time and not be representative of the actual situation.

■ NU Performance Data

The SNMU and Standby SNMU receive performance data information from all the active NUs in the Super Network. The NMUs and Standby NMUs also receive the same performance data information from all active NUs in their Network. The following information is reported by every active unit on the hour, 20 minutes past the hour, 40 minutes past the hour, and upon qualified changes.

- DLP Performance Data - optional 32 bits of information from the DLP
- Super Network Connectivity Rating - indicates how well the unit is connected in the super network
- For each Network that the unit is a member, the following data is reported
 - NU Network Status – Active, Radio Silent, or Receive-Only. If an NU is inactive in a network, that network is not included in the message, so no Inactive value is included here
 - Channel Capacity Need – The capacity needed on the network as defined in [Figure 2B.2-8](#)
 - Congestion Highest Priority – indicates the highest priority (1-4) congestion experienced by the unit since the last report. 0 indicates no congestion
 - Local Tactical Utilization – the average percentage of the channel utilization used for transmitting locally injected tactical messages
 - Relay Utilization – the average percentage of the channel utilization used for relaying messages received from other NUs
 - Neighbor Quality Percentage – an indication of the overall quality of the connection between this NU and its neighbors in the network
 - Two Legs Quality Percentage – an indication of the overall quality of the connection between this NU and NUs two legs away in the network

■ **Connectivity Monitoring**

Connectivity can also be monitored by looking at the following statistical information.

- Connectivity Information
- NU Reception Data
- NU Performance Data
 - Super Network Connectivity Rating
 - Neighbor Quality Percentage
 - Two Legs Quality Percentage

It is recommended that the SNMU and Standby SNMU, and the NMUs and their Standby NMUs always be RF neighbors. After the initial period to establish connectivity, if these types of connections do not exist, role takeovers may occur.

If connectivity with their standby becomes poor, the operator of the SNMU or NMU should consider allocating the standby role to a unit that has better connectivity, preferably before the connectivity is lost.

If connectivity becomes poor or the trend is indicating that it is deteriorating, the NMU operator should consider initiating a change in network parameters in order to optimize the network for the current conditions. Alternatively, the SNMU operator can order the NMU to perform the change in network parameters.

■ ***Capacity Monitoring***

The SNMU and NMU operator, depending on the system implementation, should be able to monitor the capacity usage of all units by looking at the following statistical information from the NU Performance Data.

- Channel Capacity Need
- Congestion Highest Priority
- Local Tactical Utilization
- Relay Utilization

If a unit is not congested, local and relay tactical utilization information indicates how much of the channel capacity a unit is using. When congestion is high the total channel utilization will also be high. Ideally the channel utilization is high and the congestion is low, which indicates that the correct amount of timeslots (capacity) has been assigned to the unit. To manage capacity effectively, an important factor is the type of mission, and therefore the priority of traffic that a given unit is injecting. This can change many times during a mission. If two units require additional capacity, it is not necessarily the one with the highest load that should be given capacity, but the one with the highest load of high priority traffic. The priority of the traffic is an important aspect that needs to be assessed.

Congestion may be relieved at the network level by the NMU operator modifying the following network parameters or by the SNMU operator ordering the NMU to modify any combination of the following parameters.

- Enable DTDMA: if not currently enabled
- Change the ONCS: change the allocation of capacity to the NUs in the network, possibly by adding or removing NUs from the network. At the SNC level, this is called “**Reconfiguration**” of the network
- Change the Media Parameters: change one or more parameters such as frequency or media setting number. At the SNC level this is called “**Re-initialization**” of the network. This may also include changing the ONCS and enabling or disabling DTDMA

□ NMU Role Management

The SNMU or NMU operator can order another unit to assume the NMU or Standby NMU role. An order can be for either a future time, or the current time. An example of an NMU ordering a unit to become the Standby NMU is shown in [Figure 2C.2-10](#).

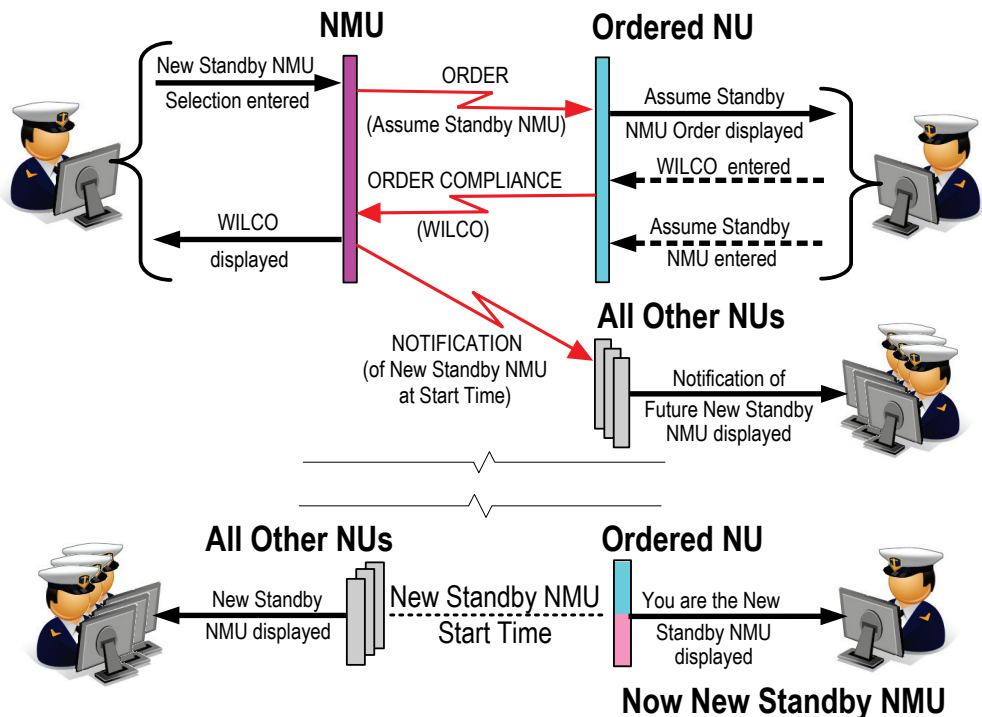


Figure 2C.2-10 New Standby NMU Order

When the Standby NMU detects the loss of the NMU, and automatic takeover is disabled, the Standby NMU operator needs to direct the unit to become the NMU, as shown in [Figure 2C.2-11](#). If the operator knows that there is a possible error in the situation, for example local hardware problems, the operator may decide not to assume the NMU role (if it is known by other means that the NMU unit is still active).

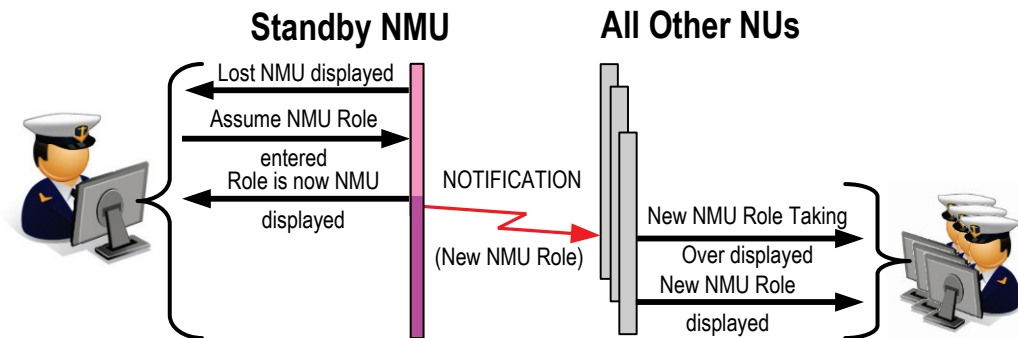


Figure 2C.2-11 Lost NMU

If automatic takeover is enabled, and the operator knows that its SNC incorrectly assumed the NMU role, the operator should direct the SNC to change its status back to the Standby NMU role.

It may be possible that more than one NU assumes the NMU role. This is reported to the operator, upon detection of relevant traffic. The situation must be resolved externally, normally with the previous standby NMU reporting the correct NMU to its SNC, and directing its SNC to become the Standby NMU again, as shown in [Figure 2C.2-12](#).

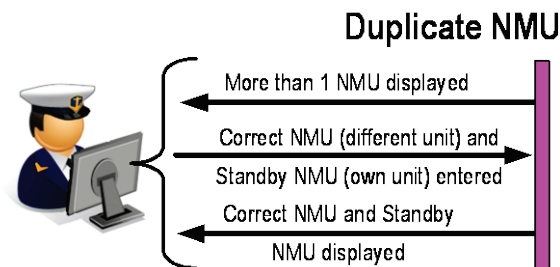


Figure 2C.2-12 Duplicate NMU

The NMU is responsible for ensuring that there is always a Standby NMU. When a new network is being started, the SNMU will order a unit to become the NMU, and normally, will also order another unit to become the Standby NMU. If after 15 minutes, no Standby NMU has been allocated by the SNMU, the NMU operator unit must assign a Standby NMU for the new network.

If both the NMU and Standby NMU are lost, the situation can be resolved by the SNMU ordering a unit to become the new NMU and another to become the new Standby NMU. All other units will be informed of the role changes.

□ ***Network Parameters Management***

Once a network has been initialized, the NMU operator has the responsibility for control of the network. The NMU operator achieves this by managing a network's parameters, which consists of the following.

- DTDMA Enabled/Disabled Flag
- Operational Network Cycle Structure
 - Provided by the DLP
 - Calculated by the SNC
- Media Segment Parameters
 - Media Type
 - Frequency / Frequency Hopset
 - Media Setting Number (Waveform)
 - Fragmentation Rate
 - LLC Integrity Flag
 - SPC Radio Power

The time the change is to take effect must also be specified. Changes can occur any time after the OST of a network during normal operation. Enough time must be given for the distribution of the information to all units, and for manual physical changes to be made, if necessary, such as switching to a different radio (different media type), changing frequency, or changing radio power.

The SNMU can also order the NMU to make changes to a network. Orders and commands must be given at least 10 minutes prior to the time the new parameters are to take effect, to allow sufficient time for distribution of the information.

Changes to a network are used to correct Network deficiencies, to optimize the overall Network performance, or to perform changes due to frequency restrictions. Threat assessment may require changing fixed frequency radios to EPM. Monitoring of the

network statistical information and its trends may be used to determine if a change to the network may be necessary.

Refer to section 2B.2.2 subsection [Planner Defines the NCS Manually](#) for considerations when providing an NCS, and subsection [The SNC will calculate the NCS](#) for details about the parameters that must be supplied when the SNC is to calculate the NCS.

■ **Changing the Network ONCS or DTDMA flag**

Figure 2C.2-13 shows what happens when the NMU operator changes the NCS parameters that the SNC uses to calculate the NCS. The modified parameters are sent to the SNC which calculates a new NCS and supplies it back for display to the NMU operator, who can accept the NCS, or send different parameters for the SNC to use to recalculate another new NCS. Figure 2C.2-13 shows the NMU operator accepting the calculated NCS. The new NCS is then distributed to all the other units in the network which acknowledge receipt. At the specified time the units will change the ONCS to the new one.

The NMU operator will be informed of which units in the network acknowledged reception of the command and which units did not.

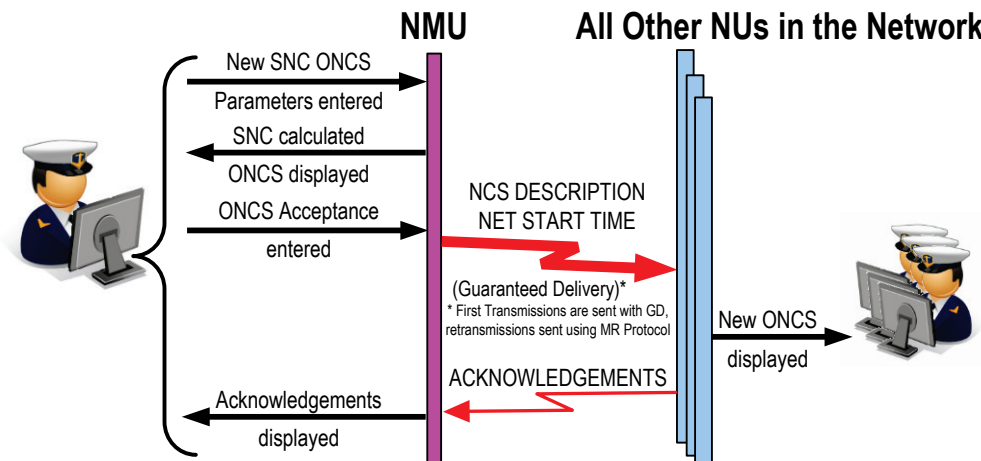


Figure 2C.2-13 Changing the ONCS

■ ***Changing the Network Media Parameters***

When changing the media parameters the operator must be aware of the capabilities of each unit to ensure that each unit is capable of using the new media parameters. For example, if the operator wants to change the Media Type, each unit in the network requires an SPC, radio and antenna for the new media. Note that special considerations must be taken when changing the media type. Refer to [Appendix B Troubleshooting](#) for further details.

When operating a HF network, media parameters (especially the frequency) may need to be changed relative to the time of day because of changing characteristics of the ionosphere. During the day, the ionosphere is more active (due to the solar radiation), and it is better to use higher frequencies. At night, the ionosphere is more stable and a lower frequency will work better; therefore different frequencies might be used during the day and night.

The diurnal variation of HF propagation is characterized by a simple rule-of-thumb: The frequency follows the sun (the higher the sun the higher the frequency and vice versa).

The Media Setting Number can be changed to increase bandwidth. However, MSNs with increased bandwidth are less error-resistant. This may cause loss of connectivity to units with already poor connectivity.

One option that the NMU has to attempt to optimize the communications, is to restart (reinitialize) the network, using probing, which causes the network members to transmit using a sequence of different media setting numbers in an attempt to find which is the best. The NMU can be ordered to do this by the SNMU, as shown in [Figure 2C.2-14](#). If the NMU is not ordered by the SNMU, then only the actions of the lower part of the figure are performed. Refer to subsection [Probing Network Initialization](#) of section [2C.1.4](#) above for further details about the Probing protocol.

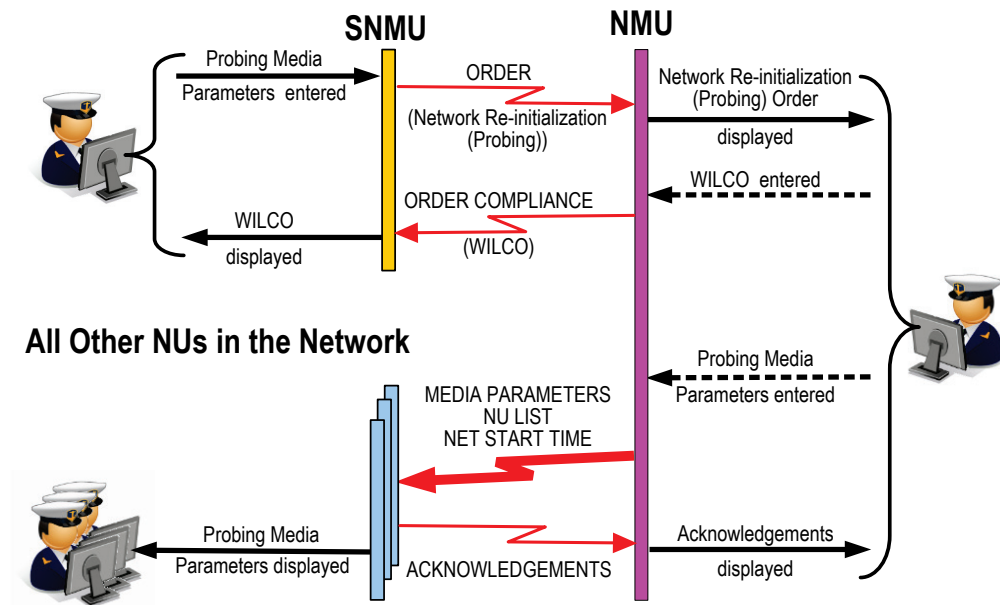


Figure 2C.2-14 Change Media Parameters Order

Note: as it uses the last probing configuration to distribute the selected configuration, it is good practice to select the last configuration as one with good probability that the NUs will receive the transmissions.

□ **LNE Support**

The NMU supports LNE by performing the following functions.

- Insertion and Removal of the LNE Slot
- Granting or Denying Transmission Capacity to the LNE Unit
- Reconfiguring the Network to include the LNE Unit in the ONCS

■ **Insertion and Removal of the LNE Slot**

When an LNE unit is not currently part of any network, and intends to perform a non-silent join, an LNE Slot must be inserted into the ONCS, prior to the time the LNE unit starts the LNE process. The LNE unit uses the LNE slot to communicate on the network during the join operation.

The NMU operator can insert the LNE Slot, or the SNMU operator can order the NMU to insert the LNE slot. The change can be for either a future time, or the current time. [Figure 2C.2-15](#) shows an Insert LNE Slot order. If the NMU operator inserts the LNE Slot without receiving an order from the SNMU, then only the lower part of the figure is performed.

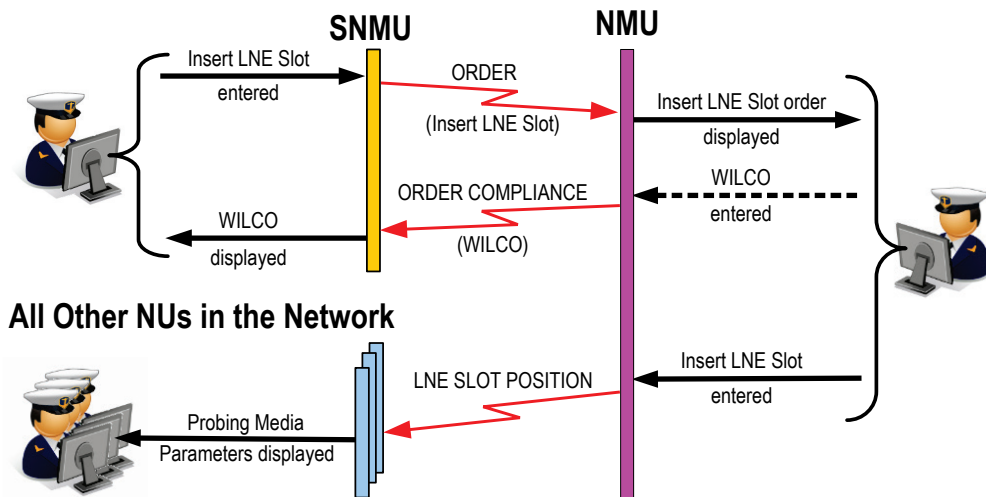


Figure 2C.2-15 Insert LNE Slot Order

The insertion or deletion of an LNE Slot at all the other units in the network is an internal SNC function, and is not displayed to the operator.

When there are no units wanting to join the network or the NMU does not want any unit(s) to attempt to join, the LNE slot is no longer required and can be removed by the NMU.

No LNE Slot is needed if the LNE unit is already active on another NILE Network within the Super Network.

■ **Granting or Denying Transmission Capacity to the LNE Unit**

If the LNE unit requires transmission capacity that is not yet allocated in the ONCS, the NMU SNC will ask the NMU DLP/TDS/operator to allocate capacity for the LNE unit. The operator/TDS/DLP can make changes to the ONCS to allocate capacity for the LNE unit as shown in [Figure 2C.2-16](#), or decide to not immediately allocate any capacity to the LNE unit and modify the network ONCS after the LNE process is

complete. Whether the NMU operator or the TDS/DLP makes the changes to the ONCS is an implementation decision.

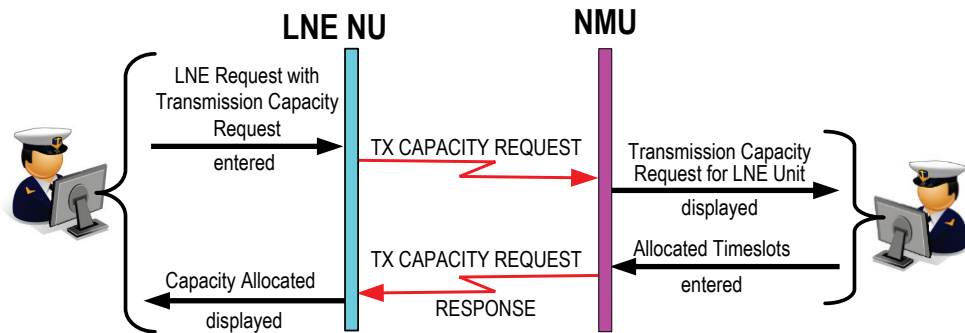


Figure 2C.2-16 LNE Transmission Capacity Request

■ **Reconfiguring the Network to include the LNE Unit in the ONCS**

The SNMU or NMU operator may want to change the network ONCS prior to the time the LNE unit is going to join the network, in anticipation of allocating capacity for the LNE unit, if necessary. The OLM may have already specified capacity for the LNE unit, in which case, no change of ONCS is necessary. The operator needs to assess interactions of protocols, as modifying the network parameters while a unit is attempting LNE may cause the process to fail. However, the system does not prevent this as the operator is in control of the priority of the activities as there may be a tactical reason for the change, and if the LNE unit fails, it can try again.

The NMU should perform network parameter changes before or after the planned LNE, but preferably not during the LNE protocol.

□ Radio Power Management

The SNMU or NMU operator can order a unit to change its radio transmission power on a network, independent of any other network changes. [Figure 2C.2-17](#) shows the NMU ordering a unit to change its radio power level. Subsection [Change Radio Power](#) of section 2C.2.1 details how the unit then adjusts its own power.

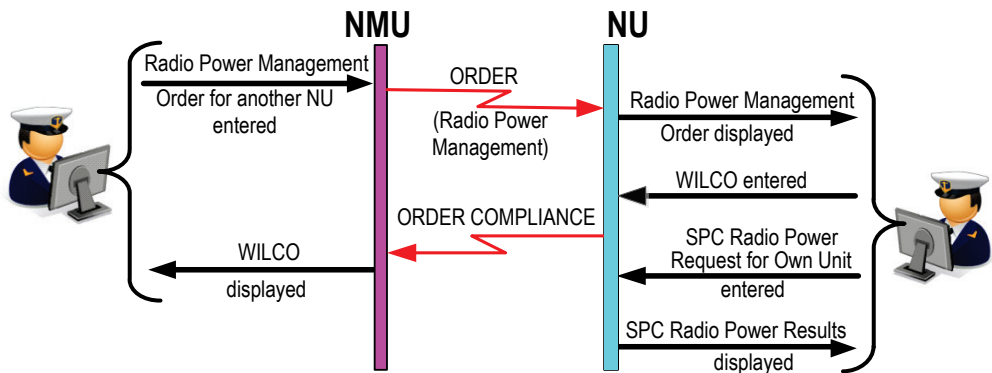


Figure 2C.2-17 Radio Power Management Order

□ Network Radio Silence

The SNMU or NMU operator can order an entire network to turn Radio Silence on or off at either a future time, or the current time. The SNMU or NMU operator can also order an individual unit to turn Radio Silence on or off in the network at either a future time, or the current time. A Radio Silence ON order can also include the time to turn Radio Silence off, as shown in [Figure 2C.2-18](#) for a Network Radio Silence order from the NMU.

If there is sufficient time for units to respond, unit responses to the order can be displayed to the operator, as shown in [Figure 2C.2-18](#). If the order requires going to Radio Silence immediately, no response is expected.

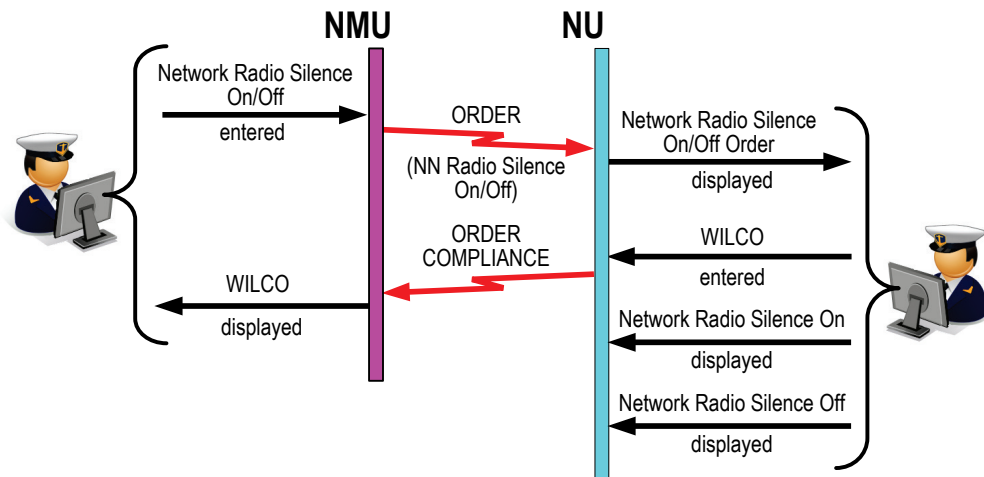


Figure 2C.2-18 Network Radio Silence Order

2C.2.4 Super Network Management

In addition to being able to order the NMU of a network to perform the network management functions described above, the SNMU operator has control over the Super Network which consists of the following areas.

- SNMU Role Management
- MASN Management
- Crypto Key Management
- New Network Creation
- Address Management
- LNE Support
- Status Management
- Relay Setting Management
- Super Network Parameter Distribution
- Super Network Radio Silence

□ **SNMU Role Management**

SNMU and Standby SNMU role management is performed by the SNMU in the same manner as NMU and Standby NMU management, as explained in the subsection

[NMU Role Management](#) of section 2C.2.3 above, but substituting NMU with SNMU, and Standby NMU with Standby SNMU.

If both the SNMU and the Standby SNMU are lost, the situation can be resolved by the operator of one NU setting itself to be the SNMU, and then ordering another NU to be the Standby SNMU. All other NUs will be informed of the role changes.

□ **MASN Management**

MASNs are lists of units, which can be initially defined in the OLM, and managed by the SNMU. There are 32 MASNs numbered 0-31, with MASNs 1–8 defined as the network membership MASNs for networks 0–7. The SNMU Operator can change any MASNs, using the following commands.

- Create MASN
- Modify MASN
- Delete MASN

These commands must be sent at least 10 minutes prior to the time of change, so that the system has time to distribute the information to all the units.

Send MASN and Network Membership Commands at least 10 minutes before the change is required to be complete.

The SNMU operator is informed of whether or not each unit in the Super Network received the MASN command.

■ **Create MASN**

The SNMU operator can create a new MASN. If the MASN defines network members for a new network, the new network membership MASN must be given prior to the order to initialize the new network.

Create the MASN for a new network before creating the new network.

Network membership MASNs should include all units expected to transmit, as well as any radio silent or receive-only units that are expected only to listen. The MASN can also include units that are expected to join the network later.

[Figure 2C.2-19](#) shows the creation of a MASN. Similar flows occur for MASN modification and deletion.

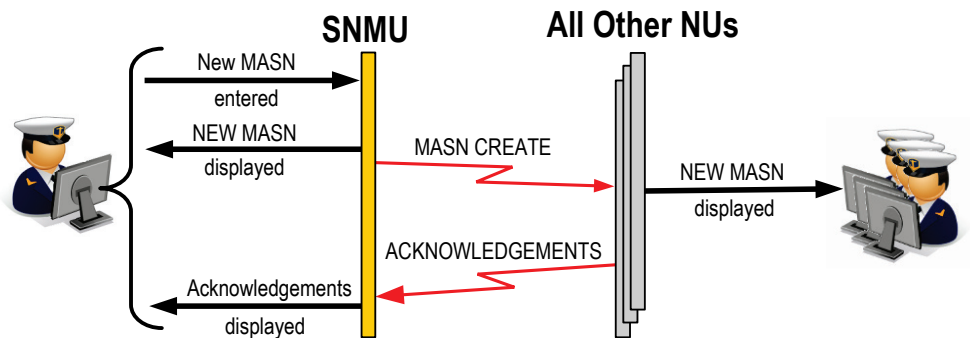


Figure 2C.2-19 Create MASN

■ **Modify MASN**

The SNMU operator can modify a MASN by adding and/or deleting units. When a unit is going to join a network, it must be added to the network's membership MASN if it is not already a member of that MASN. If the LNE is known in advance, the MASN should be updated before the start of LNE.

■ **Delete MASN**

The SNMU operator can delete a MASN. Network membership MASNs for active networks must not be deleted until the network has been shut down.

Do not delete a MASN until it is no longer needed. Do not delete a network membership MASN 1-8 until its associated network has been shut down!

□ **Crypto Key Management**

The SNMU is responsible for the following Crypto Key Management activities.

- Key Load
- Key Zeroize

Note that during normal operations, key rollovers occur automatically at midnight. No SNMU control of key rollovers is required.

■ **Key Load**

If the crypto key has been compromised or a different crypto key is planned to be used, the SNMU operator can send an order to all units in the Super Network to inform them of the time to load the new crypto key, as shown in [Figure 2C.2-20](#). Key

distribution or notification will occur through a secure channel outside the scope of Link 22. Each unit's operator must ensure that the new key material is acquired via the approved channels, and loaded at the specified time.

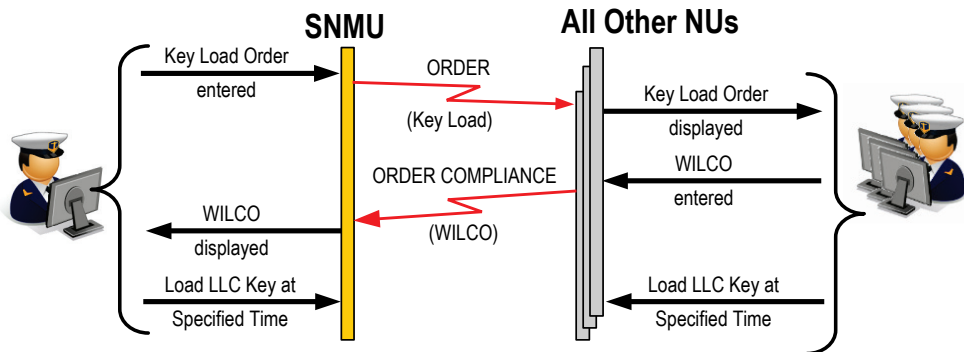


Figure 2C.2-20 Key Load Order

■ Key Zeroize

The SNMU operator can order a unit to zeroize its crypto keys immediately, as shown in [Figure 2C.2-21](#). This provides the SNMU with a means of deleting the keys of a unit that may have been physically compromised. The unit will immediately zeroize its keys, so the SNMU operator will not receive any response from the unit. The SNMU operator may want to send the order repeatedly to ensure that whenever the compromised unit can receive, the unit zeroizes its keys.

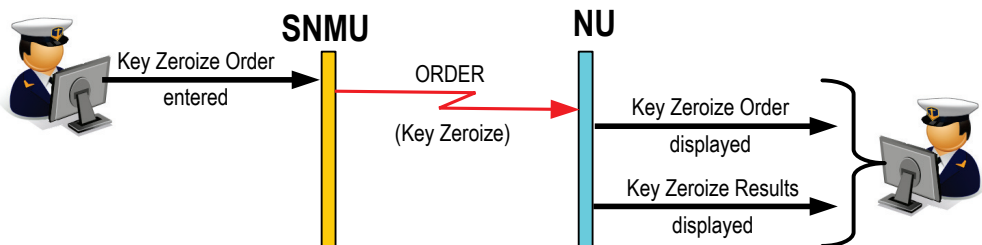


Figure 2C.2-21 Key Zeroize Order

□ **New Network Creation**

The SNMU operator can order the creation of a new NILE Network, which involves the following steps.

- Creation of the new network membership MASN
- Order network members to initialize the new network
- Order one of the members to assume the NMU role for the new network
- Order one of the members to assume the Standby NMU role for the new network

The network membership MASN for the new network must be created before the new network is created. The network membership MASN should include all units expected to transmit, as well as any radio silent or receive-only units that are expected only to listen. The MASN can also include units that are expected to join the network later.

The initialization of a new network can be performed in three ways.

- Short Initialization with operator/TDS/DLP-defined NCS
- Short Initialization with SNC-calculated NCS
- Probing Initialization

[Section B Planning](#) provides details on the parameters required for each initialization type.

[Figure 2C.2-22](#) shows the flow for an order to initialize a new network using Short Network Initialization with an operator defined NCS. Details on the actions required for each unit to initialize on the new network are included in [section 2C.2.2 Advanced NU Management](#).

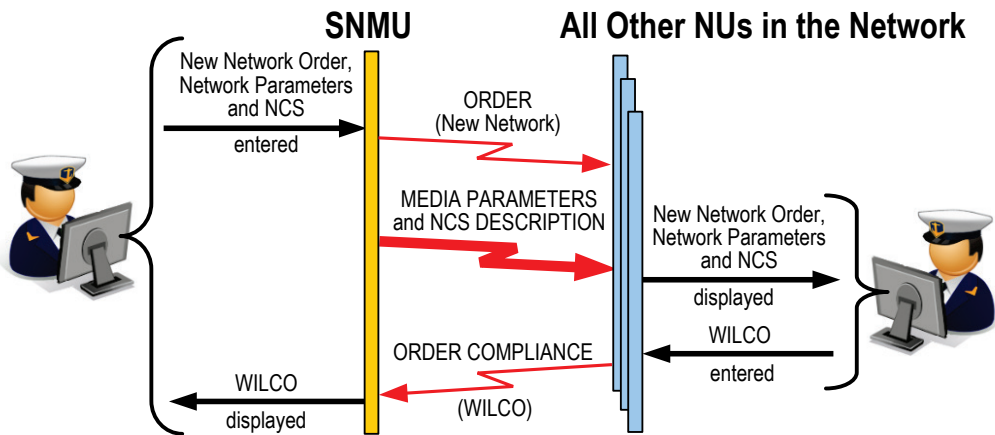


Figure 2C.2-22 New Network Order

When the SNMU operator knows which units will comply with the new network order, the operator must choose one of the new network members to assume the NMU role, and another to assume the Standby NMU role for the new network.

Depending on the start time of the new network, the SNMU should avoid sending role changes at a time that the new NMU or Standby NMU may be closing an existing network to activate the new network.

□ Address Management

The SNMU is responsible for adding a new unit's Link 22 Address to the Super Network. The Super Network is limited to 125 units. The SNMU operator will be informed of the success or failure of the addition of the new unit. If the addition of the unit decreases the number of remaining addresses to less than 10, the SNMU operator will be informed. All other units are informed of the added NU, as shown in [Figure 2C.2-23](#).

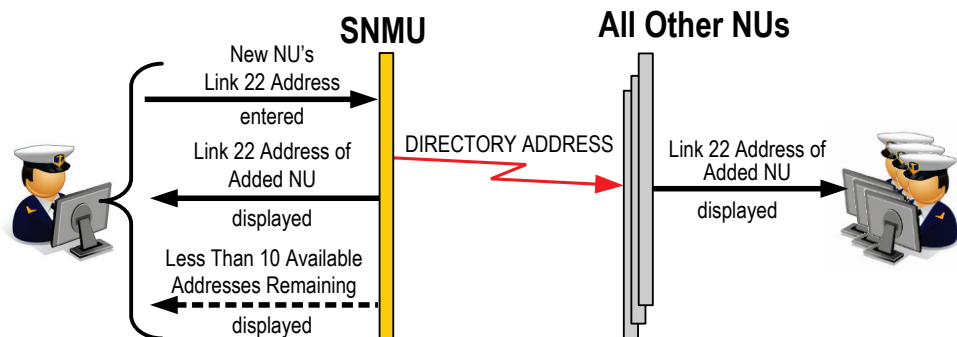


Figure 2C.2-23 Address Management

□ **LNE Support**

The SNMU supports the LNE protocol by optionally performing any of the following.

- Add the LNE unit to the Super Network
- Add the LNE unit to the Network Membership MASN
- Grant or Deny LNE access to the Network
- Order a unit to join an existing network using LNE

■ **Add the LNE unit to the Super Network**

If the LNE unit is not a member of the Super Network, the SNMU can add the unit's Link 22 address to the Super Network, as discussed in [Address Management](#) above. The addition can be completed before the LNE unit sends the request to join, or upon receiving the request during LNE.

■ **Add the LNE unit to the Network Membership MASN**

The SNMU operator should add the LNE unit to the network membership MASN prior to the time the LNE unit is going to join the network, if the unit is not already a network member. MASN operations are a separate topic detailed previously. The addition can be completed before the LNE unit sends the request to join the network, allowing the supporting unit to respond immediately, or upon receiving the request from the supporting unit, if the Link 22 address is not yet included in the MASN.

■ **Grant or Deny LNE access to the Network**

The SNMU operator will be asked to grant the LNE request, if the unit is not yet listed in the network's MASN. The SNMU operator has the following choices.

- Deny the request
- Grant the request
- Grant the request in a different network

Figure 2C.2-24 shows the SNMU granting access on the requested network.

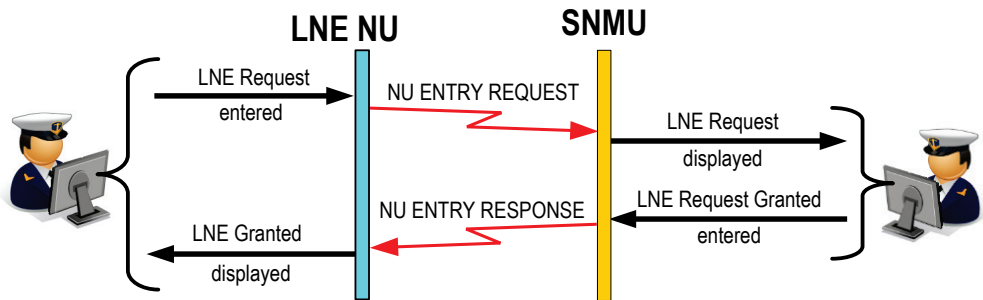


Figure 2C.2-24 LNE Request Granted

■ **Order a unit to join an existing network using LNE**

The SNMU operator can order a unit to join an existing network using LNE, if the unit is already a member of another network. The ordered unit then performs an active join LNE protocol.

□ **Status Management**

Each unit has one of the following NU Status values in the Super Network.

- Active
- Radio Silent
- Received Only
- Inactive

The SNC can automatically detect when a unit changes between some of these states, but not all of them. The SNMU operator must report the NU Status changes listed in Figure 2C.2-25, because the assessment requires knowledge not transmitted by the NU changing state. The NU Status Change protocol is shown in Figure 2C.2-26.

Current State	New State
Inactive	Receive-Only
Inactive	Radio Silent

Current State	New State
Receive-Only	Inactive
Receive-Only	Radio Silent
Radio Silent	Inactive

Figure 2C.2-25 SNMU Operator Reportable NU Status Changes

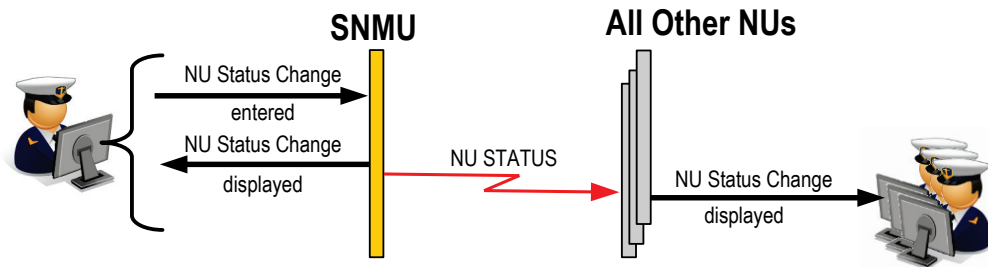


Figure 2C.2-26 NU Status Change

When a unit goes into Radio Silence on the Super Network, or when it becomes Receive-Only, the SNMU operator should ensure connectivity information is maintained. This may require neighbor units to report the connectivity between themselves and the Receive-Only or Radio Silent unit. The SNMU operator must supply the Complementary Quality of Link (CQOL) values for the neighbor unit to report, as shown in [Figure 2C.2-27](#). The CQOL value can be one of the following.

- Poor – some missing data
- Good – some corrected errors (Recommended Default)
- Excellent – no errors

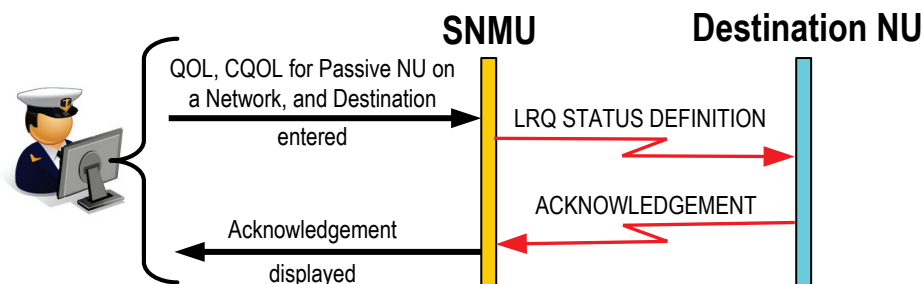


Figure 2C.2-27 Passive NU Connectivity Reporting

The SNMU Operator can also turn off the reporting of CQOL if the passive NU is no longer in the network. If transmissions are received from the passive unit, then the reporting unit will stop reporting the artificial value and send the actual value.

□ **Relay Setting Management**

The default Relay Setting of all units is set as automatic. The SNMU operator can instruct the SNC to change the Relay Setting of a unit to one of the following choices.

- Automatic
- Inhibited from performing relay
- Preferred relayer

The SNMU DLP is informed of whether the units received or did not receive the relay setting command, as shown in [Figure 2C.2-28](#).

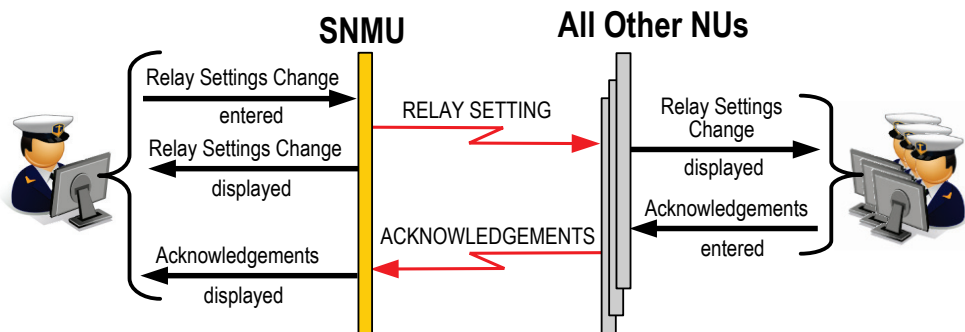


Figure 2C.2-28 Relay Setting Change

□ **Super Network Parameter Distribution**

If the SNMU operator determines that a particular unit does not have the correct Super Network parameters, known as the Super Network (SN) Directory, the SNMU operator can instruct its SNC to supply the correct parts of the SN Directory to the unit, as shown in [Figure 2C.2-29](#). This can occur when a unit has joined the network in Radio Silence.

The Super Network Directory consists of the following information:

- NU Addresses
- NU Roles
- Relay Setting
- NU Status
- MASNs

There are two copies of the SN Directory information available, the original OLM copy (version zero) and the current version. The SNMU operator must supply which version, the OLM or current version, of the SN Directory and which of the above five SN Directory components the SNC must send. An SN Directory version number greater than zero indicates that there have been changes made in that component since the OLM.

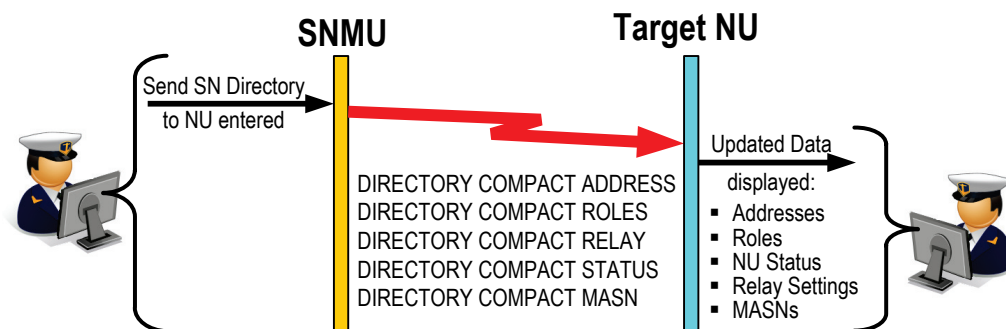


Figure 2C.2-29 SN Directory Distribution

The SNMU operator can optionally instruct the SNC to send the SN Directory information to all units.

□ **Super Network Radio Silence**

The SNMU operator can order all units to turn Radio Silence on or off in the Super Network at either a future time, or the current time. The SNMU operator can also order an individual unit to turn Radio Silence on or off in the Super Network at either a future time, or the current time. A Radio Silence ON order can also include the time to turn Radio Silence off. [Figure 2C.2-30](#) shows the SNMU ordering Radio Silence ON in the Super Network.

Each unit replies to the order, if there is time to make a response. If the order is to go to Radio Silence immediately, there should be no responses.

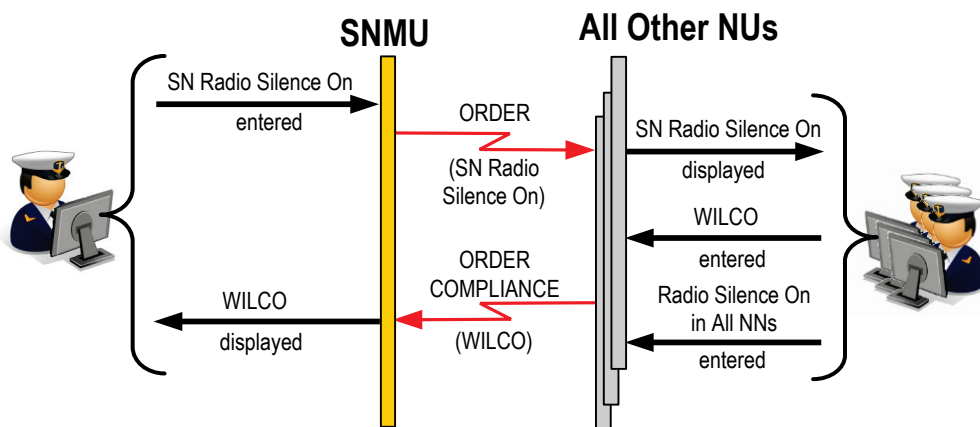


Figure 2C.2-30 Super Network Radio Silence Order

2C.3 Termination

Termination of operations occurs on three levels.

- NU Termination
- Network Termination
- Super Network Termination

2C.3.1 NU Termination

The NU operator can direct the unit to permanently leave a specific NILE Network, or the entire Super Network at a specified time. The NMU can order a NU to leave a network. The SNMU can order a NU to leave a network or the entire Super Network. All other NUs are informed about what the NU is going to do. The DLP/TDS/operator of the leaving NU is informed when communications have been terminated on the network. [Figure 2C.3-1](#) shows a NU leaving a network as requested by its operator.

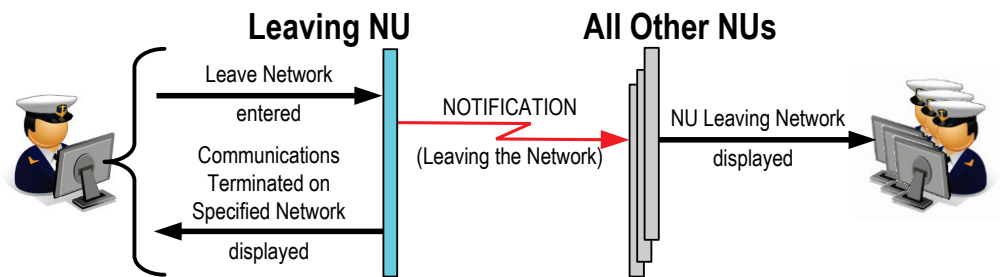


Figure 2C.3-1 NU Termination

2C.3.2 Network Termination

The SNMU or NMU operator can order a network to be shut down at a time sufficiently in the future (minimum 10 minutes) for the protocol to be completed for all NUs in the network, as shown in [Figure 2C.3-2](#), for an order from the NMU. All operators/TDS/DLPs are informed when communications have been terminated on the network.

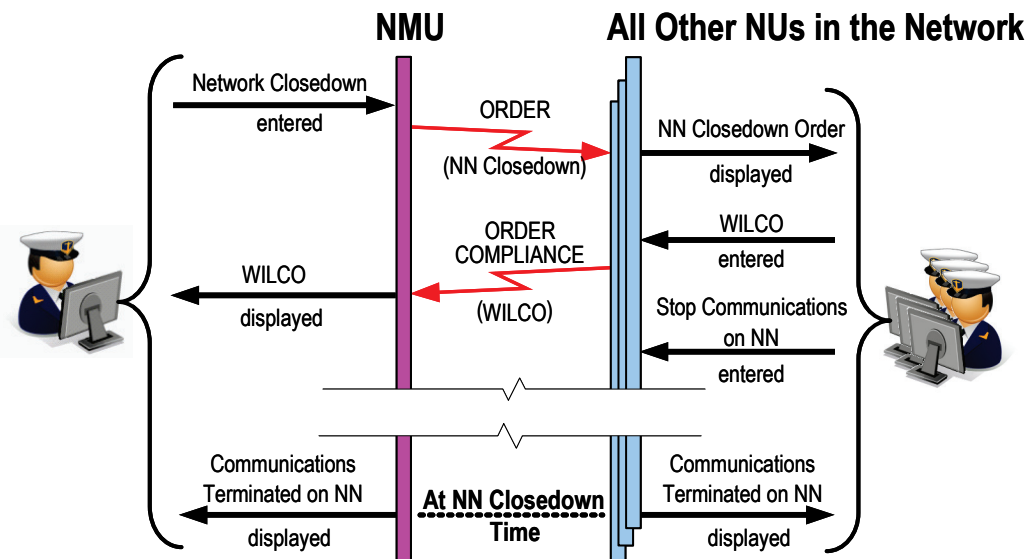


Figure 2C.3-2 Network Termination

2C.3.3 Super Network Termination

The closedown of an entire Super Network must be ordered by the Officer in Tactical Command (OTC). The SNMU operator then orders the Super Network to be shut down at a time sufficiently in the future (minimum 10 minutes) for the protocol to be completed for all NUs in the Super Network. If any NUs do not respond to the SNMU, it does not matter, as the SNMU and all other units that received the order will shut down at the specified time. The operators/TDSs/DLPs are informed when communications have been terminated in the Super Network, as shown in [Figure 2C.3-3](#). Alternatively, external notification of a Super Network closedown could be given, followed by each operator manually initiating its own closedown.

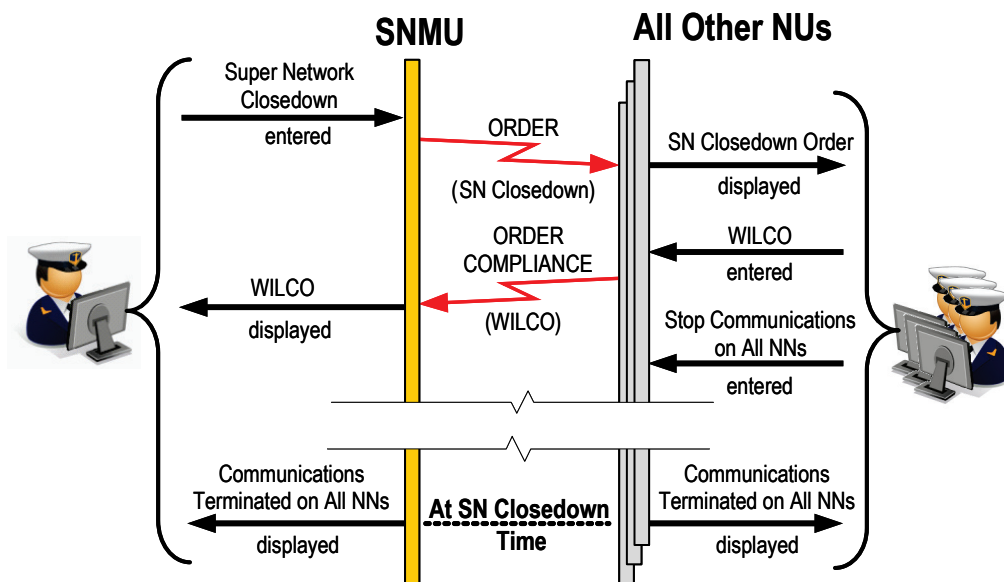


Figure 2C.3-3 Super Network Termination


Ensure sufficient time is available before sending Network or Super Network Termination, or Radio Silence for a Network or the entire Super Network, as the SNMU or NMU requires time to broadcast the change before changing its own status.

2C.4 Operator Actions Summary

Figure 2C.4-1 summarizes the management actions that can be taken during normal operations, and indicates which operators can issue the action.

Action	Issuer
NMU/Standby NMU Role Change	NMU, SNMU
SNMU/Standby SNMU Role Change	SNMU
Network Re-initialization/Reconfiguration	NMU, SNMU
New Network Creation	SNMU
MASN Change	SNMU
NU Status Management	SNMU
Link Quality Status	SNMU
Relay Setting Change	SNMU
SN Directory Distribution	SNMU
NU Radio Power Change	NU, NMU, SNMU
NU Radio Silence Change	NU, NMU, SNMU
Network Radio Silence Change	NMU, SNMU
Super Network Radio Silence Change	SNMU
Key Rollover	NU
Key Zeroize	NU, SNMU
Key Load	SNMU
Order Automation Setup	NU
Role Takeover Control Setup	NU
Relay Flow Control Decisions	NU
Request Management Information	NU
SN Directory Request	NU
Join Network (Late Network Entry)	SNMU, NU
NU Leave Network	NU, NMU, SNMU
NU Leave Super Network	NU, SNMU
Network Termination	NMU, SNMU
Super Network Termination	SNMU

Figure 2C.4-1 Management Operator Actions



This page is intentionally left blank.

Section D Tactical Messages

Link 22 conveys its tactical information in specially formatted messages. These tactical messages are composed of sets of fields, each of which is composed, in turn, of a prescribed number of bits that may be encoded into predetermined patterns to convey specific information. The fields contained within the tactical messages are defined in a data element dictionary. Each definition in the data element dictionary is indexed by a combination of two numbers, the Data Field Identifier (DFI) and the Data Use Identifier (DUI). These are more commonly referred to as the DFI:DUI. The DFI indexes to a group of fields that are similar, and the DUI indexes to the specific field in the group. Link 22 messages were defined using the Link 16 data element dictionary.

The tactical messages specifically defined for Link 22 are called the F-Series messages. Due to the use of the Link 16 (J-Series) data element dictionary, F-Series messages are part of the J-family of messages. The F-Series messages are composed of two distinct groups. The first group is an encapsulation of some of the Link 16 (J Series) 70-bit message words inside a 72-bit F-Series message word, which are called “FJ” tactical messages. The second group is the “Unique F-Series” tactical messages, which have been designed specifically for Link 22 and which have no exact corresponding message in Link 16. The reasons for these unique messages were to provide either the same capability as Link 16 but with messages that used less bandwidth than the Link 16 messages used for the same information, or to provide information communication that was not supported by Link 16.

This tactical messages section includes the specific Link 22 design goals which help to provide a better understanding of both current selections and rationale behind the choices. This section is based on [STANAG 5522] Edition 3. Any comparison to Link 11 and Link 16 in this section is only provided to emphasize the advantages of Link 22 tactical messages. More details about multilink comparisons are provided in [Section E](#).

This section consists of the following.

- Design Goals
- F-Series Catalog
- Tactical Message Hierarchy
- Message Sequence
- TMW Construction
- Message Sequence Examples
- Link 22 Message Description
- Message Extrapolation
- Stacked Fields

2D.1 Design Goals

The main goals in designing the Link 22 tactical messages were as follows.

- To be as compatible as possible with Link 16
 - Use the same geodetic reference system for track position
 - Use the same 15-bit Unit Address
 - Use the same 19-bit Track numbering
 - Use Encapsulated J-Series messages if possible
 - Define non-encapsulated, new messages to save bandwidth and provide messages not in J-Series
 - Define new messages using Link 16 Data Element Dictionary
- To provide greater accuracy than Link 11
 - Improve tracking Accuracy
 - Increase limited field sizes
 - Increase range of operation
 - Simplify forwarding difficulties
- To utilize the available bandwidth more efficiently than Link 16
 - Define new messages minimizing repetition of non-critical data
 - Have most frequently needed data in a single tactical data word
- To provide a layered communications architecture
 - Ensure that tactical data is handled at the DLP or higher level
 - Track position extrapolation to be performed by the DLP
 - Tactical messages are “sealed envelopes” opened only at DLP level

2D.2 F-Series Catalog

Figure 2D.2-1 provides the catalog of Link 22 (F-Series) tactical messages/words, as listed in [STANAG 5522].

Message/Word	Abbreviation	Message/Word Title
F01.0-0	IFF	IFF
F01.0-1	STMIS	Surface Track SAM/SSM
F01.4-0	B/R RESOLVE	Acoustic Bearing/Range Resolved
F01.4-1	B/R AMBIG	Acoustic Bearing/Range Ambiguous
F01.5-0	B/R AMP	Acoustic Bearing/Range Amplification
F01.5-1	B/R SENS	Acoustic Bearing/Range Sensor
F01.5-2	B/R FREQ	Acoustic Bearing/Range Frequency
F01.5-3	B/R AMP 1	Acoustic Bearing/Range Amplification 1
F01.6-0	BAS COM	Basic Command
F01.6-1	COM EXT1	Command Extension
F01.6-2	AIR COORD	Air Coordination
F01.7-0	R/C	Response
F02.0-0	IND PLI AMP	Indirect PLI Amplification
F02.0-1	IND PLI AMP CONT	Indirect PLI Amplification Continuation
F02.1-0	PLI IFF	PLI IFF
F02.2-0	AIR PLI CAS	Air PLI Course and Speed
F02.2-1	AIR PLI AMC	Air PLI Additional Mission Composition
F02.3-0	SUR PLI CAS	Surface PLI Course and Speed
F02.4-0	SUB PLI CAS	Subsurface PLI Course and Speed
F02.4-1	SUB PLI AMC	Subsurface PLI Mission Correlator
F02.5-0	LPT PLI CONT	Land Point PLI Continuation
F02.6-0	LTR PLI CAS	Land Track PLI Course and Speed
F02.6-1	LTR PLI MC	Land Track PLI Mission Correlator
F03.4-0	ASW INFO	ASW Contact Information
F03.4-1	ASW CONCONF	ASW Contact Confirmation
F1-0	IND PLI POS	Indirect PLI Position
F1-1	PLI POS	PLI Position
F2	AIR POS	Air Track Position
F3	SUR POS	Surface Track Position
F4-0	SUB POS	Subsurface Track Position
F4-1	SUB CAS	Subsurface Track Course and Speed

Message/Word	Abbreviation	Message/Word Title
F5-0	AIR CAS	Air Track Course and Speed
F5-1	SUR CAS	Surface Track Course and Speed
FJ3.0	REF POINT	Reference Point
FJ3.1	EMERG POINT	Emergency Point
FJ3.5	LAND PT/TRK	Land (Ground) Point/Track
FJ3.6	SPACE TRCK	Space Track
FJ3.7	EW PROD	Electronic Warfare Product
FJ6.0	AMPL	Track/Point Amplification
FJ7.0	TRACK MAN	Track Management
FJ7.1	DUR	Data Update Request
FJ7.2	CORREL	Correlation
FJ7.3	POINTER	Pointer
FJ7.4	TRACK IDENT	Track Identifier
FJ7.5	IFF MAN	IFF/SIF Management
FJ7.6	FILTER	Filter Management
FJ7.7	ASSOC	Association
FJ8.1	MSNCOR	Mission Correlator Change
FJ9.1	ENG COORD	Engagement Coordination
FJ10.2	WES	Engagement Status
FJ10.3	HANDOVER	Handover
FJ10.5	CU REPORT	Controlling Unit Report
FJ10.6	PAIRING	Pairing
FJ12.4	CON CHG	Controlling Unit Change
FJ13.0	A/F STATUS	Airfield Status
FJ13.2	AIR STATUS	Air Platform and System Status
FJ13.3	SUR STATUS	Surface Platform and System Status
FJ13.4	SUB STATUS	Subsurface Platform and System Status
FJ13.5	LAND STATUS	Land Platform and System Status
FJ14.0	PARAM INFO	Parametric Information
FJ14.2	EW CONTROL	EW Control/Coordination
FJ15.0	THREAT	Threat Warning
FJ28.2 (0)	TEXT	Text Message

Figure 2D.2-1 F-Series Tactical Messages/Words

2D.3 Tactical Message Hierarchy

Table II-1-2 of [STANAG 5522] provides a hierarchical list of Link 22 tactical messages arranged by functional group, sub-functions, and tactical message words.

The following paragraphs provide a definition of each functional group followed by a table divided into sub-functions listing the corresponding Link 22 tactical message words included in the functional area.

2D.3.1 Participant Location & Identification (PLI)

The PLI functional group provides messages to report up-to-date network participation status, identification, and location. The PLI functional group consists of the following sub-functions.

- Indirect PLI
- Air PLI
- Surface PLI
- Subsurface PLI
- Land Point PLI
- Land Track PLI

The Indirect PLI message is used by forwarding NILE units to transmit PLI information about Link 11 and Link 11B units. All the other PLI messages are used by the specific unit type to transmit the PLI information about itself. The messages/words used by these PLI sub-functions are listed in [Figure 2D.3-1](#).

Sub-function	Message/Word number	Message/Word Title
Indirect PLI	F1-0 F02.0-0 F02.0-1	Indirect PLI Position Indirect PLI Amplification Indirect PLI Amplification Continuation
Air PLI	F1-1 F02.2-0 F02.2-1 F02.1-0	PLI Position Air PLI Course and Speed Air PLI Additional Mission Composition PLI IFF
Surface PLI	F1-1 F02.3-0 F02.1-0	PLI Position Surface PLI Course and Speed PLI IFF
Subsurface PLI	F1-1 F02.4-0 F02.4-1 F02.1-0	PLI Position Subsurface PLI Course and Speed Subsurface PLI Mission Correlator PLI IFF
Land Point PLI	F1-1 F02.5-0 F02.1-0	PLI Position Land Point PLI Continuation PLI IFF
Land Track PLI	F1-1 F02.6-0 F02.6-1 F02.1-0	PLI Position Land Track PLI Course and Speed Land Track PLI Mission Correlator PLI IFF

Figure 2D.3-1 PLI Tactical Messages

2D.3.2 Surveillance

The Surveillance functional group consists of the detecting, tracking, identifying, and reporting of space, air, surface, land, reference point, and subsurface environment tracks. Included in the Surveillance functional group is the computation and reporting of track position, position quality (track quality), course, and speed. The Surveillance functional group is broken into the following sub-functions.

- Point Surveillance
- Air Surveillance
- Surface (Maritime) Surveillance
- Subsurface (Maritime) Surveillance
- Land (Ground)/Point/Track Surveillance
- Anti-Submarine Warfare (ASW) Bearing/Contact Surveillance
- Space Track Surveillance
- Electronic Warfare (EW) Product Surveillance
- Surveillance (General)

Point Surveillance consists of reference point, line, area, and emergency point data. Lines and areas are considered as reference points. ASW Bearing/Contact Surveillance provides Acoustic Bearing/Range information and ASW contact amplifying information on subsurface tracks. Space Track Surveillance provides support for Ballistic Missile Defense. Space Track Surveillance Messages express missile track data in the form of a position and velocity vector of magnitude and direction that completely describes the ballistic missile's location, rate of change of location, and time. EW Product Surveillance provides bearings, fixes, and areas of probability. Surveillance (General) provides alphanumeric free text messages. The messages/words used by these Surveillance sub-functions are listed in [Figure 2D.3-2](#).

Sub-function	Message/Word Number	Message/Word Title
Point Surveillance	FJ3.0I FJ3.0E0 FJ3.0C1 FJ3.0C2 FJ3.0C3 FJ3.0C4 FJ3.0C5 FJ3.1I FJ3.1E0 FJ3.1C1	Reference Pt/Line/Area Initial Reference Point/Line/Area Extension Reference Point /Line/Area Continuation 1 Reference Point /Line/Area Continuation 2 Reference Point /Line/Area Continuation 3 Reference Point /Line/Area Continuation 4 Reference Point /Line/Area Continuation 5 Emergency Point Initial Emergency Point Extension Disused
Air Surveillance	F2 F5-0 F01.0-0	Air Track Position Air Track Course and Speed IFF
Surface Surveillance	F3 F5-1 F01.0-0 F01.0-1	Surface Track Position Surface Track Course and Speed IFF Surface Track SAM/SSM
Subsurface Surveillance	F4-0 F4-1 F01.0-0	Subsurface Track Position Subsurface Track Course and Speed IFF
Land (Ground) Point/Track Surveillance	FJ3.5I FJ3.5E0 FJ3.5C1 FJ3.5C3	Land (Ground) Point/Track Initial Land (Ground) Point/Track Extension Land (Ground) Point/Track Continuation 1 Land (Ground) Point/Track Continuation 3
ASW	F01.4-0 F01.4-1 F01.5-0 F01.5-1 F01.5-2 F01.5-3 F03.4-0 F03.4-1	Acoustic Bearing/Range Resolved Acoustic Bearing/Range Ambiguous Acoustic Bearing/Range Amplification Acoustic Bearing/Range Sensor Acoustic Bearing/Range Frequency Acoustic Bearing/Range Amplification 1 ASW Contact Information ASW Contact Confirmation
Space Track	FJ3.6I FJ3.6E0 FJ3.6E1	Space Track Initial Space Track Extension 0 Space Track Extension 1

Sub-function	Message/Word Number	Message/Word Title
	FJ3.6C1	Space Track Continuation 1
	FJ3.6C2	Space Track Continuation 2
	FJ3.6C3	Space Track Continuation 3
	FJ3.6C4	Space Track Continuation 4
	FJ3.6C5	Space Track Continuation 5
	FJ3.6C6	Space Track Continuation 6
Electronic Warfare Product	FJ3.7I	EW Product Information Initial
	FJ3.7C1	EW Product Information Continuation 1
	FJ3.7C2	EW Product Information Continuation 2
	FJ3.7C3	EW Product Information Continuation 3
	FJ3.7C4	EW Product Information Continuation 4
	FJ3.7C5	EW Product Information Continuation 5
Surveillance (General)	FJ28.2(0)I	Text Initial
	FJ28.2(0)E0	Text Extension

Figure 2D.3-2 Surveillance Tactical Messages

2D.3.3 *Electronic Warfare (EW)*

The EW functional group provides for the amplification of surveillance information and the dissemination of tactical intelligence. The EW functional group is broken into the following sub-functions.

- EW Parametric Reporting
- EW Control and Coordination

EW Parametric Reporting messages contain EW information on bearings, fixes, areas of probability, parametric and product data on detected electronic emission sources. EW Control and Coordination messages are used to coordinate and direct electronic warfare activities among NUs and EW operators. The messages/words used by these EW sub-functions are listed in [Figure 2D.3-3](#).

Sub-function	Message/Word Number	Message/Word Title
Electronic Warfare Parametric Reporting	FJ14.0I	Parametric Information Initial
	FJ14.0E0	Parametric Information Extension
	FJ14.0C1	Parametric Information Continuation 1
	FJ14.0C2	Parametric Information Continuation 2
	FJ14.0C3	Parametric Information Continuation 3
	FJ14.0C4	Parametric Information Continuation 4
	FJ14.0C5	Parametric Information Continuation 5
Electronic Warfare Control and Coordination	FJ14.0C6	Parametric Information Continuation 6
	FJ14.2I	EW Control/Coordination Initial
	FJ14.2E0	EW Control/Coordination Extension
	FJ14.2C1	EW Control/Coordination Continuation 1
	FJ14.2C2	EW Control/Coordination Continuation 2
	FJ14.2C3	EW Control/Coordination Continuation 3
	FJ14.2C4	EW Control/Coordination Continuation 4
	FJ14.2C5	EW Control/Coordination Continuation 5
	FJ14.2C6	EW Control/Coordination Continuation 6
	FJ14.2C7	EW Control/Coordination Continuation 7
	FJ14.2C8	EW Control/Coordination Continuation 8

Figure 2D.3-3 *Electronic Warfare Tactical Messages*

2D.3.4 Amplification Data

The Amplification Data functional group provides for the dissemination of tactical Amplification Data. The messages/words used by this function are listed in [Figure 2D.3-4](#).

Function	Message/Word Number	Message/Word Title
Amplification Data	FJ6.0I	Track/Point Amplification Initial
	FJ6.0E0	Track/Point Amplification Extension
	FJ6.0C1	Track/Point Amplification Continuation

Figure 2D.3-4 Amplification Data Tactical Messages

2D.3.5 Threat Warning

The Threat Warning functional group messages are used to transmit the warning of an immediate threat to another unit or units. The Threat Warning tactical message is originated by any NU having knowledge of a threat to either an NU or another friendly track/point and is independent of track reporting and reporting responsibility. The messages/words used by this function are listed in [Figure 2D.3-5](#).

Function	Message/Word Number	Message/Word Title
Threat Warning	FJ15.0I	Threat Warning Initial
	FJ15.0E0	Threat Warning Extension
	FJ15.0C1	Threat Warning Continuation 1

Figure 2D.3-5 Threat Warning Tactical Messages

2D.3.6 Information Management

The Information Management functional group consists of the procedures and information exchange required to ensure that the platform/systems can properly exchange information when operationally interfaced. These procedures are accomplished through the use of Information Management messages. These messages are provided to clarify, correct, and control the flow of data when necessary. The messages/words used by this function are listed in [Figure 2D.3-6](#).

Function	Message/Word Number	Message/Word Title
Information Management	FJ7.0I	Track Management Initial
	FJ7.0C1	Track Management Continuation 1
	FJ7.1I	Data Update Request Initial
	FJ7.1C1	Data Update Request Continuation 1
	FJ7.2I	Correlation
	FJ7.3I	Pointer Initial
	FJ7.3C1	Pointer Continuation 1
	FJ7.3C2	Pointer Continuation 2
	FJ7.3C3	Pointer Continuation 3
	FJ7.4I	Track Identifier Initial
	FJ7.4E0	Track Identifier Extension
	FJ7.5I	IFF/SIF Management Initial
	FJ7.6I	Filter Management Initial
	FJ7.6E0	Filter Management Extension
	FJ7.6C1	Filter Management Continuation 1
	FJ7.6C2	Filter Management Continuation 2
	FJ7.6C3	Filter Management Continuation 3
	FJ7.7I	Association Initial
	FJ8.1I	Mission Correlator Change Message Initial

Figure 2D.3-6 Information Management Tactical Messages

2D.3.7 Weapons Coordination and Management

Weapons coordination and management functional group consists of the exchange of commands and status information necessary to effect optimum employment for all weapons and to prevent mutual interference during tactical operations. The messages/words used by this function are listed in [Figure 2D.3-7](#).

Function	Message/Word Number	Message/Word Title
Weapons Coordination And Management	F01.6-0	Basic Command
	F01.6-1	Command Extension
	F01.6-2	Air Coordination
	F01.7-0	Response
	FJ9.1	Engagement Coordination
	FJ10.2I	Engagement Status Initial
	FJ10.2C1	Engagement Status Continuation 1
	FJ10.2C2	Engagement Status Continuation 2
	FJ10.3I	Handover Initial
	FJ10.3E0	Handover Extension
	FJ10.3C1	Handover Continuation 1
	FJ10.3C2	Handover Continuation 2
	FJ10.5I	Controlling Unit Report Initial
	FJ10.6I	Pairing Initial
	FJ12.4I	Controlling Unit Change Initial
	FJ12.4E0	Controlling Unit Change Extension

Figure 2D.3-7 Weapons Coordination and Management Tactical Messages

2D.3.8 Status

The Status functional group is used by NUs to report the status of the following platform types.

- Airfields
- Air Platforms
- Surface Platforms
- Subsurface Platforms
- Land Platforms

An Airfield can report its operational status and the status of its runways, airfield facilities, and aircraft carrier flight decks. An Air Platform can report its current status of fuel, ordnance status, operational status, and on board systems' status. A Surface Platform can report its current ordnance load, operational status and on board systems' status. A Subsurface Platform can report its current operational status and on board systems' status. A Land Platform can report its current operational weapons and equipment status. The messages/words used by this function are listed in Figure 2D.3-8.

Function	Message/Word Number	Title
Status	FJ13.0I	Airfield Status Initial
	FJ13.0E0	Airfield Status Extension
	FJ13.0C1	Airfield Status Continuation 1
	FJ13.0C2	Airfield Status Continuation 2
	FJ13.2I	Air Platform and System Status Initial
	FJ13.2C1	Air Platform and System Status C1
	FJ13.2C2	Air Platform and System Status C2
	FJ13.2C3	Air Platform and System Status C3
	FJ13.2C4	Air Platform and System Status C4
	FJ13.2C5	Air Platform and System Status C5
	FJ13.2C6	Air Platform and System Status C6
	FJ13.2C7	Air Platform and System Status C7
	FJ13.3I	Surface Platform and System Status Initial
	FJ13.3C1	Surface Platform and System Status Cont. 1
	FJ13.3C2	Surface Platform and System Status Cont. 2
	FJ13.3C3	Surface Platform and System Status Cont. 3
	FJ13.3C5	Surface Platform and System Status Cont. 5
	FJ13.3C6	Surface Platform and System Status Cont. 6
	FJ13.3C7	Surface Platform and System Status Cont. 7
	FJ13.4I	Subsurface Platform and System Status Initial
	FJ13.4C1	Subsurface Platform and System Status C1
	FJ13.4C2	Subsurface Platform and System Status C2
	FJ13.5I	Land Platform and System Status Initial
	FJ13.5C1	Land Platform and System Status Cont. 1

Figure 2D.3-8 Status Tactical Messages

2D.4 Message Sequence

Link 22 tactical messages are composed of one or more Tactical Message Words (TMWs). A Link 22 tactical message is also known as a Link 22 message sequence. Generally, when the TMW contains the Track Number Reference or the Track Number Source, the message sequence containing the TMW may consist of just the TMW. [STANAG 5522] lists the correct message sequences at the end of each sub-function section of Annex B.

Link 22 “FJ” message sequences are the same as those used by the corresponding J-Series messages. An example of a Link 22 “FJ” message sequence is discussed in section 2D.6.1 FJ Message Sequence.

An example of a Link 22 “F” message sequence is shown in section 2D.6.2 F Message Sequence, along with the comparison of the same track being transmitted on Link 16.

2D.5 TMW Construction

All Link 22 word titles are identified by the initial "F". The Least Significant Bit (LSB) (bit 0) of each word contains the Series Indicator (SER IND) that indicates whether the word is a Unique F-Series word (SER IND = 0), or some other non-unique F-Series format (SER IND = 1). When the Series Indicator is 1, the Packed Message Indicator (PMI) in the next bit (bit 1) indicates whether the word is a Packed J-Series word (PMI = 0), or some other format (PMI=1). Packed J-Series word titles have the letter “J” following the “F” (FJ). Figure 2D.5-1 depicts the structure of the beginning of a Link 22 tactical message word.

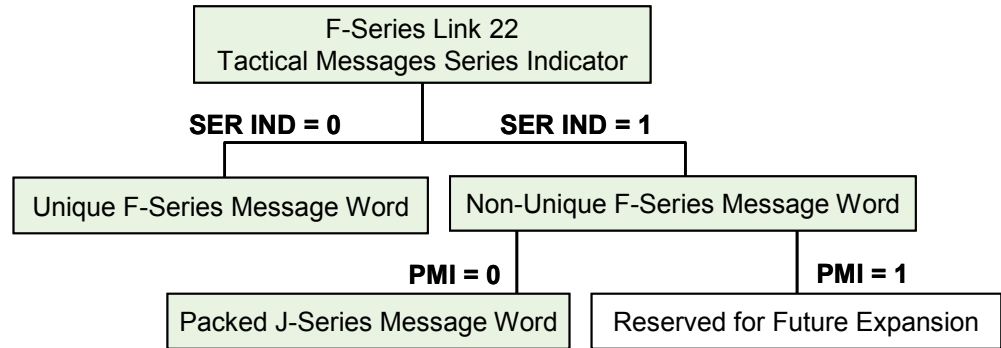


Figure 2D.5-1 Link 22 Tactical Message Structure

2D.5.1 Unique F-Series Message Words

The digit following the "F" in the title of a Unique F-Series message word is the Label Indicator. There are three different structures of the Unique F-Series message words which are as follows.

- Label Indicator field is zero
- Label Indicator non-zero and single word message
- Label Indicator non-zero and multiple word message

□ Label Indicator field is zero

When the Label Indicator field is zero, it is followed by the fields that are listed below.

- F-Series Label
- A period
- F-Series Sub-label
- A Hyphen
- Word Number field (starts at 0)

When it appears in written representation it is as shown in [Figure 2D.5-2](#).

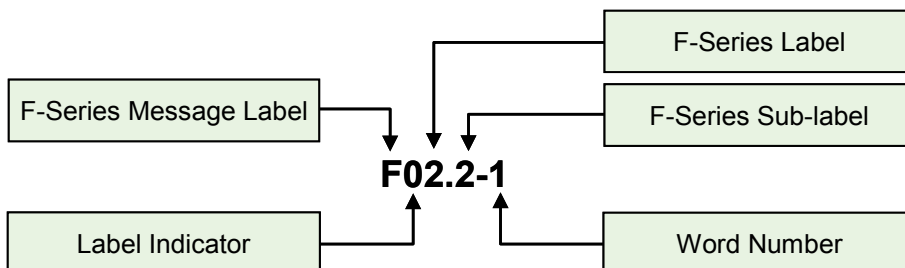


Figure 2D.5-2 Message with Label Indicator of Zero

The bit layout of these message words is shown in [Figure 2D.5-3](#). The Word Number field varies in length (1-3) depending on how many different message words are present in the message. The example in [Figure 2D.5-3](#) has a 2-bit Word Number field (message has 3 or 4 words).

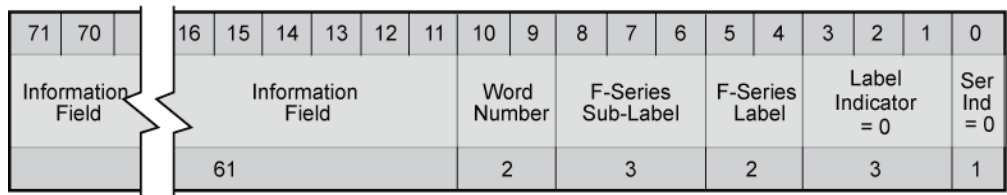


Figure 2D.5-3 Bit Layout of Message with Label Indicator of Zero

□ **Label Indicator non-zero and single word message**

When the Label Indicator field is greater than zero and the message is a single word, the F-Series Label, the F-Series Sub-label and the Word Number fields are not present. This gives a simple structure e.g. “F2”, as shown in Figure 2D.5-4.

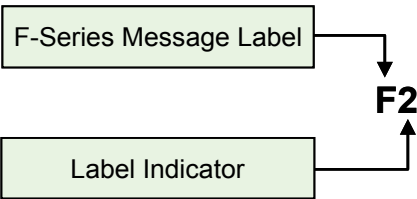


Figure 2D.5-4 Single Word Message (Label Indicator>0)

The bit layout of the word is shown in Figure 2D.5-5.

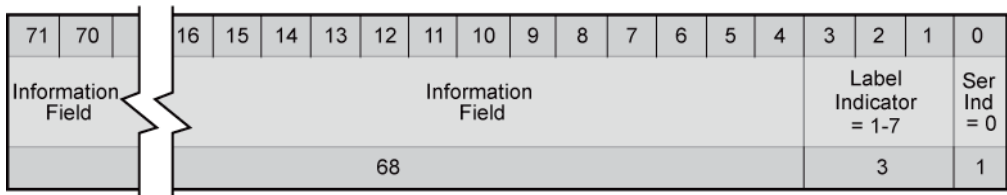


Figure 2D.5-5 Bit Layout of Single Word Message (Label Indicator>0)

□ **Label Indicator non-zero and multiple word message**

When the Label Indicator field is greater than zero and the message has multiple words, the F-Series Label and the F-Series Sub-label fields are not present. This gives the structure e.g. F1-1 as shown in Figure 2D.5-6.

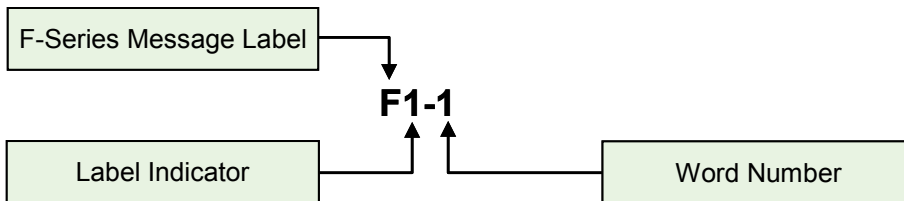


Figure 2D.5-6 Multiple Word Message (Label Indicator>1)

The bit layout of these message words is shown in Figure 2D.5-7. The Word Number field varies in length (1-3) depending on how many different message words are present in the message. The example in Figure 2D.5-7 has a 1-bit Word Number field (message has 2 words).

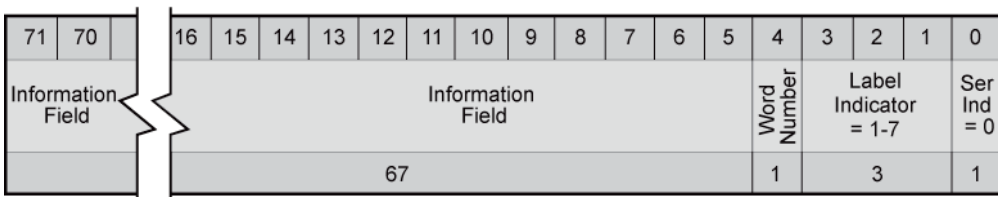


Figure 2D.5-7 Bit Layout of Multiple Word Message (Label Indicator>1)

2D.5.2 Packed J-Series Message Words

Packed J-Series messages are indicated by a “J” following the “F”. The “FJ” is followed by the J-Series Label and Sub-Label numbers. A J-Series Label is a 5-bit field that can contain the values 0-31. The Sub-Label field is a 3-bit field that can contain the values 0-7. This gives the message number. The individual words of the message are indicated by additional characters. The next character indicates the 2-bit Word Format field of the word, which indicates one of the following.

- Initial Word (I)
- Extension Words (E)
- Continuation Words (C)
- Variable Format – (Not currently used by Link 22)

□ Initial Word

The numbering convention for the initial word of an FJ message is to append the character “I” to the end (e.g. FJ3.6I Space Track Initial Word).

The message length indicator 3-bit field in the initial word indicates the number (0-7) of extension plus continuation words that follow the initial word. The initial word has the bit layout as shown in [Figure 2D.5-8](#).

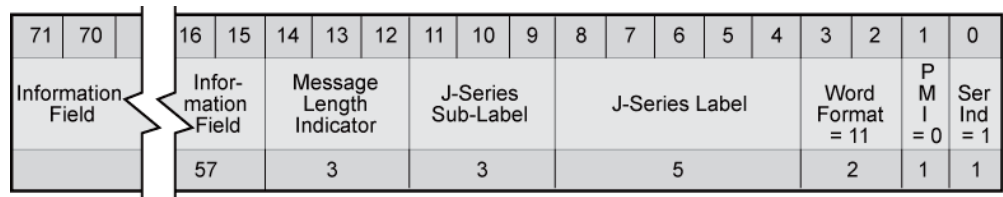


Figure 2D.5-8 Bit Layout of FJ Message Initial Word

□ Extension Words

The numbering convention for the extension words of an FJ message is to append the character “E”, followed by the extension word number (starting at zero) to the end (e.g. FJ3.6E1 Space Track second Extension Word).

Extension Words are defined for an initial word when the length of the data field grouping logically transmitted as an entity exceeds the space available in the initial word. They are defined and interpreted solely with respect to the J-Series Label and J-Series Sub-label combination for an initial word. They are required to be transmitted in serial order. The extension word has the bit layout as shown in [Figure 2D.5-9](#).

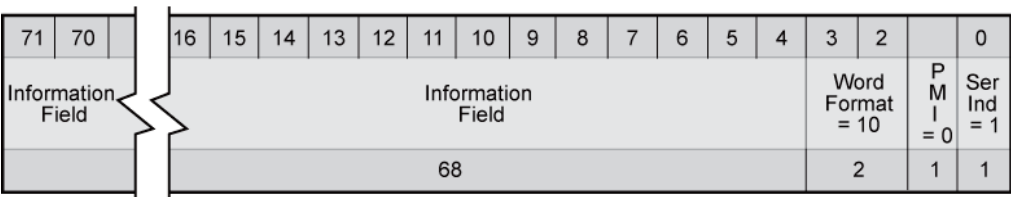


Figure 2D.5-9 Bit Layout of FJ Message Extension Word

□ **Continuation Words**

The numbering convention for the continuation words of an FJ message is to append the character “C”, followed by the continuation word number (starting at one) to the end (e.g. FJ3.6C4 Space Track fourth Continuation Word).

Continuation Words provide additional amplifying information in support of the initial word and extension words. They are transmitted after the last extension word, or immediately after the initial word if no extension words are transmitted. They can be sent in any order unless otherwise specified in individual message transmission rules. The Continuation word has the bit layout as shown in [Figure 2D.5-10](#).

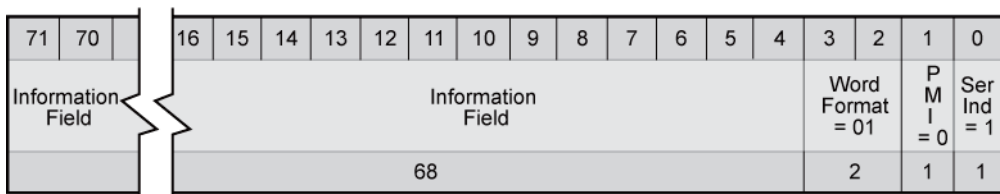


Figure 2D.5-10 Bit Layout of FJ Message Continuation Word

2D.6 Message Sequence Examples

A tactical message sequence is composed of one or more Tactical Message Words (TMWs). The F-Series messages are composed of two distinct groups, the “FJ” and the “F” tactical messages. This section gives an example of a message sequence for each group, and also compares the F message sequence with the corresponding Link 16 J-Series message sequence.

2D.6.1 FJ Message Sequence

In general, each FJ tactical message Initial word and any Extension words are transmitted together at the earliest transmit opportunity. Additionally, any FJ Continuation words that contain attributes that have changed will be transmitted together with the Initial word and the Extension words at the earliest transmit opportunity.

When a FJ message varies from the general case, the FJ message sequences will correspond to those used by J-Series message sequences.

Figure 2D.6-1 illustrates the FJ-Series message sequence of a space track with full covariance.

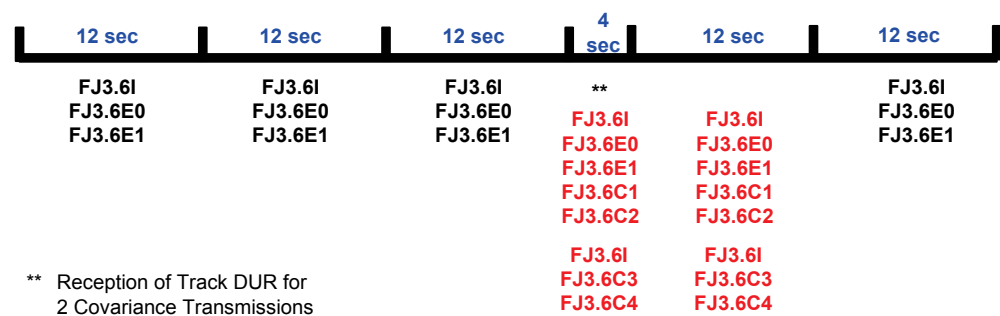


Figure 2D.6-1 Space Track FJ-Series Message Sequence

In this sequence, the space track has its non-covariance data reported every 12 seconds. Upon receipt and processing of a space track Data Update Request (DUR) message, Continuation words are immediately transmitted along with the Initial word and the Extension words. Note that two transmission sequences are output to fulfill the data update request. Upon fulfilling the data update requested transmission cycle (two in this example), the space track will return to its non-covariance data transmission sequence.

2D.6.2 F Message Sequence

Figure 2D.6-2 illustrates the F-Series message sequence of a friendly general air track with no IFF, platform, or specific type attributes.

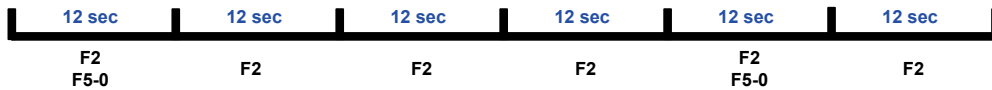


Figure 2D.6-2 Air Track F-Series Message Sequence

Every 12 seconds, a single 72-bit F2 tactical message word must be transmitted in order to communicate the core attributes of Track Number Reference, Identity, and position (Latitude & Longitude). Every fourth transmission opportunity, an additional F5-0 tactical message word is also transmitted unless an attribute contained within the F5-0 changes. If an attribute within the F5-0 changes, both the F2 and F5-0 will be transmitted together.

To highlight the savings in bandwidth of the F-Series with respect to the J-Series, the same transmission of a friendly general air track with no IFF, platform, or specific type attributes performed on Link 16 is shown in Figure 2D.6-3.

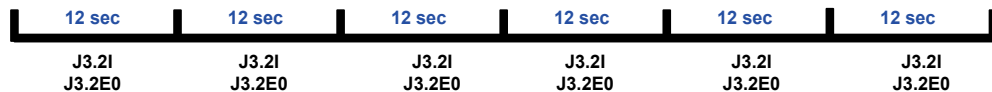


Figure 2D.6-3 Air Track J-Series Message Sequence

Link 16 transmits two 70-bit words every 12 seconds. The J3.2E0 must be transmitted along with the J3.2I in order to communicate the track's core attributes of Identity, Position (Latitude & Longitude), and Track Number Reference. This is because some of the core attributes are in the second word as highlighted in the word contents comparison in Figure 2D.6-4, where the core attributes are in red.

It can be seen from Figure 2D.6-2 that in a 48 second period Link 22 needs 5 TMWs = $5 * 72 = 360$ bits and from Figure 2D.6-3 that Link 16 needs 8 TMWs = $8 * 70 = 560$ bits. Therefore, Link 22 needs 200 fewer bits which is a savings of more than 35%.

F2	J3.2I
Emergency Indicator	Altitude Source
Exercise Indicator	Altitude, 25 Ft
Force Tell Indicator	Emergency Indicator
Identity	Exercise Indicator
Latitude	Force Tell Indicator
Longitude	Identity
Simulation Indicator	Identity Confidence
Track Number, Reference	Identity Difference Indicator
Track Quality	PPLI Track Number and Identity Indicator
F5-0	Simulation Indicator
Air Platform	Special Interest Indicator
Air Platform Activity	Special Processing Indicator
Altitude, 25 Ft	Strength
Altitude Source	Track Number, Reference
Identity Confidence	Track Quality
Passive/Active Indicator	J3.2E0
Slow Update Rate Indicator	Course
Special Interest Indicator	Latitude, 0.0051 Minute
Strength	Longitude, 0.0051 Minute
	Passive/Active Indicator
	Speed

Figure 2D.6-4 F-Series & J-Series Air Track Message Sequence Fields

2D.7 Link 22 Message Description

The Link 22 tactical messages are defined in [STANAG 5522]. This section lists the information that is provided by the STANAG for each tactical message, and shows an example extracted from the STANAG.

For each tactical message the STANAG contains the following information.

- Message Summary (see [Figure 2D.7-1](#))
 - Purpose
 - List of Data elements, including bit length of each element
- Word Presentation
 - Word Map - shows the field construction for each word (see [Figure 2D.7-2](#))
 - Word Description for each data element within the word (see [Figure 2D.7-3](#))
 - ◆ Data Field Identifier (DFI)/Data Use Identifier (DUI) reference number
 - ◆ Field descriptor, if applicable
 - ◆ Bit positions of the data element within the word
 - ◆ Length of the data element in bits
 - ◆ Any applicable resolution or coding
 - Field Coding - defines each value of each data element (see [Figure 2D.7-4](#))
- Transmission/Reception Rules
 - Transmission Rules (see [Figure 2D.7-5](#))
 - Reception Rules (see [Figure 2D.7-6](#))
 - Prioritization (see [Figure 2D.7-7](#))

The Message Summary section in the STANAG consists of the message purpose and a summary list of the Data Elements. [Figure 2D.7-1](#) is an example of a message summary from the STANAG.

SURFACE TRACK POSITION MESSAGE SUMMARY		
Purpose: The Surface Track message is used to exchange information on Surface Tracks.		
Data Element Summary		
F3	DATA ELEMENTS	# BITS
	SERIES INDICATOR	1
	LABEL INDICATOR	3
	TRACK NUMBER, REFERENCE	19
	LAT/LONG SCALE INDICATOR	1
	LATITUDE, 0.0103 MINUTE LSB (18)	37
	LONGITUDE, 0.0103 MINUTE LSB (19)	
	LATITUDE, 0.0412 MINUTE (18)	
	LONGITUDE, 0.0412 MINUTE (19)	
	TRACK QUALITY	4
	IDENTITY (3)	3
	IDENTITY AMPLIFYING DESCRIPTOR (3)	
	EXERCISE INDICATOR	1
	FORCE TELL INDICATOR	1
	EMERGENCY INDICATOR	1
	SIMULATION INDICATOR	1
F5-1	DATA ELEMENTS	# BITS
	SERIES INDICATOR	1
	LABEL INDICATOR	3
	WORD NUMBER, 1	1
	COURSE	9
	SPEED (SURFACE/LAND)	9
	SURFACE (MARITIME) PLATFORM	6
	SURFACE (MARITIME) PLATFORM ACTIVITY	7
	SURFACE (MARITIME) SPECIFIC TYPE	12
	MINUTE	6
	HOUR	5
	DISUSED	4
	STRENGTH	4
	SPECIAL INTEREST INDICATOR	1
F5-1 (Continued)		# BITS
	PASSIVE/ACTIVE INDICATOR	1
	IDENTITY DIFFERENCE INDICATOR	1
	PLI TN/ID INDICATOR	1
	SPECIAL PROCESSING INDICATOR	1
F01.0-0	DATA ELEMENTS	# BITS
	SERIES INDICATOR	1
	LABEL INDICATOR	3
	LABEL, F-Series	2
	SUBLABEL, F-Series	3
	WORD NUMBER, 2	2
	TRACK NUMBER, REFERENCE	19
	MODE I CODE	5
	MODE II CODE	12
	MODE III CODE	12
	MODE IV INDICATOR	2
	PLI IFF/SIF INDICATOR	2
	SPARE	9
F01.0-1	DATA ELEMENTS	# BITS
	SERIES INDICATOR	1
	LABEL INDICATOR	3
	LABEL, F-Series	2
	SUBLABEL, F-Series	3
	WORD NUMBER, 2	2
	SAM/SSM TYPE, 1	9
	SAM/SSM TYPE, 2	9
	SAM/SSM TYPE, 3	9
	SPARE	34

Figure 2D.7-1 STANAG 5522 Message Summary Example

The Word Map section in the STANAG shows the field construction of the tactical message word. [Figure 2D.7-2](#) is an example of a Word Map from the STANAG.

<u>WORD MAP</u>																												
WORD NUMBER: F3																												
WORD TITLE: SURFACE TRACK POSITION																												
23	22	21	20	19	18	17	16	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00					
LLS Ind	Track Number Reference																			Label Indicator			Ser Ind =0					
1	19																			3			1					
47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24					
						Latitude, 0.0103 Minute LSB																						
						Latitude, 0.0421 Minute																						
37																												
71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48					
SIM Ind	EMG Ind	FT Ind	EX Ind	Identity		Track Quality					Longitude, 0.0103 Minute LSB																	
				Identity Amplifying Descriptor							Longitude, 0.0412 Minute																	
1	1	1	1	3		4																						

Figure 2D.7-2 STANAG 5522 Word Map Example

The Word Description section in the STANAG describes the fields of the tactical message word. [Figure 2D.7-3](#) is an example of a Word Description from the STANAG.

WORD DESCRIPTION				
WORD NUMBER:		F3		
MESSAGE TITLE:		SURFACE TRACK POSITION		
REFERENCE	BIT	#	CODING,	
DFI/DUI	DATA FIELD DESCRIPTOR	POSITION	BITS	RESOLUTION, ETC.
1560 001	SERIES INDICATOR (SER IND)	0	1	0
270 008	LABEL INDICATOR	1- 3	3	011
769 002	TRACK NUMBER, REFERENCE	4- 22	19	
1565 002	LAT/LONG SCALE INDICATOR LLS IND)	23	1	
281 018	LATITUDE, 0.0103 MINUTE LSB	24- 41	18	
282 016	LONGITUDE, 0.0103 MINUTE LSB	42- 60	19	
281 016	LATITUDE, 0.0412 MINUTE	24- 41	18	
282 012	LONGITUDE, 0.0412 MINUTE	42- 60	19	
280 001	TRACK QUALITY	61- 64	4	
376 007	IDENTITY	65- 67	3	
376 001	IDENTITY AMPLIFYING DESCRIPTOR (ID AMP DESCR)	65- 67	3	
385 003	EXERCISE INDICATOR (EX IND)	68	1	
354 002	FORCE TELL INDICATOR (FT IND)	69	1	
355 002	EMERGENCY INDICATOR (EMG IND)	70	1	
1604 001	SIMULATION INDICATOR (SIM IND)	71	1	

Figure 2D.7-3 STANAG 5522 Word Description Example

The Field Coding section in the STANAG explains the coding and usage of each of the fields of the tactical message word. The example in [Figure 2D.7-4](#) is part of a Field Coding section from the STANAG.

FIELD CODING FOR F3 (SHEET 4)				
DFI	DUI	DUI/DI NAME	DI BIT CODE	DUI/DI EXPLANATION
769	002	<u>TRACK NUMBER REFERENCE</u>	(CONTINUED)	
		70000-77776	114688 THROUGH 118782	BE USED FOR TACTICAL INFORMATION REPORTING, E.G., TRACKS AND REFERENCE POINTS. ASSIGNED AS IDENTIFICATION NUMBERS FOR JUS AND ALLOCATED IN BLOCKS TO C2 JUS TO BE USED FOR TACTICAL INFORMATION REPORTING, E.G., TRACKS AND REFERENCE POINTS.
		77777	118783	ASSIGNED AS THE NETWORK MANAGER DEDICATED ADDRESS.
		7A000-ZZ777	118784 THROUGH 524287	ALLOCATED IN BLOCKS TO C2 JUS TO BE USED FOR TACTICAL INFORMATION REPORTING, E.G., TRACKS AND REFERENCE POINTS.
1565	002	<u>LAT/LONG SCALE INDICATOR</u>		INDICATES WHICH OF THE LAT/LONG FIELD DUIS IS TO BE USED.
		USE DFI/DUI 281 018 FOR LATITUDE AND DFI/DUI 282 016 FOR LONGITUDE	0	
		USE DFI/DUI 281 016 FOR LATITUDE AND DFI/DUI 282 012 FOR LONGITUDE	1	

Figure 2D.7-4 STANAG 5522 Field Coding Example

The STANAG defines all applicable transmission rules for each tactical message, which identify the need for transmission and the quality of service associated with each transmission. The example in [Figure 2D.7-5](#) is part of a Transmission Rules section from the STANAG.

“SURFACE TRACK POSITION TRANSMISSION/ RECEPTION RULES

PART 1 -- TRANSMISSION RULES

1.1 MESSAGE APPLICABILITY

The Surface Track message is applicable to real-time and non real-time surface tracks. Each transmission of one or more words of a message will be referred to in this document as a "report." Reports shall be queued for transmission in accordance with the priorities addressed in Part 3. The Surface Track message consists of four 72-bit words as follows:

- a. The F3 Surface Track Position Word, abbreviated "SUR POS".
- b. The F5-1 Surface Track Course and Speed Word, abbreviated "SUR CAS".
- c. The F01.0-0 IFF Word, abbreviated "IFF".
- d. The F01.0-1 Surface Track SAM/SSM Word, abbreviated "STMIS".
- e. When the SUR POS and SUR CAS words are transmitted together as a pair, the combination is called the Basic Bi-Word. In this case, the SUR POS word shall immediately precede transmission of the SUR CAS word. The IFF word contains Reference TN and may be transmitted independently from the SUR POS word.

1.2 INITIAL DETECTION REPORT

The NU that detects a surface track shall transmit the appropriate words of this message in ...”

Figure 2D.7-5 STANAG 5522 Transmission Rules Example

The STANAG defines all applicable reception rules for each tactical message, which are the actions required upon reception of a message. The example in [Figure 2D.7-6](#) is part of a Reception Rules section from the STANAG.

PART 2 -- RECEPTION RULES

The initial report concerning Reference TN will be received with the LLS IND set to value 1 and the position of Reference TN reported with LSBs in the Latitude and Longitude fields equal to 0.0412 minute. NUs shall retain the MSBs in this report in their database since the following nine periodic updates will be received with the LLS IND set to value 0 and the LSBs in the Latitude and Longitude fields equal to 0.0103 minute. If an NU receives a track report with the LLS IND set to value 0 and no prior report has been received with LLS IND set to value 1, the NU shall discard the message and transmit an FJ7.1 Data Update Request message for Reference TN.

Figure 2D.7-6 STANAG 5522 Reception Rules Example

The Prioritization section in the STANAG defines the priority assigned when transmitting a tactical message. The example in [Figure 2D.7-7](#) is part of a Prioritization section from the STANAG.

PART 3 -- PRIORITIZATION				
Surface Track reports shall be queued for transmission with the priorities specified in Table II-4-7.				
SER	OCCASION	WORDS TX	TX	PRI
1	INITIAL SURFACE TRACK HOSTILE/FAKER REPORT OR CHANGE OF ID TO/FROM HOSTILE FAKER	SUR POS, SUR CAS, IFF(D/F), STMIS(D)	1/AO	1/EPI
2	INITIAL SURFACE TRACK REPORT FOR NON-HOSTILE IDS; NEXT REPORT AFTER FORCE TELL OR EMERGENCY INDICATOR IS SET TO VALUE 1; REPORT IN RESPONSE TO DUR BY TN; ALL NONPERIODIC NRT HOSTILE/FAKER REPORTS, INCLUDING CHANGE TO/FROM HOSTILE/FAKER ID	SUR POS, SUR CAS, IFF(D/F), STMIS(D)	1/AO	2
3	LATE OR HUR PERIODIC REPORT OF HOSTILE/FAKER; LATE HUR PERIODIC REPORT OF NON-HOSTILE TRACK; EXCESSIVELY LATE PERIODIC REPORT OF NON-HOSTILE TRACK	SUR POS, SUR CAS(4), IFF(D/F), STMIS(D)	1/AO	2
4	REPORT OF ID CHANGE BUT NOT TO/FROM HOSTILE/FAKER	SUR POS, SUR CAS(P), STMIS(D)	1/AO	3
5	REPORT CHANGE IN IFF DATA, RESPONSE TO IFF DUR, OR RESOLUTION OF IFF CONFLICT	IFF(F)	1/AO	3
6	CHANGE IN ANY DATA IN THE SUR CAS WORD	SUR POS, SUR CAS	1/AO	3
6a	CHANGE IN ANY DATA IN THE STMIS WORD	SUR POS, SUR CAS (P), STMIS	1/AO	3
7	LATE OR HUR PERIODIC REPORT OF NON-HOSTILE TRACK; NORMAL OR EARLY PERIODIC REPORT OF HOSTILE/FAKER TRACK	SUR POS, SUR CAS(4), STMIS(D)	1/AO	3
8	CHANGE IN R2, ALL NON-PERIODIC REPORTS OF NON-HOSTILE NRT TRACKS	SUR POS, SUR CAS, IFF(D/F), STIMS(D)	1/AO	3
9	LATE PERIODIC IFF REPORT (COUNTER >16)	IFF(D/F)	1/AO	3
10	NORMAL OR EARLY PERIODIC REPORT OF NON-HOSTILE TRACK	SUR POS, SUR CAS(4), STIMS(D)	1/AO	4
11	NORMAL PERIODIC IFF REPORT	IFF(D/F/16)	1/AO	4
12	ALL NRT PERIODIC REPORTS	SUR POS, SUR CAS(4) IFF(D/F/16), STMIS(D)	1/AO	4

Figure 2D.7-7 STANAG 5522 Prioritization Example

2D.8 Message Extrapolation

Link 22 tactical messages that contain a set of position attributes (e.g. latitude and longitude fields) must be extrapolated to the time of transmission. In Link 22, the DLP performs this function. The SNC requests the data for transmission from the DLP specifying the time it is planned to be transmitted. The DLP extrapolates the track position to the specified time and replies to the SNC with the calculated position. This protocol is used to meet one of the main design goals of Link 22, which was that the lower levels of the layered communications system do not modify or need to access the tactical message data.

2D.9 Stacked Fields

A stacked field within a tactical message word is a field where the content depends on the value of an indicator field. This means that an individual message word identified by its message label, (e.g. F5-0) can have more than one usage. Stacked fields are not unique to Link 22, and can be found in most Tactical Data Links (TDLs). The example in [Figure 2D.9-1](#) shows the word map of the F5-0 (Air Track Course and Speed) tactical message word.

23	22	21	20	19	18	17	16	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
Speed										Course										WN 1	Label Indicator	Ser Ind	
11										9										1	3	1	

47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24
Spare			Alt Src		Identity Confidence			Altitude, 25 Ft													ATI	→	
								Spare	Hour					Minute									
3			2		4			13													1		

71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
SPI	PLI Ind	ID DIF	PAS ACT	SI Ind	Strength				SP	Air Specific Type											AST Ind	SLI	
									Air Platform Activity						Air Platform								
1	1	1	1	1	4				13													1	1

Figure 2D.9-1 Word Map showing Stacked Field Usage

The F5-0 TMW contains two independent stacked fields. Their Indicator Fields (highlighted in red) are: Altitude/Time Indicator (ATI) and Air Specific Type Indicator (AST Ind). The first stacked field (highlighted in yellow) contains the Altitude when the ATI field is zero and contains the Hour and Minute fields when the ATI field is one. The second stacked field (highlighted in green) contains the Air Platform and Air Platform Activity fields when the AST Ind field is zero and contains the Air Specific Type field when the AST Ind field is one.



This page is intentionally left blank.

Section E Link 22 in a Multilink Environment

Link 22 was designed to replace Link 11 and to complement, and interoperate easily with Link 16. Link 22 is intended to be deployed both as a single link and as part of a multilink environment. No existing single link can satisfy all the operational requirements, and Multilink capability is required to ensure operational effectiveness.

One of the original goals of Link 22 was to minimize operator load in both planning and operations. In fact, Beyond Line-of-Sight (BLOS) and new automated features such as Relay and Dynamic Reallocation simplify planning and operations, offsetting any added responsibility for Link 22 deployment in both single and Multilink environments.

Link 22 can reduce the load on Link 16, if it is used to segregate the traffic based on operational responsibilities.

Link 22 BLOS can also be used as an alternative to satellite link-based systems, which are vulnerable to service denial or degradation and can be neutralized by forces not in the area of operations.

The replacement of Link 11 by Link 22 in a multilink environment will improve the accuracy and effectiveness of the tactical picture.

In this section the term Interface Unit (IU) is used to refer to any unit with a TDL capability. [Figure 2E-1](#) lists the specific designation of an IU with respect to the different link types.

Specific IU Link Definition	Description
Link 22 – NILE Unit (NU)	Unit communicating directly on Link 22
Link 16 MIDS Unit (JU) C2 (C2 JU)	Unit communicating directly on Link 16 networks with Command and Control (C2) Capability
Link 16 MIDS Unit (JU) NonC2 (NonC2 JU)	Unit communicating directly on Link 16 networks as non C2
Link 11 Participant Unit (PU)	Unit communicating directly on Link 11
Reporting Unit (RU)	Unit communicating directly on Link 11B

Figure 2E-1 IU Link Specific Definitions

Note that Link 16 characterizes units as either C2 or nonC2, while Link 22 does not make this distinction.

The main references for this section are as follow.

- [ADatP-33] that contains Operational capabilities and procedures for all deployed links
- [STANAG 5522] that contains the description of the Tactical messages and protocols of Link 22
- [STANAG 5616 Volume II] that contains the translations and data forwarding rules between Link 22 and Link 16
- [STANAG 5616] that contains the translations and data forwarding rules between Link 22 and Link 11/11B

This section is divided into the following sub-sections, which provide an overview of Multilink terminology and considerations required in planning and operating Link 22 in a multilink environment.

- Multilink Overview provides a quick overview of other links in order to emphasize elements for Planning and Operations and introduces terms used in a multilink environment
- Multilink Considerations which introduces features and functions that are important for Planning and Operations of any link and highlight commonality and differences with Link 16 and Link 11
- Multilink Planning with Link 22 introduces considerations for planning Link 22 in a multilink environment
- Multilink Operations with Link 22 introduces considerations for operations with Link 22 in a multilink environment

2E.1 Multilink Overview

This section provides an overview of links other than Link 22 and multilink terms.

- [Other Links Overview](#)
- [Multilink Terms](#)

2E.1.1 Other Links Overview

The following links are briefly introduced to highlight similarities and differences with Link 22 in order to provide an understanding of their use in the multilink environment.

- [Link 16](#)
- [JREAP](#)
- [Link 11](#)
- [Link 11B](#)
- [NATO Link 1](#)

□ *Link 16*

Link 16 is a frequency-hopping, jam-resistant, high capacity link. It operates on the principle of Time Division Multiple Access (TDMA), wherein 128 timeslots per second are allocated among all JUs for the origination and reception of data. Some Link 16 terminals also support two channels of digitized secure voice communications. The Link 16 timeslots are organized into Network Participation Groups (NPGs). Link 16 is limited to line-of-sight unless a relay platform is active. All Link 16 terminals are capable of relay, which requires consideration during planning to provide dedicated relay slots. Air platforms may be needed for effective coverage when relay is required.

The main purpose of Link 16 is the exchange of the J-Series Tactical data, part of the J-family, as defined in STANAG 5516. Link 16 did not significantly change the basic concepts of tactical data link information exchange supported for many years. Rather, Link 16 enhanced tactical employment of all equipped platforms and provides technical and operational improvements to existing tactical data link capabilities, which include the following.

- 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)

Link 16 utilizes a terminal for transmission that interfaces to the TDS/DLP. Different types of terminals exist which are listed below.

The first generation of Link 16 terminal was the Joint Tactical Information Distribution System (JTIDS).

The Multifunctional Information Distribution System (MIDS) Low-Volume Terminal (LVT) is the second generation of Link 16 terminals. Many variants of this terminal, based on three main variants (LVT-1, LVT-2 and LVT-3) have been produced, each unique in its interface and programming.

The Joint Tactical Radio System (JTRS) and MIDS JTRS will represent the next generation Link 16 capable terminals.

□ **JREAP**

The Joint Range Extension Application Protocols (JREAP) were designed to support BLOS operations and are defined in MIL-STD-3011. There are three protocols currently defined; which are as follows.

- **JREAP A**, which is similar to Satellite TDL-J (S-TDL J), utilizes the same radios and satellites but with a slightly different protocol than S-TDL-J. JREAP A utilizes military (UHF) satellite and terrestrial Radio Frequency (RF) communications that are half-duplex and use token passing techniques. S-TDL J is the original protocol used by the US Navy to communicate J-family messages through a satellite
- **JREAP B** is a full-duplex, point-to-point communications protocol that can use media such as military Super High Frequency (SHF) satellite communications, landlines (telephone lines), or field wire between shelters.

- **JREAP C** utilizes the Internet Protocol (IP) User Datagram Protocol (UDP) in Unicast and Multicast modes, as well as Transmission Control Protocol (TCP) to exchange encapsulated messages over wide and local area networks

These protocols can be adapted to support almost any message set, but the exchange of J-Series messages is currently their most prevalent use. While JREAP uses Link 16 J-family message set, it uses different protocols that make it a unique link implementation.

□ **Link 11**

Link 11 employs netted communication techniques and standard message formats for the exchange of digital information among airborne, land-based, submarine, and shipboard tactical data systems. It provides for the mutual exchange of information among net participants via High Frequency (HF) or Ultra High Frequency (UHF) radio, or via digital satellite communications. Communication of Link 11 messages over satellite are known as Satellite Link 11. Link 11 is normally a half-duplex, netted, secure link that operates in a Roll Call mode among the Participating Units (PUs), under the control of a Net Control Station. In Roll Call the units (also known as pickets) are polled by the Net Control Station, and when polled respond with their Link-11 messages. Link 11 can also be used in Broadcast and Silence mode. Link 11 utilizes M-Series messages, as defined in STANAG 5511.

□ **Link 11B**

Link 11B is a full-duplex, two-way, point-to-point link that provides for the serial transfer of data. Because it is point-to-point, each pair of units operates on a separate channel. Link 11B employs the same message standard as Link 11. However, the equipment, some message protocols, and the data rate are different from those of Link 11.

□ **NATO Link 1**

Link 1 is a NATO link. It operates as a two-way, full-duplex, point-to-point, non-secure digital data link that transfers data between NATO land-based units. Its architecture is very similar to that of Link 11B. It employs unique message standards and protocols and is limited to Air Tracks and a minimal degree of electronic warfare and weapons coordination. ADatP-12 provides details on use and translation to Link 11.

2E.1.2 Multilink Terms

Several functionalities affect planning and operations in a Multilink environment as listed below.

- Basic and Extended Multilink Interface
- Data Forwarding
- Concurrent Operations
- Data Looping and Reception Priority Scheme

□ **Basic and Extended Multilink Interface**

[ADatP-33] defines the Basic Multilink Interface to include Link 11, Link 11B, Link 16 and Link 22, besides data forwarding between all the involved TDLs. All other TDLs interfaces are collectively referred to as the “extended interface”.

Considering the approaching obsolescence of Link 11 and Link 11B and its current limitations, it is expected that Link 16 and 22 will soon form the Basic interface and Link 11/11B will be part of the extended interface to ensure interoperability with legacy platforms.

□ **Data Forwarding**

Data Forwarding is defined as the process of receiving data on one link (e.g. Link 16) and outputting the data in the proper format and protocol of another link (e.g. Link 22 or vice versa). Data Forwarding is unique to multilink operation. Although Data Forwarding is not the only type of operation that allows the exchange of information between multiple data links, it is the primary method of accomplishing the task. The following terms are used to describe forwarding units.

- Forwarding Link 16 MIDS Unit (FJU) is a JU that forwards data between Link 16, Link 22 and either or both Link 11 and/or Link 11B
- Forwarding Link 22 Unit (FNU) is a NU that forwards data between Link 22 and either or both Link 11 and/or Link 11B
- Forwarding Participating Unit (FPU) is a PU that is forwarding data between Link 11 and one or more RUs
- Forwarding Reporting Unit (FRU) is an RU that is forwarding data between 2 or more RUs

Any two links that are interconnected require the presence of a data forwarder. Standby Forwarders should be designated whenever a data forwarder is designated. Some forwarders have a standby forwarder mode, which should facilitate rapid

assumption of the data forwarding function by alerting the operator in the event that the designated data forwarder becomes inactive or degraded.

Some data forwarders are capable of establishing forwarding filters independent of filters established by its host. A data forwarding unit will not transmit data, when inhibited by a data forwarding filter.

Correlation is required before forwarding data from a link interface to another. The different granularity of positional data between Link 16/22 and Link 11 can increase the risk of dual tracks when forwarding data from Link 11 to any of the other links.

Forwarders must retain and forward all data, regardless of the message, word, field or bit level implementation of the unit.

□ Concurrent Operations

Data Forwarders increase the end-to-end delay when passing data from one link to another. Accuracy of information may also be affected when translating messages and loss of data may be due to congestion and connectivity. To overcome the above problems, some units are allowed to operate on more than one link interface at the same time, without forwarding duties. This is defined as Concurrent Operations and complements the limited number of Data Forwarders.

More precisely, a Concurrent Interface Unit is any IU that originates data simultaneously on more than one link (e.g., Link 16 and Link 22), but does not forward data between the links. The IU transmits only locally derived data and conforms to all the applicable link protocols for the links on which it is transmitting.

[ADatP-33] significantly limits the use of Concurrent Interface Units within Data Forwarding in order to avoid Data Looping as explained below.

□ Data Looping and Reception Priority Scheme

Within a multilink interface, certain operating configurations can produce data looping and dual tracks where a unit receives the same information from more than one data path and also its own data from another source. This can happen when both forwarding and concurrent operations are conducted across the same multilink interface or multiple forwarders exist. Planners and Operators should be aware that multilink configurations incorporating both data forwarding and concurrent operations could result in disruption of the tactical picture unless data looping is prevented. This is also the case when multiple forwarding units operate in the same area.

[ADatP-33] currently discourages all cases of Concurrent Operation and Data Forwarding Units that can generate data looping. The example and elements provided below are to ease the understanding of the problem and the potential solutions. This does not imply any recommended operational changes of the current allied and national doctrine.

Figure 2E.1-1 depicts an example of Multilink Operations with Data Looping, noting that the tactical picture received by all units is affected.

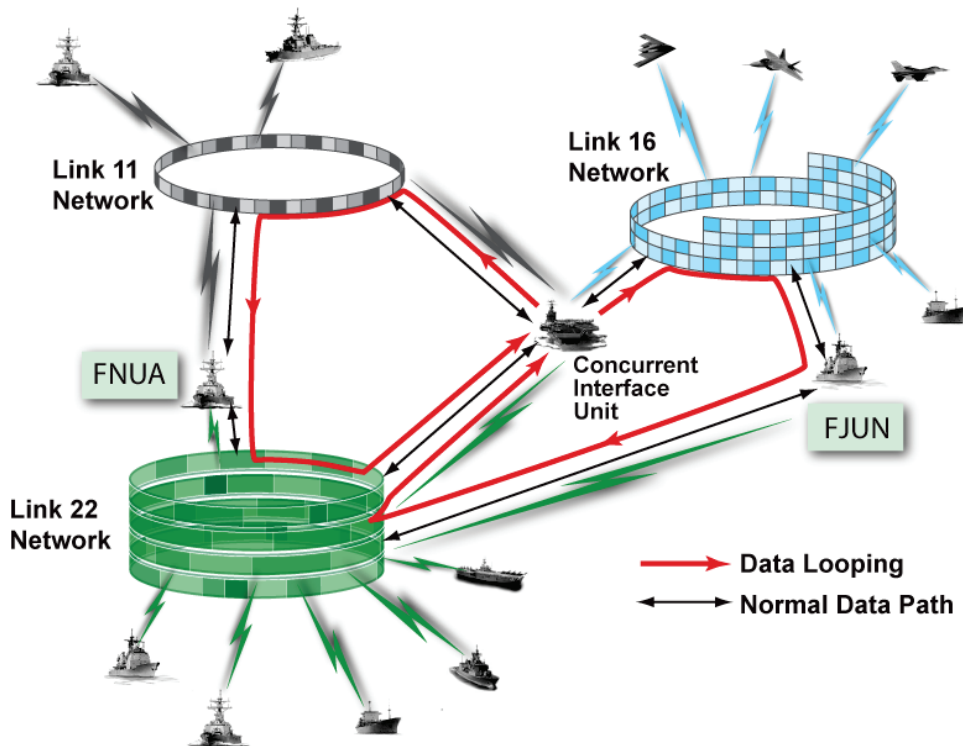


Figure 2E.1-1 Data Looping Example

The following protocols help to ensure that only one complete communications path is followed by any given item of tactical data. This is necessary to ensure against redundant, ambiguous, inefficient, and unnecessary processing of tactical data, and the potential interoperability problems which such processing can cause.

- A Forwarding IU does not forward any data received from a concurrent IU onto any link that the concurrent IU is active on
- Concurrent IUs discard any message from an IU that has been forwarded by the Forwarding IU if the information has also been received direct from the same IU
- A concurrent IU uses a priority scheme for processing received data. If an IU and its associated data are received over more than one of these paths the higher priority data is retained over the lower priority data. A possible priority ranking is provided below
 - Link 16 (MIDS or JTIDS)
 - Link 22
 - Link 11
 - JREAP

National implementations may differ in the handling of received messages when operating in multiple links with respect to both Data Forwarding rules and providing TDL data to the host. Methods used include Priority based on Link Interface (as above), Priority based on each individual track and Correlation/Data Fusion. The Planner and Operator should verify Capability & Limitations of each involved platform performing Data Forwarding and Concurrent Operations for possible conflicts.

2E.2 Multilink Considerations

Common key tactical protocols are first discussed, followed by two specific Link 16 protocols to aid the understanding of planning and operating in a multilink environment.

This sub-section is divided into the following.

- [Common Features](#)
- [Link 16 Unique Features](#)
- [Link 22 Unique Features](#)

2E.2.1 Common Features

The J-family allows the reporting of significantly more tactical information than Link 11 and Link 11B M-Series messages. Some of the field sizes have been increased to allow an improved degree of precision. Where possible, common data elements from Link 16 were used in Link 22; this provides for compatibility and ease of data forwarding between the two tactical data links. Link 22 provides significant improvements over Link 11, with many features similar to Link 16. The similarities to Link 16 are listed below.

- [Unit Addresses](#)
- [Track Numbers](#)
- [Track Quality](#)
- [Track Identification](#)
- [Friendly Platform Status](#)
- [Granularity of Measurement and Geodetic Positioning](#)
- [Lines and Areas](#)
- [Electronic Warfare](#)
- [Land Points and Tracks](#)
- [Space Tracks](#)
- [Threat Warnings](#)
- [Data Filters](#)
- [Correlation](#)
- [Data Registration](#)

□ **Unit Addresses**

Link 22 is able to use the same extended range of addresses as Link 16. This is detailed in section [2B.2.3 NILE Unit Parameters](#). This capability simplifies multilink network planning when only Link 16 and Link 22 are to be used. Link 11 may define IUs in the octal range 01-76 or 100-175 (Link 11B). Link 16 and Link 22 may define IUs in the octal range 01-76, 100-175, 200-7776, or 10000-77776, the other values are reserved (and illegal).

When planning and operating Link 16 and Link 22 together with Link 11, the Planner should use the Link 11 and Link 11B range when assigning C2 unit addresses.

□ **Track Numbers**

Link 22 is able to use the same extended range of track numbers as Link 16. This is detailed in section [2B.2.3 NILE Unit Parameters](#). This capability simplifies multilink network planning when only Link 16 and Link 22 are to be used. Link 11 uses track numbers in the range octal 0200 to 07776 which is 3967 values. Link 16 and Link 22 uses track numbers in the range octal 0000001 to 1777777 (with a few reserved values) which is 524,285 values. In multilink networking, due to the smaller range of the Link 11 track numbers, track numbers are assigned from the low range octal 0200 to 7776, before track numbers are assigned from the high range above octal 10000.

The Planner must assign Track Blocks to each unit based on the links being deployed, ensuring that if Link 11 and Link 11B are used, track blocks in the lower range are assigned to the data forwarding units. It is also recommended to use the lower range whenever possible for all units.

□ **Track Quality**

The J-family uses a four-bit Track Quality (TQ) field whose values can range from 0 through 15. Each TQ value is defined by a specific positional accuracy range. The highest Link 16/22 TQ value specifies an uncertainty area better than 1,080 ft² accuracy for air tracks. This provides a TQ error distance of 0.0031 dm or 19 ft. By comparison, Link 11 uses a three-bit TQ field, whose highest TQ value is 7. The highest Link 11 TQ value may only specify an uncertainty area better than 972,000,000 ft² accuracy for air tracks. This provides a TQ error distance of 1.1835 dm or 7,101 ft. In the case of an air track Link 16 and 22 allows a significant improvement in granularity. The difference in track quality affects multilink correlation. This allows an increased accuracy of the tactical picture when using

Link 16 and Link 22. Use of filters may reduce the effect of track quality differences when using Link 11.

□ **Track Identification**

The Track Identification (ID) reporting capabilities of the J-family have been greatly expanded compared to Link 11. A track reported by the J-family will specify track identification using the following fields: Identity, Platform, Activity, Specific Type, and Nationality. In Link 11, track identification is limited to three fields: Identity, Primary Amplification, and ID Amplification. The comparison of the field size for Track Identification reporting capabilities of the J-family are more detailed when compared to Link 11, as shown in [Figure 2E.2-1](#). This creates loss of information when translating from Link 11 and Link 16/22 and possible conflicts during operations.

Link 16/22	Bits	Link 11/11B	Bits
Identity	3	Identity	2
Platform	6	Primary Identity Amplification	2
Activity	7	Identity Amplification	3
Specific Type	12	Specific Type (Amplification Message)	6
Nationality	7	Nationality/Alliance (Amplification Message)	7

Figure 2E.2-1 Track Identification comparison

[Figure 2E.2-2](#) provides a comparison between the J-Series Identity and the Link 11 Identity and Primary Amplification. The differences are more significant when all other fields are also considered.

Link 16/22 IDENTITY	Link 11/11B IDENTITY	Link 11/11B PRIMARY IDENTITY AMPLIFICATION
Pending	Unknown	Pending
Unknown	Unknown	Unknown
Assumed Friend	Unknown	Assumed Friend
Friend	Friend	As appropriate
Neutral	Friend	General (only with id amp = 1, Neutral)
Suspect	Unknown	Suspect
Hostile	Hostile	No Statement (0)

Figure 2E.2-2 Track Identification Comparison

❑ **Friendly Platform Status**

The J-family messages provide a more detailed reporting of the status of friendly aircraft, including the following: equipment status, ordnance inventory, radar and missile channels, fuel/fuel available for transfer, gun capability, and estimated times of arrival and departure to and from station. On Link 16/22, a unit can also report its inventory of specific types of surface missiles. These items cannot be reported at all with Link 11, limiting the quality and granularity of information during operations.

❑ **Granularity of Measurement and Geodetic Positioning**

Granularity is a measure of how precisely a data item can be reported in the data link messages. The major J-family granularity improvements are in track positions (Latitude and Longitude), air track speeds, altitudes, and EW lines of bearing as depicted in [Figure 2E.2-3](#).

In particular, the J-family messages implement a three-dimensional geodetic coordinate system using latitude, longitude, and altitude, as shown in [Figure 2E.2-4](#). This allows positions to be reported anywhere in the world, subject only to display and database limitations. By contrast, Link 11 uses a two-dimensional Cartesian coordinate system, and allows track reporting only within a limited range of the reporting unit.

	Link 22	Link 16	Link 11
Air Track Position	0.0412 minutes (Course) (~250 feet) 0.0103 minutes (Fine) (~63 feet)	0.0051 minutes (~31 feet)	500 yards (Course) (1500 feet) 31.25 yards (Fine) (93.75 feet)
Air Track Speed	2 dm/hr	2 dm/hr	28.125 dm/hr (Course) 3.515625 dm/hr (Fine)
Altitude	25 feet	25 feet	500 feet (Course) 31.25 feet (Fine)
EW Lines of bearing	0.001 to >10 Degrees	0.001 to >10 Degrees	<1 to >5 Degrees

Figure 2E.2-3 Granularity Comparison Matrix

The basis of the geodetic coordinate system is the World Geodetic Survey 1984 (WGS-84). This allows for more accurate positional information. Correlation of tracks among Link 16 and 22 is ensured by similar accuracy, while dual track designations may be generated when operating with Link 11, which uses Cartesian coordinates.

This significantly improves the granularity and the quality of tactical picture during operations when using Link 16/22.

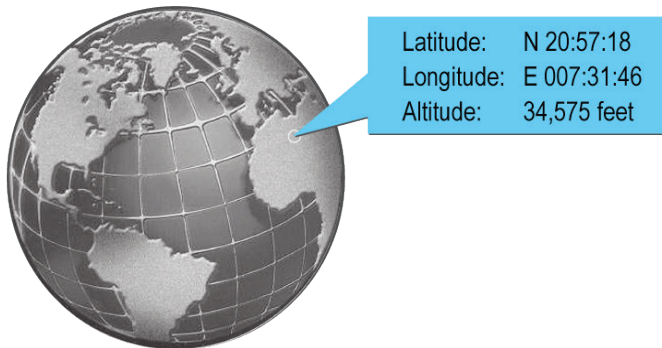


Figure 2E.2-4 Three-dimensional Geodetic Positioning

□ ***Lines and Areas***

The J-family messages allow the reporting of multi-segmented lines, as well as areas of all sizes and descriptions. Link 11, by contrast, does not allow lines, and it allows only areas of limited size that are circles, ellipses, squares, or rectangles. [Figure 2E.2-5](#) describes examples of the different types of Points, Lines, and Areas available in Link 16/22. Each type is transmitted in Link 16/22 using a series of the Initial, Extension, and Continuation words depending upon the complexity of the Line, Point, and Area. This allows for a more accurate tactical picture in Link 16/22.

Type	Description
Line	Corridor or Low Level Transit Route of 2 or 3 Points
	Corridor or Low Level Transit Route of More Than 3 Points
	Composed of 2 or 3 Points Fixed
	Composed of 2 or 3 Points each with Independent Course and Speed
	More Than 3 Points Fixed
	More Than 3 Points each with Independent Course and Speed
Point	Fixed
	With Independent Course and Speed
	Slaved Relative With Altitude
	Slaved Relative Without Altitude
	Slaved True With Altitude
	Slaved True Without Altitude
Multisided Area	More Than 3 Points Fixed
	More Than 3 Points each with Independent Course and Speed
Regular Area (a square, circle, rectangle or ellipse i.e., defined by one point)	Fixed
	Friendly Weapon Danger Area
	With Independent Course and Speed
	Slaved Relative With Altitude
	Slaved Relative Without Altitude
	Slaved True With Altitude
	Slaved True Without Altitude

Figure 2E.2-5 Type of Points, Lines, and Areas

□ **Electronic Warfare**

Electronic Warfare (EW) control directs actions to be taken by EW participants. Such actions include direction finding, jamming, deployment of decoys, and frequency protections.

J-family EW procedures are divided into EW surveillance procedures, and EW control and coordination procedures.

J-family messages allow the exchange of EW orders, a greater exchange of EW parametric information, and a wider range of EW control compared to Link 11, which has similar capability. Link 11B has no EW Command and Control functionality.

EW coordination includes all measures that ensure the sharing of data among the EW participants to provide the most complete evaluation and fixing of intercepted

electronic emissions. Examples for these measures are: requests to report EW Surveillance data, orders to cease reporting, and reports of associations / disassociations.

EW surveillance consists of EW parametric data and EW product data.

Parametric data (FJ14.0 messages) consists of raw, unevaluated EW intercepts and parameters received from EW systems. These include data on fixes, areas of probability, and lines of bearing.

Product data (FJ3.7 messages) consists of evaluated EW data. Normally, this means that an EW coordinator or other qualified operator has evaluated EW parametric data and determined an EW product.

The EW Control/Coordination (FJ14.2 messages) provides the capability to control participants, to respond to requests, and to coordinate activities among EW participants.

The major difference in EW between Link 16 and Link 22 is that, Link 16 separates the exchange parametric data and orders on to a dedicated EW NPG, while EW product information is exchanged on the Surveillance NPG. Like JREAP, Link 22 does not make a subnet separation for EW data. When significant threats are expected, a multilink planner should consider the extended capability of Link 16/Link 22.

□ ***Land Points and Tracks***

The J-family messages add Land as a track category, a category not currently available on Link 11. On Link 16/22, some of the Special Points currently reported on Link 11 are reported as Land Points, while others are reported as Reference Points. Land Points describe physical objects, such as buildings, whereas Reference Points are used for theoretical constructs, such as waypoints or stations. A Land Track is simply a mobile Land Point, such as an armored vehicle. This allows for a more accurate tactical picture in Link 16/22.

□ ***Space Tracks***

The J-family messages add Space (Ballistic Missile) as a track category. This category is no longer available on Link 11. On Link 16/22, impact areas and launch areas are reported as Special Points connected to the Ballistic Missile. Covariance data can be reported through the use of a data update request message. Link 16/22 Space Track also provides the capability of engagement coordination for Theater Ballistic Missile Defense.

□ ***Threat Warnings***

The J-family messages add a capability to report threat warning messages. Threat Warning message is originated by any C2 IU having knowledge of an immediate threat to one or more IUs or friendly tracks/points. Originating a threat warning is independent of track reporting responsibility (R2), controlling unit (CU) status, or other criteria. The Threat Warning message stimulates the automatic initiation of a track when the threat is not currently being reported.

□ ***Data Filters***

One of the most confusing yet beneficial aspects of TDL is the capability to filter data. Most platforms have the ability to filter their received or transmitted data, but they do not have access to the “Big Picture” to implement their various filters effectively. The multilink network manager has the responsibility to ensure that this capability is implemented effectively. In NATO doctrine, this role is covered by the Data Link Manager, while in the US, the role is covered by the JICO.

Data filters may be employed to inhibit selected tracks from transmission, to exclude them from track stores upon reception, and/or to inhibit them from being forwarded. Filters may be required to prevent the disclosure of protected data, or to prevent the overload of an individual unit’s database, of the data link itself, or even of the operator. Normally, filters are assigned either by Operation Order (OPORD) or OPTASK LINK. In view of both the high track density anticipated for modern and future warfare and of the greater numbers of platforms expected to participate, a versatile filtering capability is an important prerequisite for participating in data link operations.

This data filtering capability allows Reporting Responsibility (R2) to be partitioned according to various combinations of geographic areas, track environment/category, and track identity. The ordering and reporting of filter insertion can be reported over the Link 16, Link 22, or voice communications. Doctrine states that preplanned filters should be assigned in the OPTASK LINK, while others may be designed, ordered, and reported during the course of operations, as situations dictate.

Filters ordered on Link 16/22 may also apply to Link 11 and to data forwarding. The Operator needs to verify the capabilities and limitations of each platform related to filters, as these may vary greatly and may impact the ability to correctly partition the reporting responsibility in the theater of operations. The capability of separate filters for data forwarding also needs to be considered.

The selection of all units and in particular of a data forwarding unit should take into account the Capability and Limitations of each unit in the area of Data Filters.

□ **Correlation**

Correlation is a method to resolve local to remote dual designation by identifying tracks to be retained and to be dropped. Correlation is a requirement when forwarding data among multiple data links and in particular if they have different data accuracy. The planner should verify the extent of Correlation implementation and compliance to the standards when selecting a data forwarding unit, and assess the differences in the implementation of all other units. Remote to remote correlation is not a common TDL requirement and may be handled by Host/DLP systems differently. Link 11, Link 16 and Link 22 now use the same rules. However, the granularity of positional data in Link 11 may generate more duals than in Link 16 or Link 22.

□ **Data Registration**

Data registration is a feature that allows correct relative alignment between local and remote track positional data. Optimum interface data registration occurs when all IUs hold their locally derived track positional data at the same geodetic position as the remote positional data for the same track. Geodetic position is defined in terms of latitude, longitude, and altitude. The exchange of accurate track positional data is fundamental to the tactical picture. IUs that receive these reported tracks are required to attempt to correlate these tracks with local data. The correlation process is degraded when either the remote or local positional errors increase. Remote and/or local track positional errors may result in dual designations. Each TDL uses significantly different methods for maintaining data registration, as detailed in [Figure 2E.2-6](#).

Link	Method
Link 22	Geodetic Registration
Link 16	Remote IU Registration
Link 11	Gridlock
Link 11B	Site Registration

Figure 2E.2-6 Data Registration Methods by Link

Gridlock and Site Registration require each PU/RU to account for its known errors upon transmission of its track reports, whereas remote IU registration requires each IU to account for all other IU's errors upon reception of their track reports. Geodetic

registration requires each NU to account for its known errors in relation to the reference spheroid (normally WGS-84).

Furthermore, there is no requirement for Link 11/11B, Link 16 and Link 22 to use common grids, nor for the FJU/FNU to adjust forwarded track reports to account for differences between the TDLs. These differences could create significant errors in positional data exchanged between units in different links.

To ensure that data registration is maintained throughout a Link 11, Link 16 and Link 22 interface, it is essential that a C2 MIDS/JTIDS JU or a Link 22 NU be designated as the Gridlock Reference Unit (GRU) for Link 11 gridlock. This effectively aligns the Link 11 with Link 16 and Link 22 grids for track reporting purposes. The primary considerations for designation of the C2 JU or the NU to be used as a Link 11 GRU are listed below.

- The order of precedence for selecting the Interlink GRU is C2 JU, NU and then PU
- The unit should normally have reporting responsibility for a large number of tracks. Thus, an airborne C2 JU or NU is normally preferable to a surface or land C2 JU or NU
- The unit should have a high Geodetic Position Quality, which ensures that it is accurately aligned with other IUs. This can be achieved using Relative Navigation on Link 16 or other navigation systems that allow high fidelity position rating
- The unit should have a central position to allow easiest gridlock

Also the use of GPS by most IUs tends to make most reported positions extremely accurate geodetically. Direct Gridlock may still be unfeasible for widely dispersed PUs using GPS as a position reference. Correlation and Data Registration processes are interrelated, as the result of one process affects the input of the other process.

2E.2.2 Link 16 Unique Features

Link 22 does not have some of the features that Link 16 has. This subsection covers the two main features of Link 16 that have no direct equivalent in Link 22, which need to be considered in multilink planning and operations. The features are the following.

- [Relative Navigation](#)
- [Air Control](#)

□ ***Relative Navigation***

Link 22 does not include the Relative Navigation process available in Link 16 JTIDS/MIDS, as the system was developed with the knowledge that independent accurate navigation systems were already available, including GPS systems. It is important to have positional accuracy to ensure the quality of the tactical picture and this may affect the selection for Data registration.

□ ***Air Control***

Link 16 provides the means for C2 JUs to control nonC2 JUs. The C2 JU can also direct handover commands to another C2 JU. A dedicated Network Participation Groups (NPG) is used to exchange the messages in JTIDS/MIDS. Any Air Control when only using Link 22 and/or Link 11 will require Air Control executed by voice command.

2E.2.3 Link 22 Unique Features

Link 22 has some key features that enhance its efficiency and capabilities, which need to be considered in multilink planning and operations. The first three topics have operational implications, while the other topics are presented for a broader understanding of Link 22.

- High Update Rate (HUR)
- Slow Update Rate Protocol (SLURP)
- Addressing, MASN and Data Forwarding
- External Encryption
- Data Extrapolation
- Machine Receipt
- Transmission Assurance
- Track Position Reporting

□ ***High Update Rate (HUR)***

Link 22 provides a High Update Rate (HUR) capability. HUR allows a selected track to be updated for transmission more frequently than Standard Update Rate (SUR) tracks. HUR reporting occurs for a variety of operational reasons and/or when the track is the subject of an F01.6 Command message which orders the recipient to commence an aggressive action against a track. Some operational reasons for specifying a track as HUR are the following.

- Track is the objective of an engagement order
- Track is the objective of an assignment order
- Track is the object of a time critical order such as Engage Objective TN with Specific Number of ASM/SSM to Meet Impact Time
- The track is an object of particular interest to an NU that does not hold sensor contact on the track, e.g. the track has been identified as a threat, or the track is a rendezvous point, or the track is a forward observer unit in a surface fire support operation, etc.

HUR may be specified for a selected track in three ways.

- Manually initiated by the NU with reporting responsibility
- Requested by any NU with interest on the remote track
- Ordered by the authority directing an action against the track by transmitting an F01.6 message

This feature allows for more frequent updates of specific tracks.

□ ***Slow Update Rate Protocol (SLURP)***

Link 22 allows air tracks to be designated as Slow Update Rate Protocol (SLURP) tracks. SLURP allows non-hostile air tracks flying a relatively straight and level route, typically civilian airline traffic, to be reported at half the normal update rate. SLURP can only be manually initiated by the NU with reporting responsibility. This feature increases the number of air tracks which can be reported during a given time.

□ ***Addressing, MASN and Data Forwarding***

Link 22 provides two different Addressing services, which can normally be used at the same time. These are addressing with required acknowledgement and addressing without required acknowledgement. For both of these addressing services, the following five types of addressing are available.

- **Totalcast**, addressed to all link 22 units
- **Neighborcast**, addressed to all RF neighbors on each NILE Network on which the NU is transmitting
- **Mission Area Sub Network (MASN)**, addressed to a logical group of units that has been previously defined
- **Dynamic List**, addressed to a list of two to five units that are specified in the request
- **Point-to-Point**, addressed to a single unit

There are no TDL “network” addressing schemes allowing a JU or PU to transmit information to a NU; the only information they can share is the Source and the Addressee Track Number.

Moreover, while a Link 22 Network is able to forward Link 16 information on its network and still indicate which unit was the information originator, the reverse is not true. Link 16 is currently unable to perform this operation. This is also true in the case of JREAP.

Messages generated in Link 16 can be addressed to a MASN in Link 22, using a mechanism that associates group addresses to MASNs.

Addressing control is a similar concept to the NPG. The purpose of the NPG is to maximize the use of bandwidth limiting the users receiving on a specific NPG and segregating data. Addressing in Link 22 works similarly, limiting the relay of messages to those units which are required to receive the message. However, the SNC always sends any messages it receives to the DLP, even though it is not an addressee of the message.

[[STANAG 5522](#)] does not specify the use of addressing and national implementation may differ when congestion occurs. Operator should assess capability and limitation of involved units and in particular in the selection of a Link 22 capable forwarding unit.

□ ***External Encryption***

Link 22 allows for externally encrypted data to be transmitted through Link 22, further allowing the exchange of highly classified data and simplifying data segregation. Data extrapolation and Machine Receipt are two examples (described below) of protocols performed in the Link 16 terminal that prevent Link 16 from being used to transmit pre-encrypted data. Link 11 also allows for externally encrypted data.

□ ***Data Extrapolation***

Data extrapolation is required to synchronize the position of a track with the transmission time. The DLP or the terminal, computes the expected position of the track at the time of transmission, using current course and speed. The JTIDS and MIDS terminals currently provide extrapolation. This requirement makes these terminals aware of message content. In Link 22, Link 11 and JREAP the extrapolation is a function of the DLP. The SNC does not need to interpret tactical content, which therefore may be externally encrypted.

□ ***Machine Receipt***

The JTIDS and MIDS TDL interfaces currently provide TDL message machine receipt output to original order messages addressed to own unit or units listed in Secondary Track Number Lists (e.g. Source, Addressee, and Receipt Compliance field manipulations). This requirement makes these TDL interfaces aware of message content. In Link 22, the SNC does not interpret tactical content, and machine receipt is accomplished through SNC protocols that do not require access to the tactical content. Therefore this allows Link 22 system to process messages other than F-Series and FJ-Series.

□ ***Transmission Assurance***

Link 22 SNC provides the notification to the TDS/DLP of when a message has been transmitted, while this does not occur on Link 11 and Link 16 for JTIDS, MIDS, and JREAP.

□ ***Track Position Reporting***

Some of the Link 22 tactical messages have two sets of Latitude and Longitude fields overlaid. An example is represented by the F2 Air Track.

The granularity of the coarse fields is 0.0412 minute and the granularity of the fine fields is 0.0103 minute, but the fine fields omit the two Most Significant Bits (MSB). The Lat/Long Scale Indicator determines which fields of the stack are being used. When a track or PLI is initially transmitted or transmitted as a result of returning to Active status, or when crossing certain values, the coarse fields are transmitted for two reports. Thereafter, the fine fields are transmitted except in every 10th report, when the fine fields are replaced by the coarse fields. The Lat/Long Scale Indicator is set appropriately.

Units need to retain the Most Significant Bits (MSBs) in their database since the following nine periodic updates will be received with the fine granularity only. If an NU receives a track report with fine granularity (LLS IND set to value 0) and no prior report has been received with the coarse granularity (LLS IND set to value 1), the NU needs to either discard the message and transmit an FJ7.1 Data Update Request message for Reference TN.

2E.3 Multilink Planning with Link 22

Interface planning is by far the most difficult element of Multilink Operations. Determining the configuration for efficiently interconnecting the C4I and weapon systems using the various links to satisfy the operational Information Exchange Requirements (IER) is the challenge faced by Multilink Interface planners.

Prior to the introduction of Link 22, it was stated that an effective way to protect the integrity and effectiveness of a Multilink architecture and its component TDLs was to minimize the need for 'on-line' management by making every effort to optimize the architecture 'off-line'. Complex Network Monitoring and Management systems have been built to simplify 'on-line' management. This problem is significantly reduced in Link 22.

The capability to exchange data requires that the proper medium be in place in advance of initiation of any TDL system. This may be landline or frequency allocation. It is the task of planners to acquire necessary frequency clearances. With Link 16 the frequency band used is also used by systems operated by national aviation authorities. This requires a unique procedure to ensure compliance with the restrictions.

Link 22 frequencies, like those for Link 11, reside within the Military band for both HF and UHF, as depicted in [Figure 2E.3-1](#). This has the added benefit of reducing the need of Link 16 frequency band utilization. Link 22 does not have any requirement to limit transmission. Link 16 is required to compute and monitor during operations the Time Slot Duty Factor (TSDF), which is a measure of the transmission pulse density. Link 22 does not have to do this.

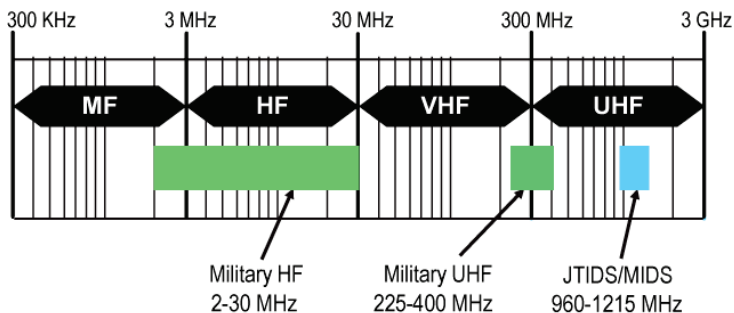


Figure 2E.3-1 Frequency Spectrum

This section describes in detail the following topics.

- Planning Process and Considerations
- Planning Comparison Link 16/Link 22
- Planning with Link 22
- First Example with Link 22, 16 and 11
- Second Example with Link 22, 16 and 11
- Example of Link 22 interconnecting two Link 16 networks

2E.3.1 Planning Process and Considerations

Multilink planning is a multiple stage iterative procedure which requires the planning of each link separately, to satisfy the overall requirements, as detailed in [ADatP-33]. Section 2B provides an overview of Link 22 planning as a single link.

In general, planning should limit the use of multiple link interfaces, unless necessary to satisfy IERs. This is because the use of Data Forwarding and Relay affects the end-to-end delay and latency of the tactical picture distribution.

The Multilink planning encompasses the design and coordination responsibilities at the tactical commander level. It is the process of specifying the communication requirements in support of planned tactical operations and translating those requirements into sets of initialization data for use by all intended Multilink participants. This includes provisions for expanding the number of participants, to include transiting platforms. A high level list of tasks and considerations is listed below.

- **Operational Environment**
 - Plans and Operational Scenario
 - Requirements Definition and Prioritization
 - Communication Equipment Characteristics
 - EW and Cryptographic Requirements
- **Participants**
 - Locations and planned movements of the Participants
 - Connectivity
 - Platform identification, including Capabilities and Limitations
 - Voice Communications Asset and Requirements
- **Produce the OPTASK LINK (OLM) and the Air Tasking Order (ATO)**

When planning a Multilink architecture, the amount of data to be transmitted may have to be limited to the least capable system. It may be necessary to use filters to reduce the traffic level on one system while taking advantage of another system's higher capacity. This is the case when all the platforms involved are part of a combined multi-network architecture and no data segregation is planned.

In Link 11 this may prevent high threat traffic from being updated at a satisfactory rate. Link 22 reduces the risk that both locally generated and forwarded messages are delayed, based on the multi level priority scheme. Link 22 can also automatically manage changes in traffic flow.

Tactical datalink use must take into consideration the geography of the area of operations and the placement of forces to ensure data is able to get from point A to point B. This may require the use of HF frequency (Link 22 and Link 11), relay (automatic in Link 22, planned/managed in Link 16) and satellite. As mentioned above, coverage and relay problems are simplified when using Link 22 by its automatic relay capability.

For multinational operations, a planner may consider the use of only Link 16 and Link 22 for the real time tactical picture, and only use satellite for reach back and reach forward capability.

2E.3.2 Planning Comparison Link 16/Link 22

Currently, in order to set up multiple TDL networks, each TDL needs to be set up according to its own requirements. A brief comparison of the steps required in Link 16 and Link 22 is provided to compare the complexity of each task.

With Link 16 multiple complex and time consuming steps are required to define a Network.

- Planning: verify geographical connectivity constraints
- Design: define a new basic network structure (or identified if an existing one can fulfill the exchange requirements. This is usually done through the use of a software design tool)
- De-confliction: ensure compliance with the Frequency Clearance Agreement (Link 16 uses a civilian radio band)
- Distribution: design needs to be distributed to network design cells using the NetMan T/1 format, optionally along with a "STANDING" OPTASK LINK

- Network Design files: Network design cells produce and distribute MIDS/JTIDS initialization files to platforms
- OPTASK LINK: finally, prior to network operations, the final OPTASK LINK (Link 16 portion), describing the list of participants, their roles and the network they will use, must be distributed

With Link 22, significantly simpler planning steps are required.

- Planning: only basic network structure needs to be planned. Tool suggested, but not required
- Frequency: verify frequencies and assets availability
- Design: not required in Link 22
- OPTASK LINK: finally, prior to network operations, the final OPTASK LINK (Link 22 portion), describing the list of participants, their roles and the network they will use, must be distributed

2E.3.3 Planning with Link 22

Even if an early deployment of a national Link 22 platform may not implement all tactical messages and network management protocols, the added capabilities provided by the SNC allows Link 22 to provide significant improvements compared to Link 11.

Link 22 has fewer restrictions than Link 16 (based on frequencies and TSDF), making it a solution for areas where Link 16 needs to be limited or cannot be used. Link 22 can be used as primary link if there is no need for automated Air Control and accurate external positional data is available.

Link 16 and Link 11 have no concept of selective addressing. When a message is received, the unit will know the originator, but not a path to exchange data with the unit, including Receipt/Compliance (R/C). Link 22 allows the recipient to identify the involved data forwarder therefore correctly addressing any R/C or required tactical message response.

When considering multilink planning, a Link 22 Super Network which may be composed of multi NILE networks only needs to be treated as a single link.

Since connectivity is one of the key factors to enable message exchange, the LOS limitation of Link 16 needs to be taken into account, which is limited to 220 NM when air platforms are involved and about 20 NM when surface units are involved. Use of Link 22 simplifies planning in an extended theater of operations. The only constraint is to ensure that the required connectivity between units can be achieved. The distance

between units in Link 22 using HF can be significantly greater than Link 16. The use of HF by Link 22 is optimized but not limited to 300 NM between any two units. Test transmissions of HF have been successful at over 800 NM. New waveforms are being validated to optimize the range up to 1000 NM and to increase the bandwidth.

When Link 22 is used as a data forwarder between two Link 16 networks or extended multilink networks are involved, planning needs to consider the effect of traffic requiring multiple relaying and data forwarding, as this substantially decreases the track per second in all the involved links. This is no different than using JREAP-A for example.

The use of priorities in Link 22 will ensure that high priority traffic will be injected first, even though the message is generated in Link 16 or Link 11 which have no concept of priority. This will automatically ensure that high threat messages are delivered even where there is congestion.

For each pair of links, a data forwarding unit needs to be defined. When multiple links operate in the same area, a single forwarding unit should be considered. A few examples are provided to show the use of Link 22, including extended area of coverage.

In a Multilink environment, there is no need to combine TDL Manager/JICO unit with the SNMU, while a reliable connection between the two units is required. The SNMU should preferably be selected among the units that combine full Link 22 Network Management implementation, an expert TDL Operator and with a central location within the Super Network.

The use of Management Tools for planning in a Multilink environment is more a necessity than when using Link 22 alone, due to complexity of Link 16 and the limitation of the Link 11. The considerations in the following examples are based on Link 16. JREAP has complexity in the use of sub-netting which is not addressed. JREAP is currently mainly only a US implementation not part of the basic interface. However other allied nations are adopting it.

□ **First Example with Link 22, 16 and 11**

A first example of multilink is when all links are used to convey all data to all involved units as if the multiple links where only a single link, as depicted in [Figure 2E.3-2](#). In this case units may be members of one or more links, depending on their capability, and all tactical messages may need to reach any unit. This requires the use of extra bandwidth for data forwarding, increasing the time between two track updates. In this case a single FJU is required and recommended. Additional data forwarding capable units should be planned in the case of connectivity changes requiring multiple forwarders.

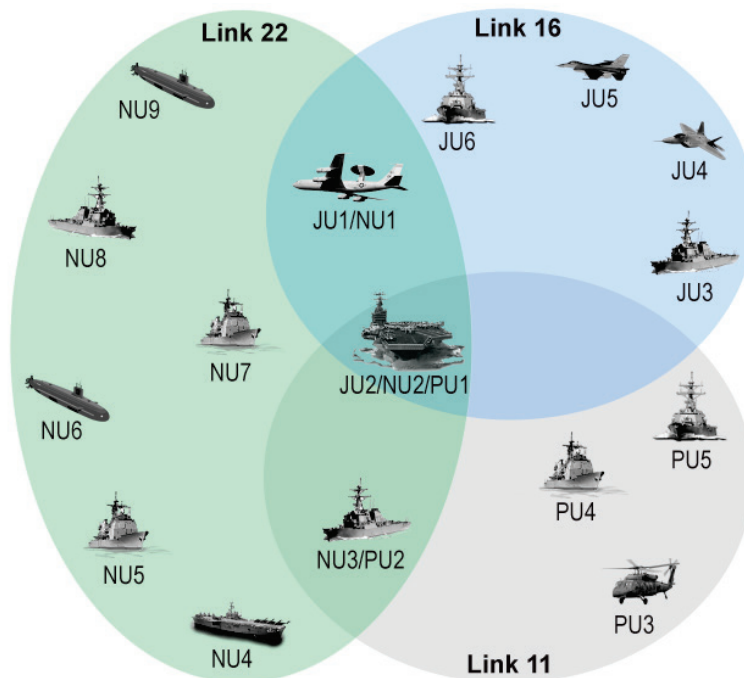


Figure 2E.3-2 Link 11, Link 16 and Link 22

2E.3.4 Second Example with Link 22, 16 and 11

Based on the extended coverage of Link 22, a second example is when Link 22 is used both to extend connectivity and to provide the main way to convey data in an extended area network. This example is suitable when the area of operation is greater than LOS limitations of Link 16. The example also assumes that different links are used with different operational objectives. Figure 2E.3-3 depicts an example where Link 22 is used for subsurface operations, while Link 16 is dedicated to Air Operations. Link 11 is used for legacy platforms. This example limits the number of potential concurrent units and data forwarding units are generating less traffic, compared to the first example. This also decreases the probability of dual tracks and data looping. When more bandwidth is available, the update rate of all tracks will also be greater improving the overall quality of the tactical picture. In this example, Link 11 may be used only to ensure connectivity with legacy platforms and most of the traffic may be limited in the direction from Link 22 to Link 11.

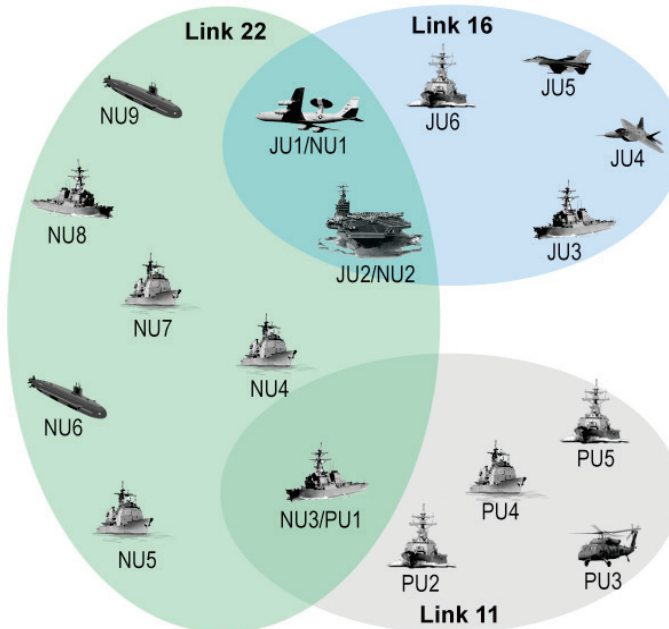


Figure 2E.3-3 Link 22 as main Maritime Interconnecting Link

2E.3.5 Example of Link 22 interconnecting two Link 16 networks

Link 22 can also be used to interconnect separate networks, such as two separate Link 16 networks. In [Figure 2E.3-4](#), traffic originated in Link 16 Network 1 can reach the Link 16 Network 2 units through Link 22 automatic relay and/or BLOS capability. Two separate data forwarders need to be defined in order to interconnect the two Link 16 networks. Proper filter definition needs to be in place not to flood the Link 22, which has a throughput comparable to JREAP A. This deployment can be an effective alternative to satellite as either a primary or alternative path.

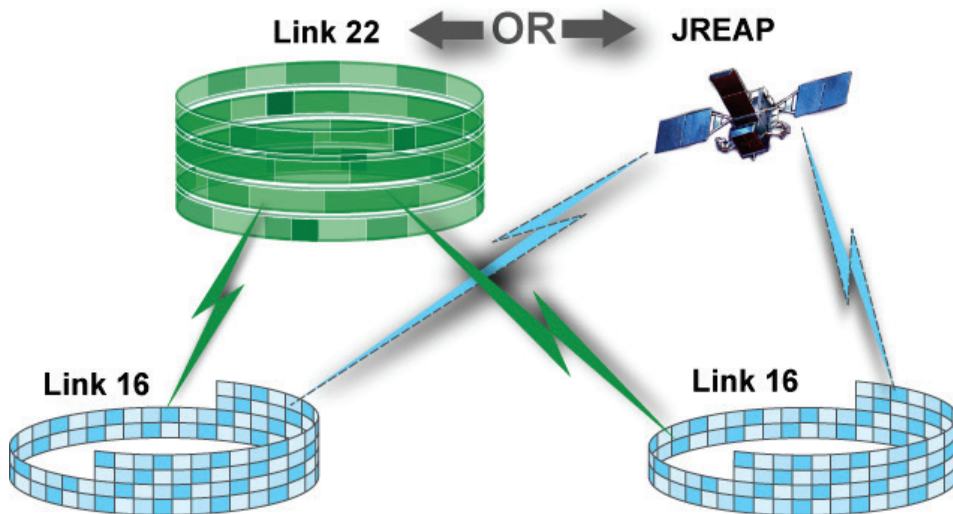


Figure 2E.3-4 Link 22 Extending Link 16 Range

Additionally, combining JREAP with Link 22 will allow the further extension of the coverage, without adding complexity. Both Link 22 and JREAP have mechanisms to detect data looping, which is achieved in Link 22 by using the information of which unit originated the track and which unit forwarded in Link 22.

2E.4 Multilink Operations with Link 22

The elements for consideration during operations are the same as those made during planning, including geographic location, coverage and relay. In addition, the effect on update rates of each link needs to be monitored when managing active networks, to avoid imbalance in the system. Monitoring of the statistics available on the DLP interfaces can provide the operator information as to whether any implemented change improved or further impaired the traffic through Link 22. The update rate of tactical messages for each involved link can be monitored, as shown in [Figure 2E.4-1](#). Section 2C provides other elements for monitoring and managing Link 22.



Figure 2E.4-1 Update Rate for a generic track in Link 16/22

Changing from Link 11 to Link 22 during operations, will not generate any side effect if all involved units are Link 22 capable or data forwarding exists to exchange data with Link 11 only equipped units.

Link 22 can easily provide the Operator with trend information about deteriorating or improving conditions that require changes, as some of the changes require operator intervention. This may be also necessary to adapt the flow of data, if traffic patterns change during operations.

The use of Management Tools during operations in a multilink environment is a necessity due to the complexity of Link 16 and the limitation of the Link 11 waveforms. Connectivity changes and limitations in frequencies and TSDF need to be assessed, when approaching new areas of operations. The need of specific Management Tools for Link 22 standalone is not required.

Connectivity changes may affect traffic exchange. The TDL manager should ensure that a connectivity path always exist to connect all units in the multilink environment. If connectivity is affected, data forwarding units may also require adjustment. Additional data forwarding units and concurrent operation unit may also be required, increasing the risk of data looping.


Automatic features of Link 22, including Relay, Role takeover, LNE and DTDMA can compensate for changes in the environment, without operator intervention or the use of a tool.

In Link 16, if a Relay unit becomes unavailable or its area coverage is reduced, some units may no longer be able to receive tactical traffic. Changes in Data forwarding rules and filters may be required and the use of Link 22 may need to be extended, to compensate for the loss of Link 16 relay unit.

During operations if the SNMU and the Standby SNMU become unavailable, the same considerations highlighted in planning should be made for assigning new roles. The SNMU and TDL Manager should ensure that a suitable Standby is always present, if the SNMU unit changes.

When any NU leaves the Super Network and the area of operations, the NMU needs to decide if changes to the ONCS are required to reassign the unused capacity to other units. The SNMU may also need to update MASN allocation, including Network Membership. When a unit joins the Super Network, the SNMU needs to update relevant MASNs, based on the operational role of the joining unit. ONCS changes may also be required.

In an extended deployment, the assigned key material may no longer be sufficient to cover the operations, so the TDL manager needs to ensure that valid keys are available and/or distributed to all participants units. For Link 22, key changes are required every week.



This page is intentionally left blank.

Chapter 3

Link 22 Technical

This chapter contains technical details of Link 22, consisting of the architecture, functions, and protocols. It is primarily intended for integrators, software engineers and testers. Readers of this chapter are expected to have knowledge and understanding of the previous chapters, as this chapter will explain details without reiterating the higher level information already provided. This chapter will discuss non-tactical Link 22 features, functions, interfaces, and messages. The tactical messages were discussed in [Chapter 2 Section D](#).

Section A Architecture

This section contains a more technical description of the components of the architecture (shown in [Figure 3A-1](#)) and the interfaces between the components.

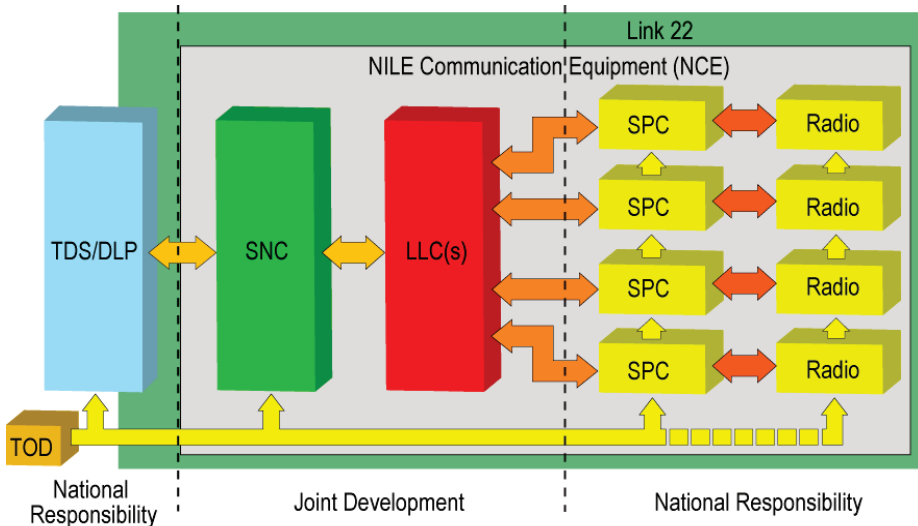


Figure 3A-1 Link 22 Functional Architecture

The components and interfaces described are as follows.

- DLP
- TOD
- DLP-SNC Interface
- SNC
- SNC-to-LLC Interface
- LLC
- LLC-to-SPC Interface
- SPC
- SPC-to-Radio Interface
- Radio Equipment

3A.1 DLP

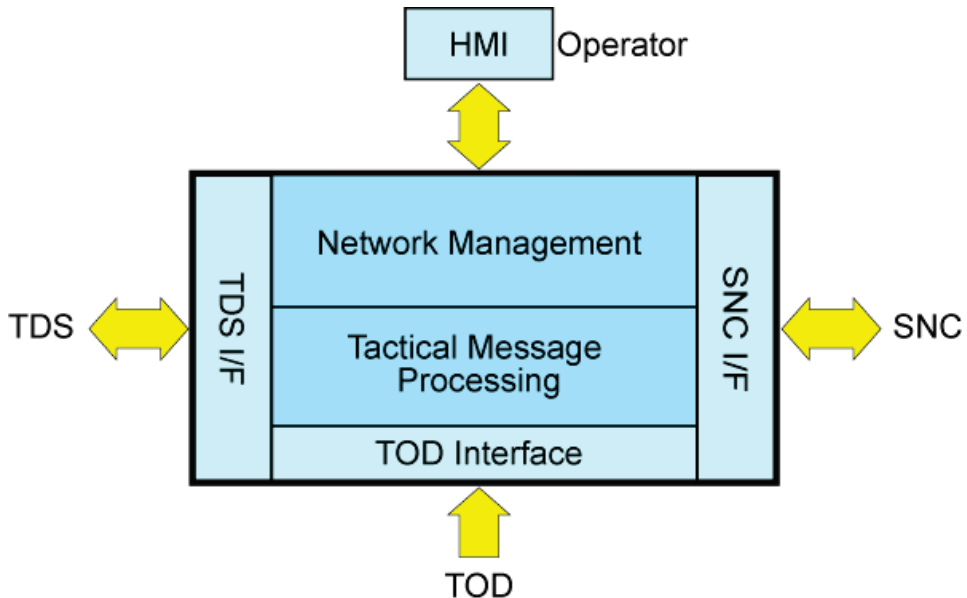


Figure 3A.1-1 DLP Functional Architecture

The two major Link 22 functions performed by the Data Link Processor (DLP) are Tactical Message Processing and Network Management. The DLP interfaces with the Tactical Data System, the Operator (by use of a Human Machine Interface (HMI), which may be provided by the TDS), the Time of Day (TOD) and the System Network Controller (SNC). These are shown in [Figure 3A.1-1](#). The DLP-SNC interface is the only DLP interface that is a part of Link 22. All the other interfaces are beyond the boundaries of Link 22.

3A.2 TOD

The Link 22 System requires that a TOD reference be provided at each NU which is within +/- 0.5 milliseconds of UTC. This accurate TOD is required for the SPC and EPM Radios to ensure that transmissions occur at the correct time. The TOD is also supplied to the SNC as it needs to get requests for transmission and reception to the media segment before they occur. As shown in the DLP section, the DLP also has a TOD input. This TOD is required so that the DLP can ensure the accuracy of the tactical picture, but does not need to be as accurate as that provided to the rest of the system. The DLP has to extrapolate track position to the time of transmission which is in units of seconds. Each part of the Link 22 system may have their own TOD input or may share a common TOD input. The LLC does not have or require a TOD input as it encrypts for a future timeslot and decrypts for data received in a previous timeslot, based on the time of the timeslot as supplied by the requesting component.

The TOD Interface provides a Time Figure Of Merit (TFOM), associated with the TOD, which represents the inaccuracy of the TOD from the UTC. If the TFOM value is too large, as shown in [Figure 3A.2-1](#), then transmission has to be inhibited, to stop the NU from transmitting at the wrong time, relative to the other NUs. Attempted reception continues on all networks irrespective of the TFOM value.

TFOM	Transmissions
< 1 millisecond	Allowed
1-10 milliseconds	Stopped for UHF FF and UHF EPM
> 10 milliseconds	Stopped for all networks

Figure 3A.2-1 TFOM Transmission Rules

The UTC time input to the DLP, SPCs and EPM Radios is an implementation issue for the manufacturer of the equipment, although the SPC specification recommends the use of the Extended Have Quick format as specified in [[STANAG 4430](#)].

The SNC has a device independent TOD interface which consists of a shared memory area and the time from the computer system clock. An interface program connects to whatever hardware the TOD uses and reads the TOD input. This Read TOD application then compares the supplied TOD to the system clock and stores this offset in the shared memory, as shown in [Figure 3A.2-2](#). The separation of the Read TOD application (TOD Hardware Dependent Software) from the SNC, provides better

portability of the SNC code and allows for the implementation of different TOD inputs without modification to the SNC. The Read TOD and the SNC applications must use the same system clock, and therefore should run on the same processor. An example of a Read TOD application is provided as part of the NRS software.

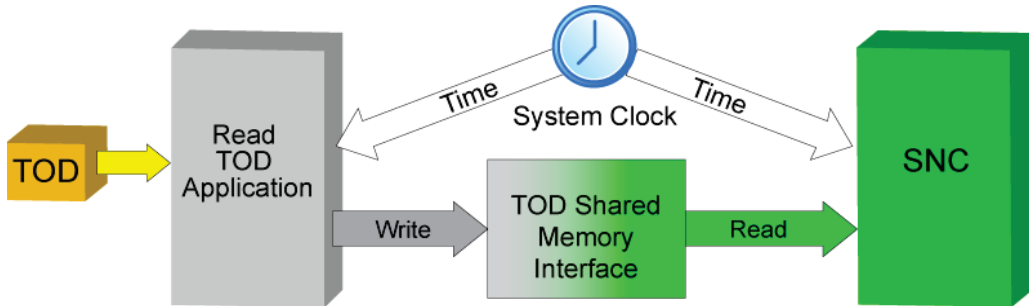


Figure 3A.2-2 TOD Shared Memory Interface

The SNC calculates the UTC time by adding the offset in the shared memory to the system clock. All other time information such as the day of year, leap year, leap second information and TFOM information is also passed to the SNC via the shared memory location. The status of the TOD input and the time when the interface was last updated are both stored in the shared memory so that the SNC can know the status of the TOD and know that the time is being constantly updated. The structure of the shared memory area is documented in the [NRS IDD], section 3.5.3 Internal Shared Memory Interface.

Details about TOD input failure and TFOM processing are included in Appendix B, Troubleshooting.

3A.3 DLP-SNC Interface

The DLP-SNC Interface enables the exchange of data between the DLP and the SNC components. The DLP-SNC Interface is defined in the [DLP-SNC IDD], and is described in the following sub-sections.

- Physical Interface
- Functional Interface
- Message Definition
- Tactical Interface
- Control and Status Interface

3A.3.1 Physical Interface

The DLP interfaces with the SNC portion of the NCE, as shown in Figure 3A.3-1.



Figure 3A.3-1 Physical Interface between DLP and SNC

The DLP-SNC Interface uses TCP/IP over an Ethernet based Local Area Network (LAN) connection (ANSI/IEEE 802.3 or ISO 8802/3). A faster Ethernet interface (100Mbps or faster) reduces the latency across the interface, and is recommended. The speed selected is dependent on the interfaces available on the DLP and SNC processors. If the DLP and SNC are hosted on the same processor then the TCP connection is internal to the processor and not dependent on the hardware. This single physical point-to-point interface carries both tactical data, and control and status information.

3A.3.2 Functional Interface

The DLP-SNC Interface consists of two different functional interfaces: the Tactical Interface and the Control and Status Interface, as shown in [Figure 3A.3-2](#). The Tactical Interface provides connection between the DLP Tactical Message Processing function and the Communications Transport (CT) function of the SNC. The Control and Status Interface provides connection between the DLP Network Management function and the Management Function (MF) of the SNC.

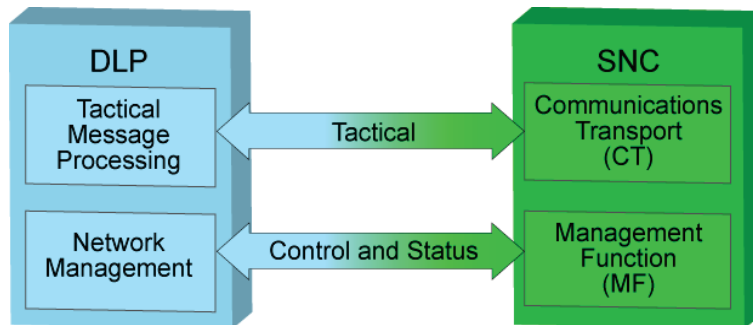


Figure 3A.3-2 Functional Interfaces between DLP and SNC

The DLP has to process tactical data received on the tactical interface and provide to the interface the tactical data it wants to transmit. The DLP provides the management of the system via the control and status interface. The implementation of both these functions within the DLP remains a national responsibility.

3A.3.3 Message Definition

Ethernet packets are transmitted on the Ethernet LAN. Ethernet packets contain TCP/IP network packets, which consists of a header and an interface network packet. Details about Ethernet packets and TCP/IP network packets can be found in the [DLP-SNC IDD]. The DLP-SNC messages are contained within the interface network packets.

Due to the maximum size of an Ethernet packet, the recommended maximum interface packet size is 1460 bytes. DLP-SNC messages larger than 1460 bytes are fragmented by TCP, which is transparent to the DLP-SNC interface. TCP fragmentation increases latency and bandwidth usage, and therefore the DLP-SNC interface attempts to avoid the use of large messages where possible.

The DLP-SNC interface communications on the LAN use ‘Little Endian’ byte format, which is the opposite of ‘Network Standard’ order.

□ Interface Network Packet Format

The structure of the interface network packet is shown in Figure 3A.3-3. The mandatory network packet header contains the interface network packet length and the number of messages. The interface network packet length is the sum of the network packet header length (4 bytes) and the lengths of all the messages. The number of messages defines how many messages follow the network packet header (variable number, at least one). This allows for more than one message to be put into one interface network packet (depending on their total size) and sent at the same time. This reduces latency and saves bandwidth, as long as the maximum size of the interface network packet does not exceed the recommended maximum of 1460 bytes.

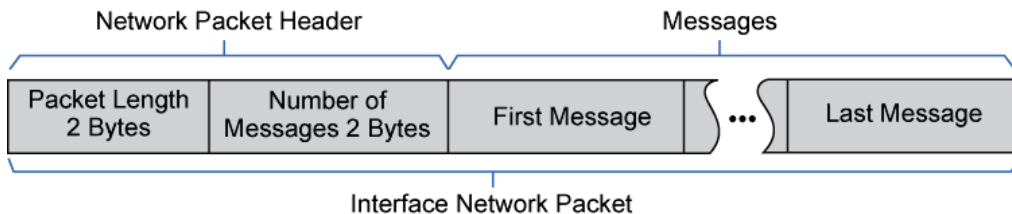


Figure 3A.3-3 DLP-SNC Interface Network Packet Structure

❑ **Message Format**

The structure of the DLP-SNC messages is shown in Figure 3A.3-4. The mandatory Message Header contains the Message Length and the Message Type. The Message Length is the sum of the length of the Message Header (4 bytes) and the lengths of all the message fields. The Message Length has a minimum value of 4 bytes when there are no message fields. Messages with no fields are used when the Message Type alone represents the information that needs to be conveyed by the message. An example of a message without data fields is a ‘Key-Zeroization Request’ (321h) message.

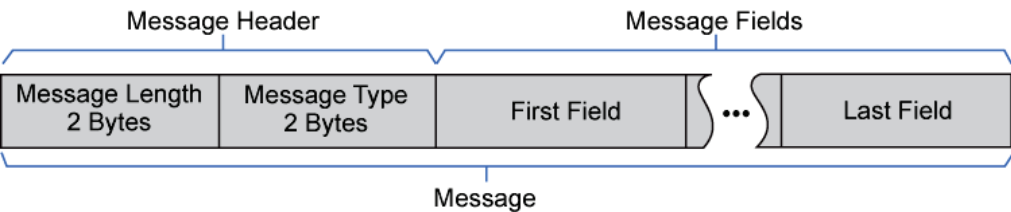


Figure 3A.3-4 DLP-SNC Message Structure

The Message Type uniquely defines the message, and the message structure and contents define how many message fields follow the Message Header. The DLP-SNC interface Message Type is represented throughout the guidebook as a hexadecimal number (without leading zeros) followed by a lowercase letter h to indicate hexadecimal, surrounded by parentheses, which are usually found after the message name (e.g. ‘DLP Cannot Comply’ (104h)). The structure of the Message Type as shown in Figure 3A.3-5, consists of three sub-fields: the Message Variant, the Message Group and the Message Number.

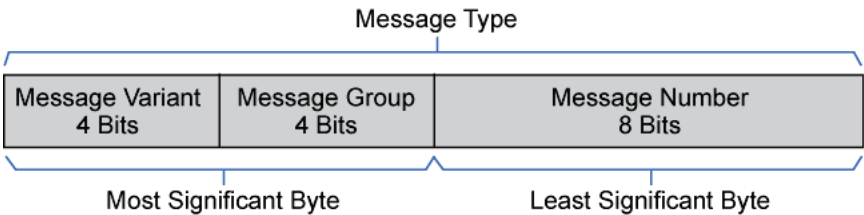


Figure 3A.3-5 Message Type Structure

The ‘Message Number’ identifies a specific message within a specific ‘Message Group’ for a specific ‘Message Variant’.

The ‘Message Group’ number indicates which functional group the message belongs to, for a specific ‘Message Variant’. When the ‘Message Variant’ is zero, odd numbered message groups indicate the message is produced by the DLP, and even numbered message groups indicate that it is produced by the SNC. The ‘Message Group’ values and their meanings are shown in [Figure 3A.3-6](#). When the ‘Message Variant’ is non zero, this rule no longer applies.

Message Group	Meaning
1	Tactical Interface Messages from DLP-to-SNC
2	Tactical Interface Messages from SNC-to-DLP
3	Control & Status Interface Messages from DLP-to-SNC
4	Control & Status Interface Messages from SNC-to-DLP
6	Monitoring Messages from SNC-to-DLP
8	Fault Messages from SNC-to-DLP

Figure 3A.3-6 Message Group Meaning

The ‘Message Variant’, the most significant hexadecimal digit of the ‘Message Type’ field, is used to indicate special variants of the message. Normally it is set to zero and this leading hexadecimal digit of the ‘Message Type’ is not printed.

A value of 1 in the ‘Message Variant’ is used to cancel a previously sent message. The previously sent message is identified by the next three hexadecimal digits of the ‘Message Type’ field. This allows the DLP to cancel a previously sent Control & Status message that has a future start time, by setting the ‘Message Variant’ to 1 and re-sending the message to the SNC. If the message is still waiting to be processed in the SNC, the message will be deleted.

A value of 2 in the ‘Message Variant’ allows the SNC to send back to the DLP any previously sent Control & Status message that has a future start time and is still waiting to be processed in the SNC, in response to a ‘DLP Request Management Info’ (312h) message with the List Queued Messages Flag set. The uses of the message variants are shown in [Figure 3A.3-7](#).

A value of 4 in the ‘Message Variant’ allows the SNC to send back to the DLP the requested message, in response to a ‘DLP Request Management Info’ (312h) message with the Control & Status Message Flag set. The [\[DLP-SNC IDD\]](#) defines which messages can be requested.

Message Variant	Usage
0	Normal Message Usage
1	Message Cancellation
2	Queued Message Output
3	Unused
4	Requested C&S Message
5-7	Unused
8	Reserved for internal usage
9-F _{Hex}	Unused

Figure 3A.3-7 Message Variant Usage

3A.3.4 Tactical Interface

The Tactical Interface is used to exchange, and to control the exchange of, Tactical Messages as defined in [STANAG 5522]. The SNC does not interpret the Tactical Messages that are sent across this interface. They are treated as sealed envelopes. The Tactical Messages are encapsulated within messages exchanged over the Tactical Interface, which are called Tactical Interface messages.

Details of the tactical interface protocols are included in section 3C.2 DLP TSR Management. The messages used on the tactical interface are listed in the Figure 3A.3-8.

Msg	Message Name (DLP-to-SNC)	Msg	Message Name (SNC-to-DLP)
101h	Transmission Service Request	201h	Message Preparation Request
102h	Transmission Service Request with Data	202h	Transmission Completed
103h	Cancel Service Request	203h	SNC Cannot Comply
104h	DLP Cannot Comply	204h	Confirm Cancellation
105h	Preparation Request Response	205h	Acknowledgement
106h	Priority Change Request	206h	Tactical Messages Available
107h	Ready to Receive	207h	Received Tactical Messages

Figure 3A.3-8 Tactical Interface Messages between DLP and SNC

3A.3.5 Control and Status Interface

The Control and Status Interface is used by the DLP for the management of the SNC, which is accomplished by sending control messages and the receipt of status messages.

The SNC responds to valid control messages with either a defined message or where there is not a defined response message, the 'SNC C&S Acknowledgement' (421h) message is used by the SNC to inform the DLP that its message has been received and to inform the DLP of the outcome of its processing. The 'SNC C&S Acknowledgement' (421h) message can also be used to inform the DLP that a message it sent to the SNC on the Control and Status Interface cannot be processed. Use of the 'SNC C&S Acknowledgement' (421h) message to report a negative outcome to the DLP can be applied to any message that is sent to the SNC on the Control and Status Interface.

If an expected 'SNC C&S Acknowledgement' (421h) message is not received by the DLP within 5 seconds, or the 'SNC C&S Acknowledgement' (421h) message indicates that a message from the DLP has not been processed, corrective action must be taken by the DLP. The messages used on the Control & Status (C&S) interface are listed in [Figure 3A.3-9](#) and [Figure 3A.3-10](#).

Msg	Message Name (DLP-to-SNC)	Msg	Message Name (DLP-to-SNC)
301h	MPT Specification	31Dh	Relay Flow Response
302h	LLC LAN Configuration Request	31Fh	NILE Address Allocation Request
303h	LLC Port Configuration Request	320h	Key-Rollover Request
304h	Link 22 Super Network Participants	321h	Key-Zeroization Request
305h	Super Network Special Duties	322h	LLC Status Request
306h	Network Parameters (SNC NCS)	323h	LLC Error Report Request
307h	Network Parameters (Probing)	324h	LLC Alarm Report Request
308h	Radio Silence	325h	Continue Processing
30Bh	Operational NCS Request	326h	Clear Requests
30Ch	NCS Acknowledgement	327h	Network Late Initialization Request
30Dh	DLP NCS Description	328h	Link Quality Status
30Eh	Network Parameters (DLP NCS)	329h	Network Reconfiguration Request (SNC NCS)
30Fh	Change Media Parameters	32Ah	Insert LNE Slot
310h	Network Reconfiguration Request (DLP NCS)	32Bh	Remove LNE Slot
311h	DLP DTDMA Change	32Ch	SNC Initialization Complete
312h	DLP Request Management Info	32Dh	SPC Radio Power Request
313h	Create MASN	32Eh	Notify SN Directory
314h	Modify MASN	32Fh	NU Status
315h	Delete MASN	330h	SN Directory Update
316h	DLP LNE Request	331h	Role Takeover Control
317h	DLP LNE Response	332h	DLP NU Performance Data
318h	Transmission Capacity Response	333h	Order
319h	Stop Communication	334h	Order Compliance
31Ah	NU Leave	335h	Function Management Setup
31Bh	Role Change	336h	DLP OLM Checksum
31Ch	Change Relay Settings		

Figure 3A.3-9 Management Messages from DLP-to-SNC

Msg	Message Name (SNC-to-DLP)	Msg	Message Name (SNC-to-DLP)
401h	Probing Results	418h	Relay Setting Change
402h	End of Probing	419h	Relay Flow Control
403h	Received Network Parameters (Probing)	41Ch	Key-Rollover Response
404h	SNC NCS Description	41Dh	Key-Zeroization Response
405h	Media Parameters	41Eh	LLC Status Response
407h	Link Participants	41Fh	LLC Alarm Report Response
408h	SNC LNE Request	420h	LLC Error Report Response
409h	LNE Status	421h	SNC C&S Acknowledgement
40Ah	LNE Failure	422h	Network Initialization Complete
40Bh	Transmission Capacity Request	423h	MASN Creation
40Ch	Communication Terminated	424h	MASN Modification
40Dh	Role Status	425h	MASN Deletion
40Eh	SNC DTDMA Change	426h	Radio Power Management Request
40Fh	NILE Address Allocated	427h	NU Performance Data
410h	NILE Address Availability	428h	Received Order
411h	Acknowledgement Response	429h	Received Order Compliance
412h	Permanent Reallocation	42Ah	Received Network Parameters (SNC NCS)
413h	SNC Status	42Bh	Received Notification
414h	NU Status Changed	42Ch	TOD Status
415h	SNC Network Reconfiguration	42Dh	Network Information
416h	Received Network Parameters (DLP NCS)	42Eh	Network Congestion Indexes
417h	SPC Radio Power Response	42Fh	NU Capabilities

Figure 3A.3-10 Management Messages from SNC-to-DLP

The monitoring messages and when they are sent by the SNC to the DLP; are listed in [Figure 3A.3-11](#).

Msg	Message Name (SNC-to-DLP)	When Sent
601h	Channel Utilization	For each of the NU's transmission timeslots
602h	Connectivity Information (LRQ)	Upon Request by the DLP
603h	Congestion Alert	Once per NCT for each network
604h	Error Rate Characteristics	Once per NCT for each network
605h	DTDMA Participation	10 NCT for each network with DTDMA enabled
606h	NU Data	Every 60 seconds
607h	Connectivity Information (LCD)	Upon Request by the DLP

Figure 3A.3-11 Monitoring messages from SNC-to-DLP

Fault messages, listed in [Figure 3A.3-12](#), are sent by the SNC to the DLP when error events occur.

Msg	Message Name (SNC-to-DLP)	Msg	Message Name (SNC-to-DLP)
801h	SPC Configuration Failure	807h	LLC Disabled
802h	Built in Test	80Ah	Media Interface Congestion
803h	SPC Disabled	80Bh	LLC Configuration Failure
804h	Timeslot Violation	80Eh	SNC NP Rejection Error
806h	LLC Alarm/Error Report	80Fh	SPC Alarm/Error Report

Figure 3A.3-12 Fault messages from SNC-to-DLP

3A.4 SNC

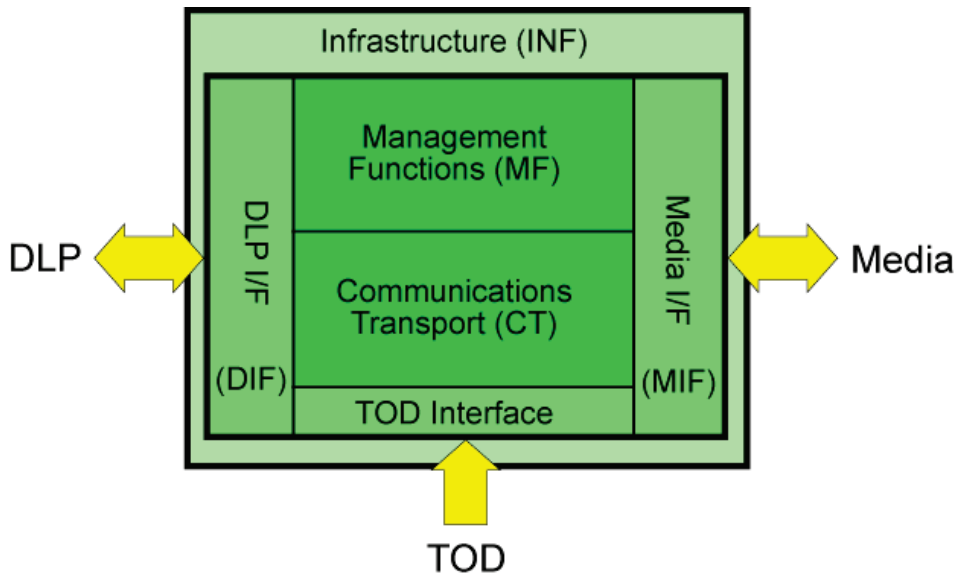


Figure 3A.4-1 SNC Functional Architecture

The System Network Controller (SNC) is divided into three major functional areas and three interfaces, as shown in [Figure 3A.4-1](#).

These six components consist of one or more software units. [Figure 3A.4-2](#) shows the mapping of components to software units.

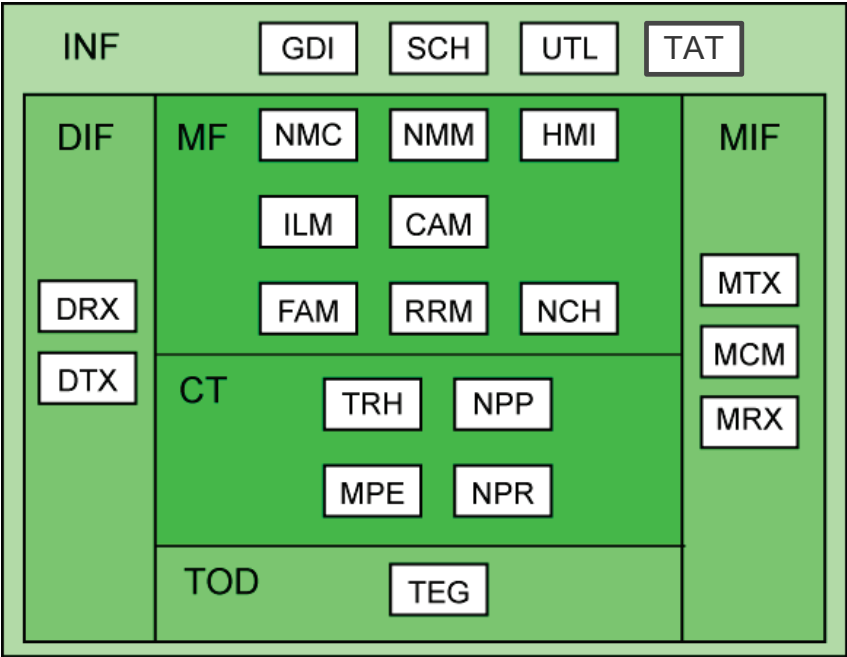


Figure 3A.4-2 SNC Components to Software Unit Mapping

Figure 3A.4-3 lists the software unit abbreviations in alphabetical order, with their full name and which component they are part of.

Abbreviation	Full Name	Component
CAM	Congestion Assessment Management	MF
DRX	DLP Interface Reception	DIF
DTX	DLP Interface Transmission	DIF
FAM	Fault Management	MF
GDI	Global Data and Initialization	INF
HMI	Human Machine Interface	MF
ILM	Initialization, LNE and Configuration Management	MF
MCM	Media Control and Management	MIF
MPE	Message Packet Expansion	CT
MRX	Media Reception	MIF
MTX	Media Transmission	MIF
NCH	NCS Handler	MF
NMC	Network Management and Control	MF
NMM	Network and Monitoring Management	MF
NPP	Network Packet Production	CT
NPR	Network Packet Reception	CT
RRM	Relay and Routing Management	MF
SCH	Scheduler	INF
TAT	TCP/IP Active Tap	TAT
TEG	Timing Event Generator	TOD
TRH	Transmission Request Handler	CT
UTL	Utilities	INF

Figure 3A.4-3 Alphabetical List of Software Units

The six components listed below are described in the following sub-sections.

- Communications Transport
- Management Function
- Infrastructure
- DLP Interface
- Media Interface
- Time of Day Interface

3A.4.1 Communications Transport

The Communications Transport (CT) function provides the Message Delivery service of the SNC. It performs this service by the communication of Network Packets between SNCs. The Communications Transport function controls the transmission and reception of the Network Packets on Link 22, accessing the media using the Media Interface (MIF). The software units communicate with the other parts of the SNC via messages using the Infrastructure message passing utility function. The main components of CT are the software units and Major Data Structures which can be seen in [Figure 3A.4-4](#). This figure also shows a diagrammatic representation of the major message flows between the software units of CT, and the major data structures.

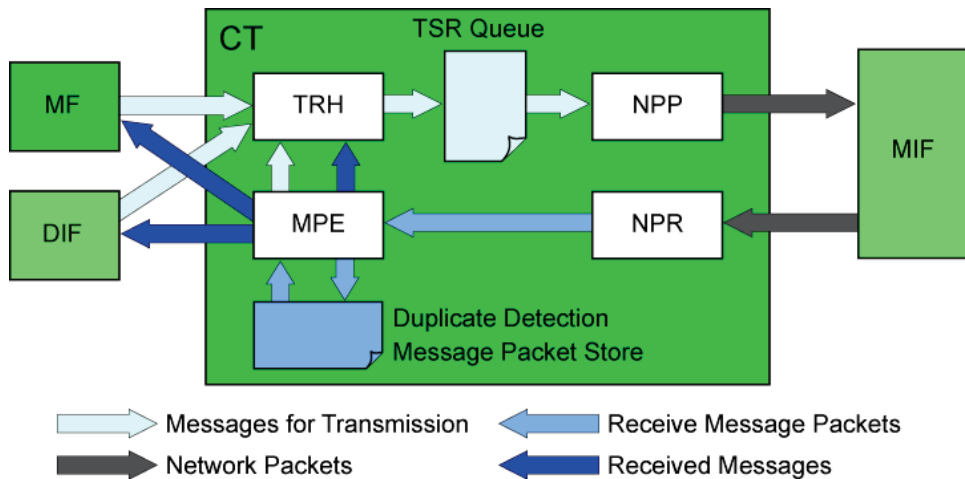


Figure 3A.4-4 Major Message Flows of CT Software Units

As shown in [Figure 3A.4-4](#), the Communications Transport function is composed of the following major components.

- Transmission Request Handler (TRH)
- Network Packet Production (NPP)
- Network Packet Reception (NPR)
- Message Packet Expansion (MPE)
- Transmission Service Request (TSR) Queue
- Duplicate Detection Message Packet Store

□ ***Transmission Request Handler (TRH)***

TRH receives all Transmission Service Requests (TSR) and their associated message data and stores them in the TSR Queue. It receives Tactical Messages for transmission from the DLP via the DLP Interface (DIF). It receives Technical Messages for transmission from the Management Function (MF). It receives Acknowledgement Messages for transmission from the MPE software unit. TRH also controls all of the transmission protocols (such as Guaranteed Delivery or Machine Receipt).

□ ***Network Packet Production (NPP)***

NPP packs the messages from the TSR Queue into Message Packets, which are packed into one or more Network Packets for transmission via MIF. Routing information is provided to NPP from the MF software unit RRM. When the transmission time is approaching, messages are selected via a packing algorithm that determines an efficient fit of the available messages. The data for the selected messages is then requested from the message source if necessary. The supplied data will be stored in the TSR Queue by TRH. Just before transmission time NPP recalculates the packing based on the messages in the TSR Queue that have data available. It then packs the messages into Message Packets, into Leg Injection Packets and finally into Network Packets for transmission via the Media Interface.

□ ***Network Packet Reception (NPR)***

NPR parses all received Network Packets from MIF and discards any with invalid structure. It unpacks valid Network Packets into Leg Injection Packets and then into Message Packets, which may include re-building Message Packets from fragments. NPR then sends the Message Packets to Message Packet Expansion (MPE).

□ ***Message Packet Expansion (MPE)***

MPE processes all the received Message Packets from NPR, discarding duplicates, extracting the messages from the Message Packets and delivers them to the required destination. Received Tactical Messages are sent to the DLP via DIF. Received Technical Messages are queued to the destination software unit in MF. Received messages that contain acknowledgements are sent to TRH. MPE may also need to transmit acknowledgement messages which it does by requesting transmission from TRH.

□ ***Transmission Service Request (TSR) Queue***

The TSR Queue is used by TRH software unit to store TSRs from both the DLP and internally by other software units in the SNC. It consists of the information about the TSR, the contents of TSR and the contents of the message requested to be transmitted. It also consists of access mechanisms that allow fast and easy access to the TSRs and provide the priority ordering. Refer to section [3C.3 SNC TSR Queue](#) for details of this data structure.

□ ***Duplicate Detection Message Packet Store***

The duplicate detection message packet store data structure is used by MPE to store information about message packets it has already received and their contents, so that it can detect whether a received message packet has previously been received. Refer to section [3C.6.1 Message Packet Store](#) for details of this data structure.

3A.4.2 Management Function

The Management Function (MF) of the SNC is composed of the software units shown below. The software units can communicate with other parts of MF or the SNC by using the message passing utilities provided by the Infrastructure. Some of the software units provide services to others or are relatively self-contained with only minor interaction with others. The major architectural components (software units and data structures) of the Management Function are shown in [Figure 3A.4-5](#).

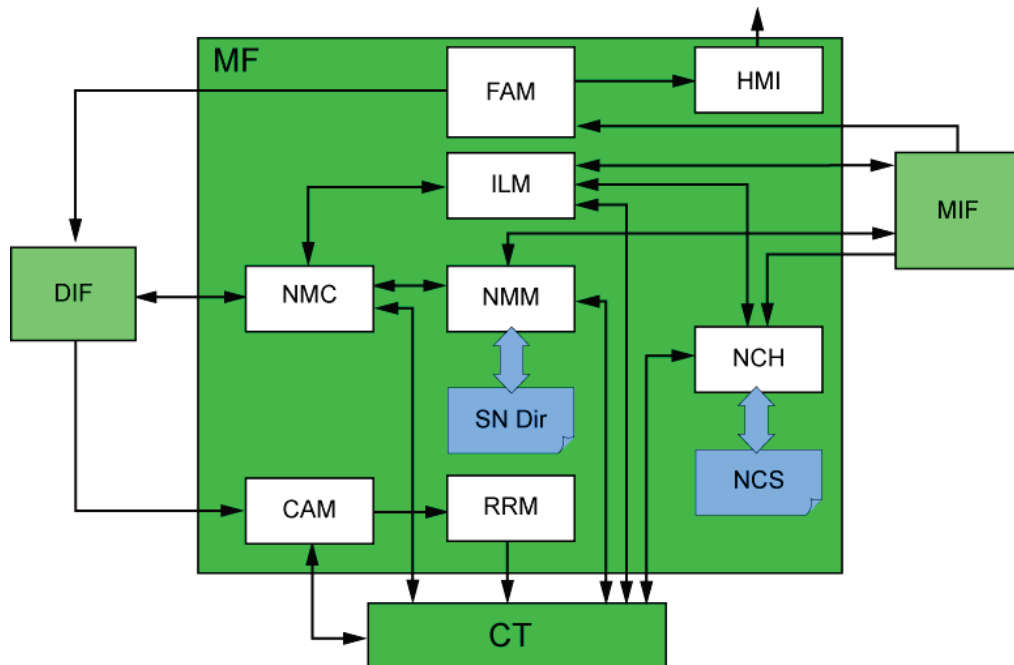


Figure 3A.4-5 Management Function Software Unit Decomposition

The following lists the major components of the Management Function, as shown in Figure 3A.4-5.

- Congestion Assessment Management (CAM)
- Fault Management (FAM)
- Initialization, LNE and Configuration Management (ILM)
- NCS Handler (NCH)
- Network Management and Control (NMC)
- Network and Monitoring Management (NMM)
- Relay and Routing Management (RRM)
- Human Machine Interface (HMI)
- Super Network Directory
- Network Cycle Structure (NCS)

□ Congestion Assessment Management (CAM)

CAM maintains information on the congestion in each NILE network, and distributes this information using Technical Messages. It maintains information about congestion of other NUs from the technical messages that it receives. It also manages the DTDMA protocol and the activation of the Relay Flow Control protocols.

□ Fault Management (FAM)

The Fault Management software unit performs the Built-In-Test (BIT) procedure when activated and then it performs the same procedure periodically. The results of the BIT are provided to the DLP, and to the HMI software unit. Any alarm and error messages generated by the Media Segment are processed and sent to the DLP, when detected or when requested from the DLP. Upon request from the DLP, FAM requests the LLC Status from the Media Segment and returns it to the DLP. It also sends to the DLP the Media Segment Congestion value received from MIF.

□ Initialization, LNE and Configuration Management (ILM)

The Initialization, LNE and Configuration Management (ILM) software unit manages the initialization of a NILE Unit. ILM also manages the closedown of a NILE Unit, in a NILE Network or in the Super Network, or the closedown of an entire NILE Network or of the entire Super Network. ILM also performs the LNE protocol and manages the re-initialization and the reconfiguration of a NILE Network.

□ ***NCS Handler (NCH)***

For each connected NILE Network the NCH maintains the current Operational NCS. An NCS is defined as a number of timeslots with their size in minislots and their owner NILE Address. NCH stores the NCS that it receives (during initialization, re-initialization and reconfiguration), or computes a new NCS when instructed to do so. During LNE NCH controls the ONCS used during the various phases of the protocol. NCH also modifies the ONCS during DTDMA. NCH maintains two copies of the ONCS, the baseline and the current. The baseline ONCS is the one generated during initialization or changes. When requested, the NMU will distribute the baseline ONCS. The current ONCS is updated based on received traffic due to, for example, temporary DTDMA reallocations.

□ ***Network Management and Control (NMC)***

The Network Management Control (NMC) software unit manages the Network Management messages received from and sent to the DLP (via DIF). It controls the transmission and reception of the technical messages associated with the Network Management orders, and handles the associated protocols. It passes the implementation of the management functions to either ILM or NMM. It controls the operation of the ‘Automatically Comply’ and the ‘Automatically Perform Function’ switches. It also performs the queuing of requests that are more than 20 minutes in the future.

□ ***Network and Monitoring Management (NMM)***

The Network and Monitoring Management (NMM) software unit performs the SNC Initialization. During this phase NMM receives from the DLP Interface, the messages to connect and configure the Media Segment, which it sends to the Media Interface. When it receives the connection and configuration status for all the connected LLC it sends the data to the DLP (via DIF). It maintains the SN Directory based on information received from the DLP or received via Technical Messages. NMM sends received directory updates to the DLP or transmits updates to others SNC via technical messages.

□ ***Relay and Routing Management (RRM)***

The Relay and Routine Management (RRM) software unit collects and dispatches reception quality and connectivity information and supports both the routing and relay of Message Packets. To do this RRM maintains information on the connectivity between the NUs based on the quality of the link information that it receives. Based

on the connectivity and congestion information RRM controls the routing and relay of messages within the system by providing the data to CT.

□ ***Human Machine Interface (HMI)***

The HMI software unit is not necessary to the operation of the SNC, and so can be ignored. It can be used to output some very basic status information, and has no input capability. It is provided in the architecture so that if a particular implementation of an SNC wanted some hardware specific status indicators then the software to provide the facility would be in an isolated software unit.

□ ***Super Network Directory***

The SN Directory data structure contains all the information about the Link 22 Super Network. This data structure contains the following information.

- NILE Unit's Link 22 Address
- Address Component
- MASN Component
- Status Component
- Role Component
- NILE Network Information

□ ***Network Cycle Structure (NCS)***

The NCS Data structure contains all the information about the Operational NCS for each Network in which the unit is a member.

3A.4.3 Infrastructure

The Infrastructure (INF) component provides the environment for the other components to operate in. The Infrastructure component is composed of the following software units.

- Scheduler (SCH)
- Global Data and Initialization (GDI)
- Utilities (UTL)
- TCP/IP Active Tap (TAT)

□ Scheduler (SCH)

The Scheduler (SCH) is the top-level procedure of the SNC. The Scheduler performs the initialization of the SNC by using the GDI function. After initialization the scheduler controls how and when the processing procedures that make up the system are run. It does this by looping and continually checking for timed events and then scheduling the software units for execution. If there are any timed events on the timer queue (messages scheduled for delivery at a specified time) that are due, the message is taken off the timer queue and added to the appropriate priority destination queue. The Scheduler then finds the highest priority message to be processed, and calls the software unit that processes that message. Each message is processed to completion before control is returned to the scheduler. This ensures that the most important message is processed first. If there are no messages to process, the scheduler performs idle processing, before going around the loop again. This is shown in [Figure 3A.4-6](#).

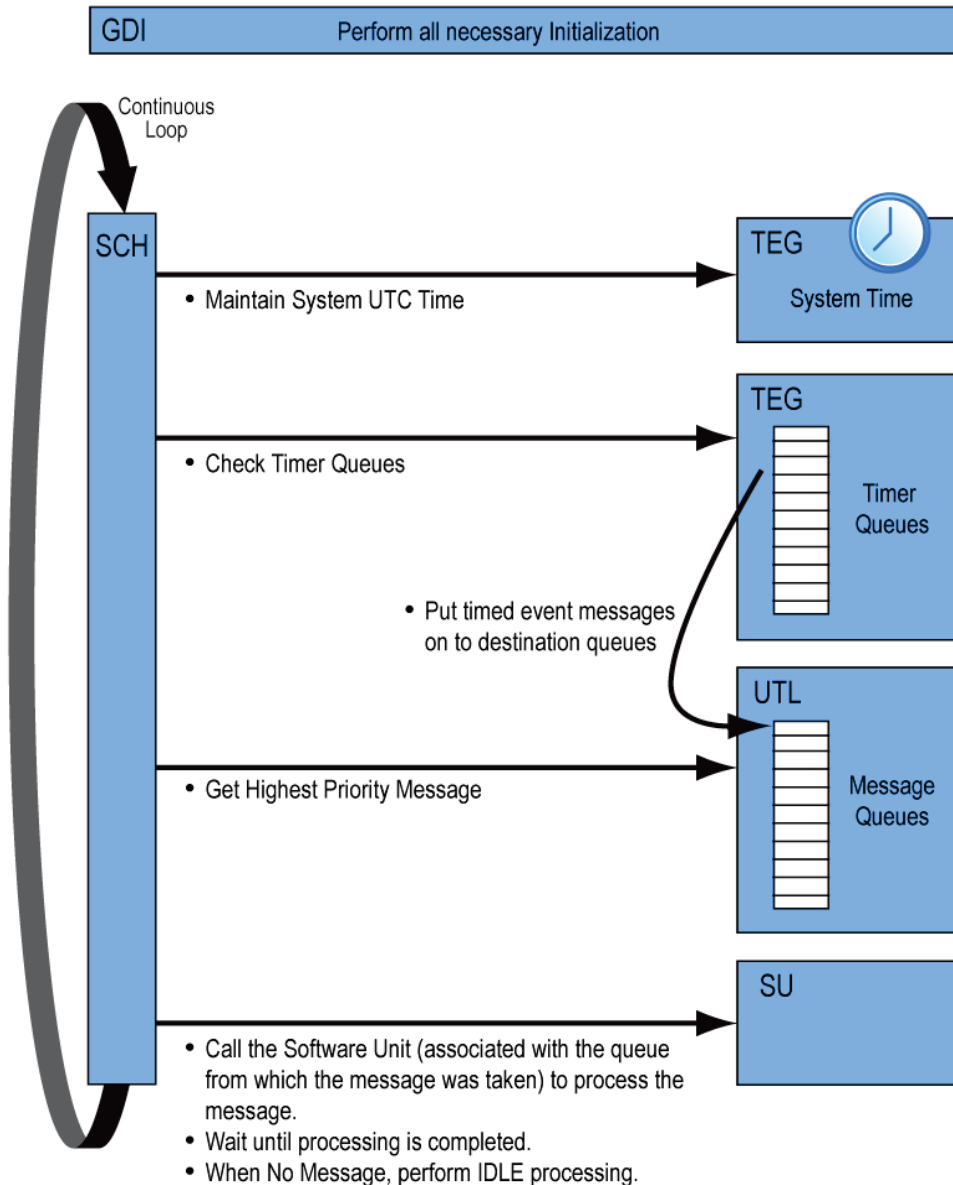


Figure 3A.4-6 Scheduler Operation

□ ***Global Data and Initialization (GDI)***

The Global Data and Initialization (GDI) function is responsible for initializing the SNC in the correct order. Global Data and Initialization calls the initialization procedures of the software within the SNC in the correct order to ensure that the initialization of dependent data structures occurs correctly. The last initialization is of the DLP interface, thereby allowing the DLP to connect to the SNC via TCP/IP.

□ ***Utilities (UTL)***

The Utilities (UTL) are a collection of general purpose software that can be called by any other software within the SNC. Utilities avoid duplicating code within the various SNC sub-functions and isolates code that has hardware or operating system dependencies, to enable easier portability of the code. The functions provided by Utilities are listed below.

- Message Passing
- Optimized Data Handling
 - Field Swap
 - Network Format
 - Byte Order
 - Modular Time Functions
- Platform Dependent Procedures
 - TCP Communications
 - Shared Memory
 - System Clock
- Error Logging

The most important function of Utilities is the message passing mechanism used for the internal communication within the SNC and so some additional information is provided.

The Message Passing utility provides a set of procedures that are used to manipulate the internal message queues. Each software unit that receives internal messages has a high and low priority queue. The order of priority of the queues is set so that the most important software units get to process their messages first. There is also a free queue that contains the unused elements of the queues. A separate data structure holds the message data, which is divided into small, medium and large message sizes. There are more small messages than large and so this reduces the memory used. The queues are implemented by chaining the message queue records together, using a field in the

records. All information about the message is stored in the message queue record and the actual message is stored in a storage array. This can be seen in [Figure 3A.4-7](#). Associated with the data structure are pointers to the top and bottom of every message queue and the free queue.

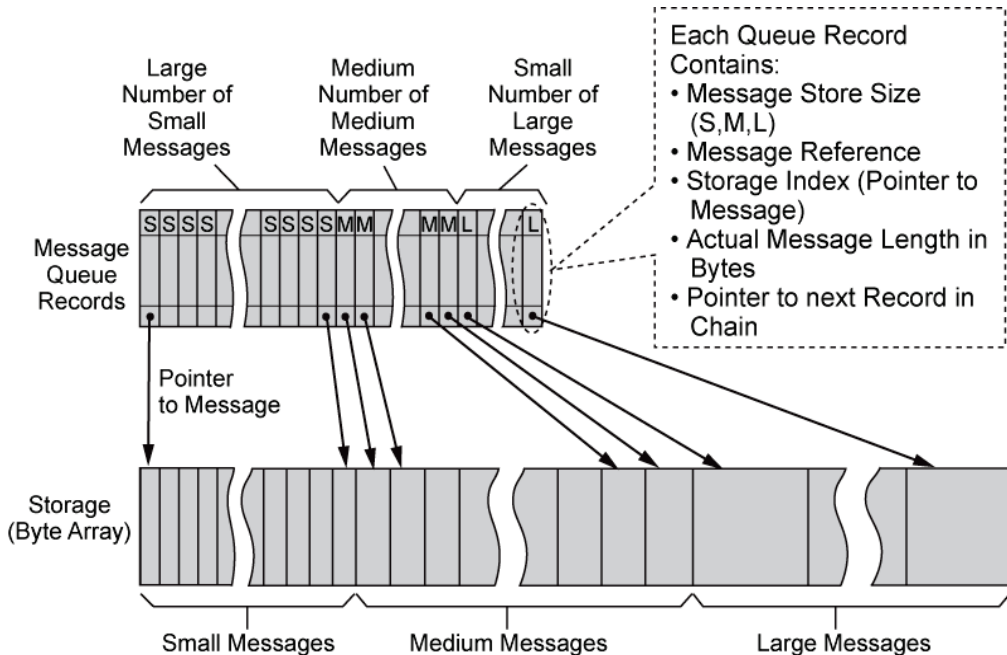


Figure 3A.4-7 Message Queue Data Structure

□ TCP/IP Active Tap (TAT)

The TCP/IP Active Tap (TAT) consists of utilities for actively tapping the TCP/IP interfaces within the SNC. The DLP Interface (DIF) and the Media Interface (MIF) can be configured to call the tapping function whenever they receive or transmit a message on their TCP/IP interface. The tapped messages are then sent via a TCP/IP connection to an external message logging application, in a format compatible with the NRS SG Extractor program. The `snc.ini` file defines whether the SNC active tapping is enabled (default is disabled), and the IP address and Port of the logging application. It also controls whether remote control of the active tapping is enabled via UDP messages, and the UDP port number for the remote control messages. It also specifies initially whether tapping is enabled or disabled for DIF and MIF.

3A.4.4 DLP Interface

The DLP Interface (DIF) component is composed of the following software units.

- DLP Interface Reception (DRX)
- DLP Interface Transmission (DTX)

DRX receives messages from the DLP-to-SNC interface converts them to internal format and passes them to the Infrastructure message passing function for delivery to the software unit that will process the message. DRX is also responsible for handling of TCP/IP connection requests from the DLP.

DTX receives messages from the internal SNC functions via the Infrastructure message passing function, converts them to external format, and sends them to the DLP.

3A.4.5 Media Interface

The Media Interface (MIF) component is composed of the following software units.

- Media Control and Management (MCM)
- Media Reception (MRX)
- Media Transmission (MTX)

MCM is responsible for handling of the TCP/IP connection requests to the LLCs, and controls the operation of the media interface.

MRX receives messages from the SNC-to-LLC interface converts them to internal format and passes them to the Infrastructure message passing function for delivery to the software unit that will process the message.

MTX receives messages from the internal SNC functions via the Infrastructure message passing function, converts them to external format, and sends them to the LLC.

3A.4.6 Time of Day Interface

The TOD Interface component is composed of a single software unit called the Timing Event Generator (TEG). It is responsible for reading the TOD input and provides all of the timing mechanisms within the SNC. It does this by maintaining timing queues where internal messages can be stored until the specified time before being delivered for scheduling.

3A.5 SNC-to-LLC Interface

The SNC-to-LLC Interface enables the exchange of red (unencrypted) data between the SNC and LLC components. A single SNC can communicate with up to four LLCs. The interface also provides a means for the SNC to communicate with up to four SPCs, through the LLCs. The SNC-to-LLC Interface is fully defined in the [LLC IRS].

The SNC-to-LLC Interface carries red data to be transmitted, red data that has been received, and control and management information for the different media.

3A.5.1 Physical Interface

The SNC interfaces with at least one, but optionally up to four LLCs, as shown in Figure 3A.5-1.

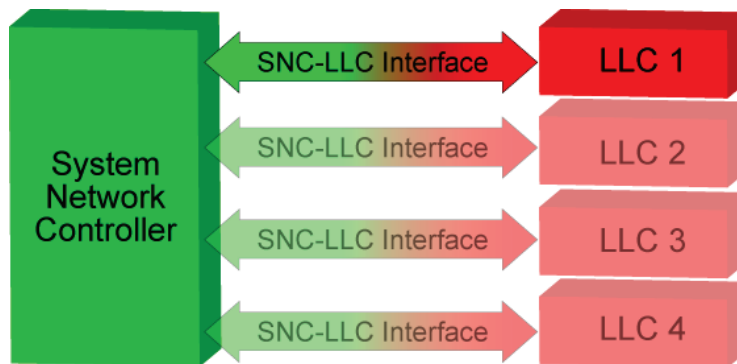


Figure 3A.5-1 Physical Interface between SNC and LLCs

Each SNC-to-LLC Interface uses TCP/IP over an Ethernet LAN connection (ANSI/IEEE 802.3 or ISO 8802/3). The current LLC has a 10/100 Mbps Ethernet interface. The use of the faster speed is recommended as it reduces the latency across the interface.

The SNC-to-LLC Interface is replicated for each LLC that is connected to a single SNC. Replication of the SNC-to-LLC Interface can be performed functionally and logically over a common LAN, or through physical replication with the use of separate LAN controllers on the SNC for each LLC.

3A.5.2 Functional Interface

The SNC-to-LLC Interface contains one functional interface, as shown below. However, every message contains three main parts (partitions), which are associated with the three LLC functions; Crypto Control, Bypass, and Data Encryption, as shown in [Figure 3A.5-2](#). All three partitions exist in a message, although a partition may be empty.

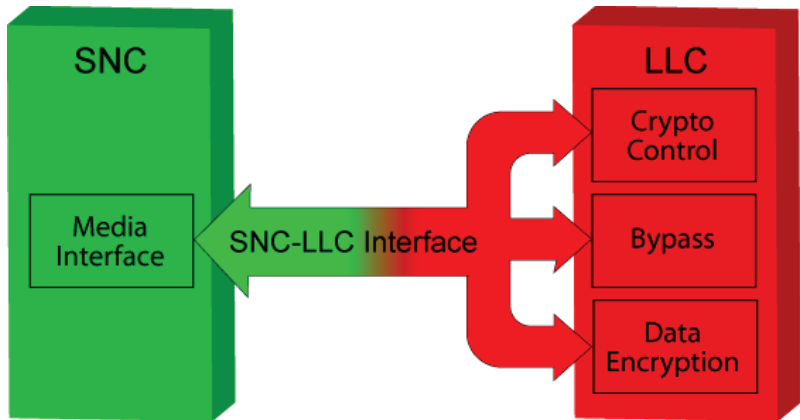


Figure 3A.5-2 Functional Interface between SNC and LLCs

3A.5.3 Message Definition

TCP/IP provides a serial byte stream at the application level. This byte stream contains the SNC-to-LLC Interface messages, which are defined by their structure and content. An SNC-to-LLC Interface message consists of a Socket Header and a Serial Interface Message, the fields of which are shown in [Figure 3A.5-3](#).

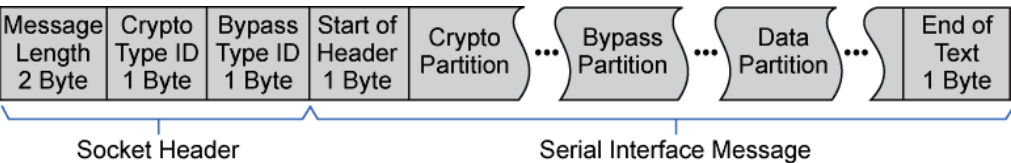


Figure 3A.5-3 SNC-to-LLC Interface Message Structure

The following applies to the fields of the Socket Header.

- The Message Length field contains length in bytes of the serial interface message

- The Crypto Type Identifier contains the Crypto Message Type ID field of the Crypto Partition of the serial interface message
- The Bypass Type Identifier contains the Bypass Message Type ID field of the Bypass Partition of the serial interface message

The format for the Serial Interface messages consists of five parts.

- Start of Header, a byte set to 01 Hex
- Crypto Partition, which contains the message information used to control the LLC, or the response from the LLC
- Bypass Partition, which contains the message information for the control of the SPC or the status information from the SPC
- Data Partition, which contains the unencrypted (RED) data (NPs) to be transmitted, or that has been received
- End of Text, a byte set to 03 Hex

The SNC-to-LLC interface communications on the LAN use ‘Big Endian’ byte format, which is ‘Network Standard’ order.

□ **General Format of the Partitions**

The general format of all three partitions (crypto, bypass, and data partitions) is shown in [Figure 3A.5-4](#).

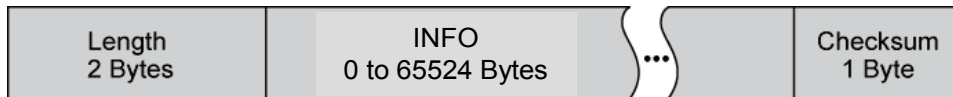


Figure 3A.5-4 General Format of Message Partitions

Each partition consists of 3 fields as listed below.

- Length field, specifying the size of the INFO field in bytes
- INFO field, variable integer number of bytes (0-1981), containing the message data
- Checksum, used for error detection, which is the result of an exclusive OR on the Length field and the INFO field on a byte basis

The minimum size of a partition will be 3 bytes, because when there is no information in the partition (zero length <INFO> field) there are two bytes for the <Length> field (set to zero) and 1 byte for the <Checksum> field (set to zero). This is called a **Null Partition** (three zero bytes) and is used whenever a partition is not part of the message (for example, all Crypto Partitions on the LLC-to-SPC Interface are Null Partitions).

❑ **Crypto Partition**

The Crypto partition contains control information for the LLC and has the format as shown in [Figure 3A.5-5](#).

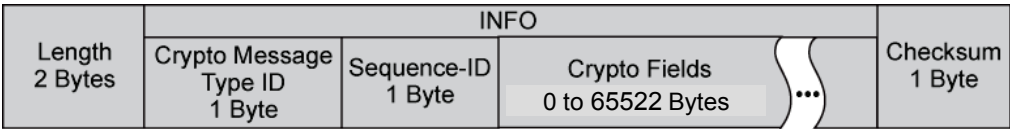


Figure 3A.5-5 Crypto Partition Format

The <Crypto Message Type ID> field indicates what message type information is in the <Crypto Fields>. The <Sequence-ID> field contains the Sequence Identifier which is used to bind requests and responses, as discussed in [Chapter 3 Section C](#). The <Crypto Fields> field is variable in length depending on which Crypto Message Type it contains and the information within the message.

❑ **Bypass Partition**

The Bypass partition contains information to be passed to, or received from, the SPC. The Bypass Partition has the format as shown in [Figure 3A.5-6](#).

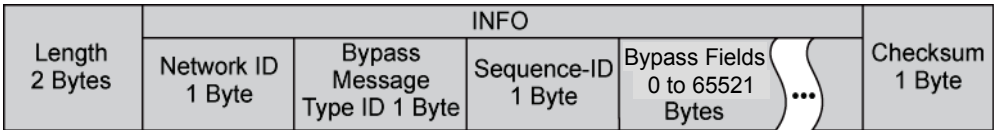


Figure 3A.5-6 Bypass Partition Format

The <Network ID> field indicates to the LLC, the SPC to which the bypass information is addressed. In a multi-network environment, the LLC uses the Network ID to determine the SPC to which it must deliver the message. For messages sent by an SPC to the SNC, the <Network ID> field indicates to the SNC which SPC generated the message. The <Bypass Message Type ID> field indicates the kind of information found in the <Bypass Fields> field. The <Sequence-ID> field contains the Sequence Identifier which is used to bind requests with responses that form a single transaction. The <Bypass Fields> is variable in length depending on which Bypass Message Type it contains and the information within the message.

□ **Data Partition**

The Data Partition is only used by the messages that contain data to be transmitted or data that has been received, and for all other messages the Data Partition is set to be the Null Partition. For those messages where the Data Partition is used (irrespective of whether it contains any data) the Null Partition is invalid, and the Data partition has the format as shown in [Figure 3A.5-7](#).

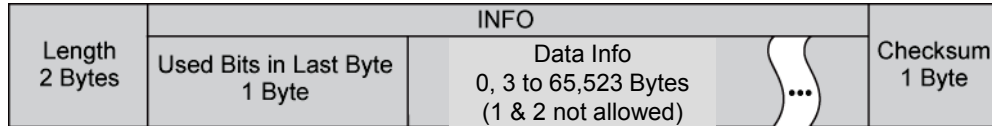


Figure 3A.5-7 Data Partition Format

Though the <Data Info> field always contains an integer number of bytes, the actual user data in the field does not have to fill all of the last byte. The <Used Bits in Last Byte> field indicates the number of user bits present in the last byte of the <Data Info> field. The remaining unused bits in the last byte of the <Data Info> field, starting with the Least Significant Bit (LSB) will be assumed to be fill bits and are set to zero.

The value of the Data Partition <Length> field is equal to the length in bytes of the <Data Info> field plus the one-byte length of the <Used Bits in Last Byte> field.

When the <Data Info> field is zero bytes (no data) the <Length> field is 1 due to the <Used Bits in Last Byte> field (field set to zero); this is called an **Empty Data Partition**, which is not the same as the Null Partition.

A <Data Info> field of length 1 or 2 is invalid. This defines the minimum length of data (when the partition contains data); 3 bytes with the last byte containing a minimum of 1 used bit, therefore defining data length as 17 bits.

3A.5.4 SNC-to-LLC Messages

The messages the SNC can send to the LLC are listed in [Figure 3A.5-8](#). The LLC sends some of the messages onto the SPC. A zero value for the crypto or bypass ID indicates that the corresponding partition is empty. Only the ‘LLC Transmit Network Packet Request’ (0303H) message uses the data partition, as described in the data partition section above. All other messages in the table set the data partition to be a null partition. For the ‘LLC Transmit Network Packet Request’ (0303H) and the ‘LLC Receive Header Request’ (0404H) messages, the LLC clears the crypto partition before sending the message to the SPC. Refer to section [3A.7.4](#) for LLC-to-SPC messages.

Message Name	Crypto: Bypass ID	Partitions			Protocol
		Crypto	Bypass	Data	
LLC Configuration Request	8100H		null	null	LLC Control
LLC Status Request	0100H		null	null	
Key Management Request	8200H		null	null	
SPC Configuration Request	00C1H	null		null	SPC Control
SPC Status Request	0001H	null		null	
SPC Transmit Header Request	0002H	null		null	Transmission
LLC Transmit Network Packet Request	0303H				
LLC Receive Header Request	0404H			null	Reception

Figure 3A.5-8 SNC-to-LLC Messages

[Figure 3A.5-8](#) and [Figure 3A.5-9](#) show for each message the partitions that are not used and which have to be set to be the null partition. Conversely where there is no null, the partition cannot be a null partition and must have the correct partition structure. The last column shows what protocol the message is part of.

3A.5.5 LLC-to-SNC Messages

The messages the LLC can send to the SNC are listed in [Figure 3A.5-9](#). Some of the messages originate from the SPC. A zero value for the crypto or bypass ID indicates that the corresponding partition is empty. Only the ‘LLC Receive Network Packet Response’ (F5F3H) message uses the data partition, as described in the data partition section above. All other messages in the table set the data partition, to be a null partition. The LLC receives the 00F3H from the SPC, and then fills the empty crypto partition before sending it to the SNC as F5F3H. Refer to section [3A.7.5](#) for SPC-to-LLC messages.

Message Name	Crypto: Bypass ID	Partitions			Protocol
		Crypto	Bypass	Data	
LLC Configuration Response	A100H		null	null	LLC Status
LLC Status Response	F100H		null	null	
Key Management Response	E200H		null	null	
LLC Error Report	FF00H		null	null	
LLC Alarm Message	BB00H		null	null	
SPC Configuration Response	00E1H	null		null	SPC Status
SPC Status Response	00F1H	null		null	
SPC Error Report	00FFH	null		null	
SPC Alarm Message	00BBH	null		null	
SPC Transmit Response	00F2H	null		null	Transmission
SPC Reject Transmit Network Packet	00D3H	null		null	
LLC Receive Network Packet Response	F5F3H				Reception
SPC Receive Response	00F4H	null		null	
SPC Receive Preamble Response	00F6H	null		null	

Figure 3A.5-9 LLC-to-SNC Messages

3A.5.6 Protocols

The protocols on the interface are detailed in section [3C.14](#) of this chapter.

3A.6 LLC

The LLC provides the interface between the SNC and SPCs. It provides communication security services at the data link level for the Link 22 System.

A single LLC can handle 4 networks of any of the currently defined media. The LLC-7M has been tested with 4 networks with a maximum of 64,000 bits per second on each network, thereby allowing for future higher bandwidth media.

The LLC hardware architecture is shown in [Figure 3A.6-1](#).

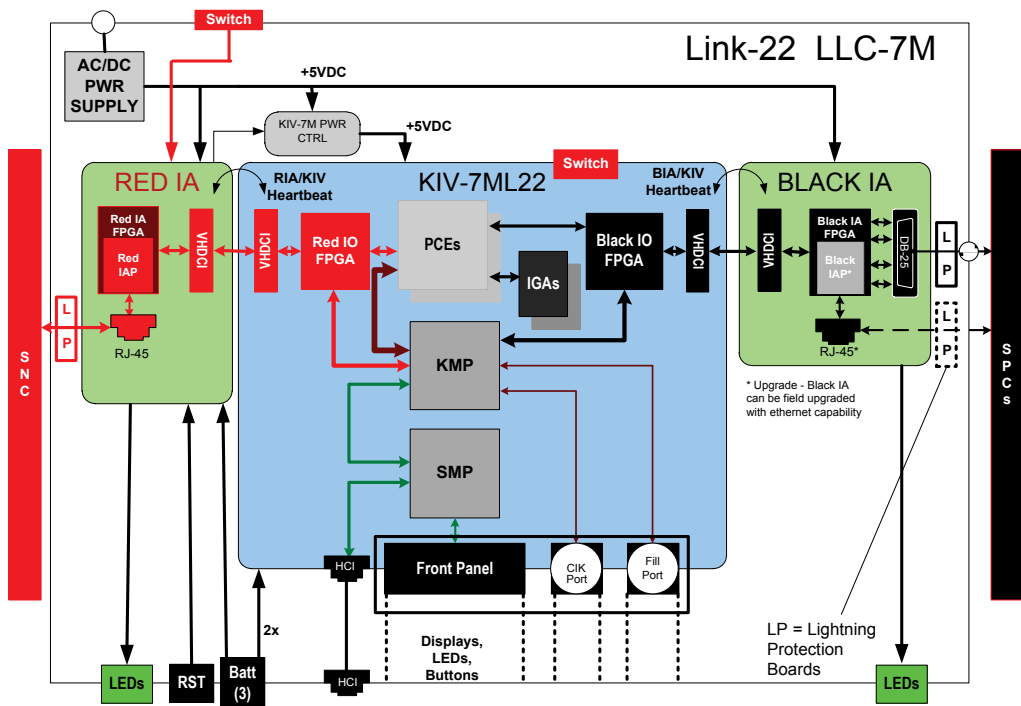


Figure 3A.6-1 LLC-7M Hardware Architecture

The SNC interfaces via Ethernet to the red side of the embedded crypto device (KIV-7M) via the Red Interface Adapter (Red IA, or RIA). The red side components are those that access unencrypted information. The SPCs interface via separate serial lines to the black side of the KIV-7M via the Black Interface Adapter (Black IA, or BIA). The black side components are those that only access encrypted information.

The KIV-7M maintains the separation between the red and black sides, by providing the data encryption/decryption function and a trusted bypass mechanism to control the SPCs. The KIV-7M is an existing hardware box that is physically located within the LLC-7M. The front panel controls of the KIV-7M are accessible through the front panel of the LLC-7M, providing the key fill port, the CIK (Crypto-Ignition Key), the status display and the input push buttons. The LLC provides separate power for the red IA, the KIV-7M and the black IA. The LLC includes batteries (a quantity of 3) which provide power backup to the LLC to retain crypto keys and system software when the primary power is removed. If the batteries fail when there is no primary power the device will be un-operational and will have to be sent back to depot to be reloaded, so maintaining good batteries is very important. The batteries should be replaced whenever the “Low Battery” Light-Emitting Diode (LED) is illuminated.

Do not change the batteries without main power being supplied or at a time when the main power may be lost while changing the batteries.

3A.6.1 Use and Operation

In general, the use and operation of the LLC is straightforward. Most configuring is automatic, and subsequent operation is dependent on the message interface with the SNC and the SPCs. When installing an LLC, the IP address of the Ethernet interface (on the "red" side) must be configured (refer to paragraph 5-4.2 of the LLC-7M Operator's Manual [LLC OPM]), and the serial interfaces (on the "black" side) must be physically connected.

Once installed, the LLC only needs to be powered on, and correct keys loaded according to the key management plan. Besides new key loading, operator interaction with the LLC is minimal. Configuration of the LLC is accomplished via the message interface with the SNC. Error messages and alarms are reported via messages back to the SNC, which in turn are reported to the DLP. Front panel indicators reflect conditions such as power connection status, no key loaded, or encryption and decryption activity. Importantly, in the case of failure or tamper, an alarm will cause illumination of the Alarm LED and zeroization of the crypto keys.

The LLC-7M external interfaces can be seen in the illustrations of the front and rear panels of the LLC shown in [Figure 3A.6-2](#) and [Figure 3A.6-4](#). The figures identify the controls, indicators, and connectors.

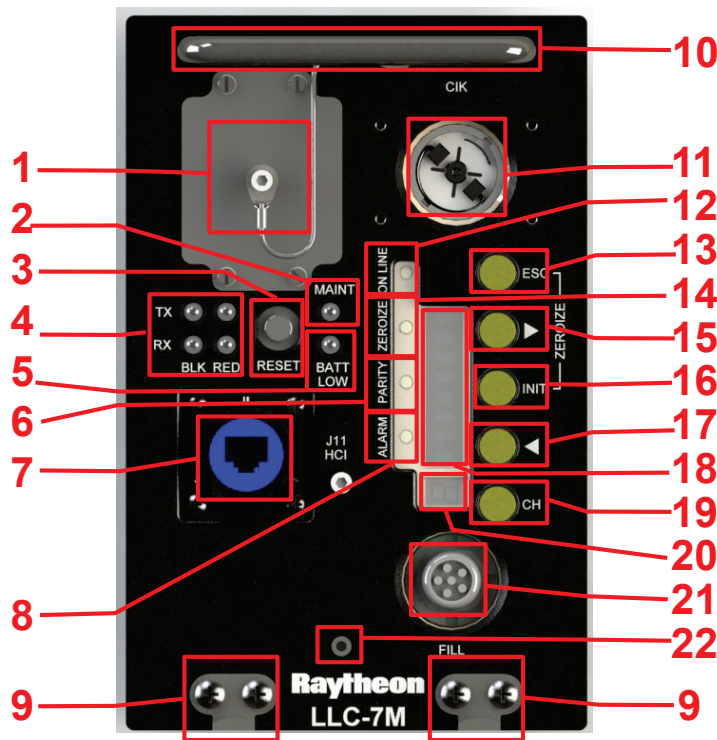


Figure 3A.6-2 LLC Front Panel

Each of the numbered items on the LLC front panel along with its name, type, and brief function is listed in [Figure 3A.6-3](#). For additional details refer to the LLC-7M Operator’s Manual [[LLC OPM](#)].

#	Name	Type	Function
1	Battery compartment		Provides access to the 3 batteries
2	MAINT Indicator	LED	When illuminated indicates that the LLC has been compromised and is no longer operational
3	RESET	Recessed Push button	A momentary pushbutton switch, which initiates a system reset of the LLC-7M regardless of channel activity and online/offline state. A system reset will terminate any connection to the SNC or SPC, which will need to be re-established once the LLC-7M completes boot up initialization and self-tests.

#	Name	Type	Function
4	Tx and Rx LEDs	4 Green LEDs	Shows Transmit and Receive in progress on both the red and black interfaces
5	BATT LOW Indicator	LED	When illuminated indicates at least one of the batteries has a low voltage and all 3 need to be replaced
6	KIV-7M Parity LED	Red LED	This red indicator lights when there is a parity error during key loading, key selection, or key transfers. The PARITY indicator turns on when a key load is initiated and turns off when the key load operation is complete, regardless of if passed or failed.
7	HCI, J11	RJ-45	Ethernet connection to a PC browser based user interface
8	KIV-7M Alarm LED	Red LED	This red indicator lights when there is an alarm condition. The indicator also blinks when alarm checks are being performed.
9	Mounting clips	Metal Hooks	Used to fasten the unit to a standard ½ Long ATR mounting tray, the fasteners on the tray attach to the hooks and the thumbscrews are tightened on the fastener to secure the unit to the tray.
10	Handle		For lifting and handling the LLC
11	Crypto-Ignition Key (CIK) receptacle	KSD4000	Permits access to the operational features of the LLC-7M when inserted and protects internally stored keys when removed. Removing and reinserting the CIK resets the LLC-7M
12	KIV-7M Online LED	Green LED	This green indicator is on when the channel is in the ONLINE state, which means that there is at least one configured port (with or without a key). When in the offline state, meaning that all four ports are de-configured, the ONLINE indicator blinks.
13	KIV-7M ESC button	Push button	Pressing and releasing the ESC button causes the LLC-7M to back up by one menu level in the menu tree. Pressing and holding the ESC button causes the LLC-7M to return to the top of the menu tree you are using. Pressing the ESC button and INIT button simultaneously initiates zeroization of all internally stored operational keys for all key banks of the LLC-7M
14	KIV-7M Zeroize LED	Red LED	This red indicator lights at any time when the system is in the zeroized state, meaning that there are no user keys (TEKs or KEKs) in the system.
15	KIV-7M ► button	Push button	Scrolls down through the command and status messages displayed in the command/status display

#	Name	Type	Function
16	KIV-7M INIT button	Push button	Selects the function or configuration menu option currently shown in the command/status display. Pressing the INIT button and ESC button simultaneously initiates zeroization of all internally stored operational keys for all key banks of the LLC-7M
17	KIV-7M ◀ button	Push button	Scrolls up through the command and status messages displayed in the command/status display
18	KIV-7M command/status display	8 Character dot matrix display	Provides information display and menus for control of the KIV-7M from the front panel push buttons
19	KIV-7M CH button	Push button	Select the channel to configure and operate
20	KIV-7M Channel Display	single seven segment alphanumeric display	The Channel display is a single character that identifies the selection made using the CH button
21	FILL	KEY FILL Connector	Six pin D circular connector for DS-101 compatible key fill device
22	Front Ground Lug		To ground the device using a copper ground strap at the front of the device

Figure 3A.6-3 LLC Front Panel Controls, Indicators, and Connectors

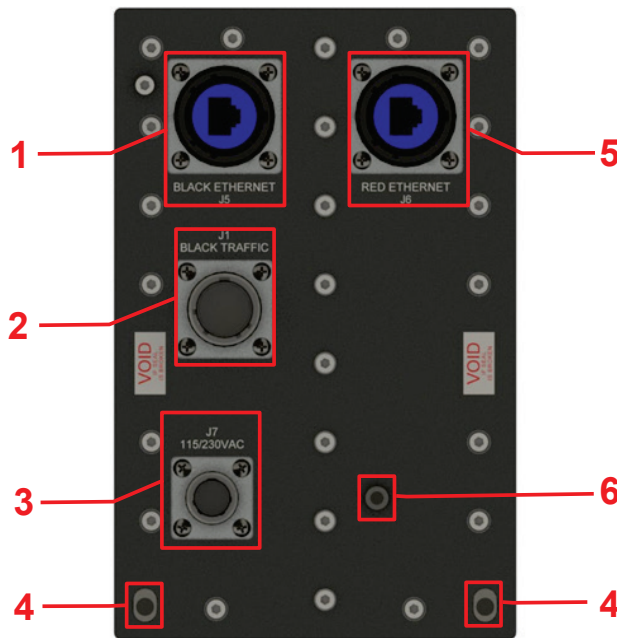


Figure 3A.6-4 LLC Rear Panel

Each of the numbered items on the LLC back panel along with its name, type, and function are listed in [Figure 3A.6-5](#).

#	Name	Type	Function
1	Black Ethernet, J5	RJ-45 (currently unused)	Possible Future (black) Ethernet Interface to SPCs
2	Black Serial Traffic, J1	MIL-DTL-38999/20WC35PN Circular Male Receptacle, Four sets of RS-422 signals	Black (encrypted) serial data to SPCs
3	Universal Power input 90/240 VAC, 50-400 Hz, J7	Male 3-pin circular crew-type pin (D38999/20WA98PN)	Power Input connector
4	Mounting indentations		Secures the device at the rear of a ½ long ATR mounting tray
5	Red Ethernet Traffic, J6	Circular Bayonet RJ-45 Socket (RJF2SA5G)	Red (unencrypted) Ethernet Connection to SNC
6	Ground Lug		To ground the device using a copper ground strap

Figure 3A.6-5 LLC Rear Panel Connectors

3A.6.2 Performance

The LLC-7M has been tested using 4 networks running at 64 Kbps. At this rate it can use the minimum possible Media Coding Frame (MCF) duration of 5.5ms using NP sizes of 352 bits, with both small timeslot size and maximum size timeslots, with and without LLC Integrity. A reception transaction requires 3 messages plus a message for each NP. So the worst case is for a minimum size timeslot of 4 minislots (preamble + 3 NPs), requires 6 messages; which for 5.5ms MCF duration is 1090 messages per second per network. The LLC processes any received transmission requests before processing reception requests. The LLC can handle on the serial interface sustained data rates of up to 460.8 Kbps on all four channels for an aggregate serial rate of 1,843.2 Kbps.

3A.6.3 Information Flow through the LLC

The SNC-to-LLC and the LLC-to-SPC functional interfaces are shown in Figure 3A.6-6.

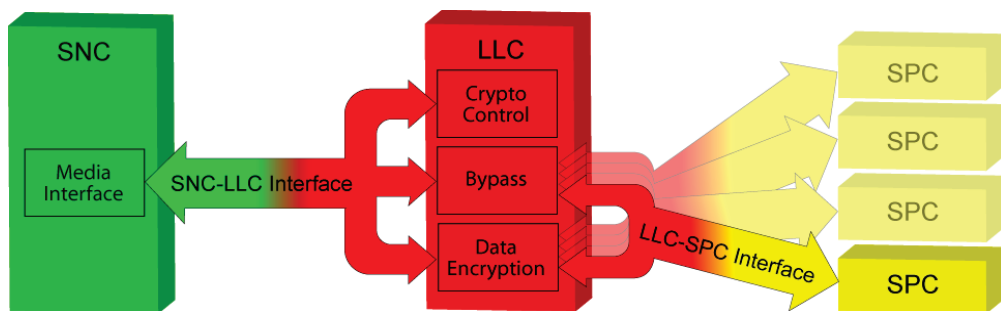


Figure 3A.6-6 Functional Interface between SNC, LLC, and SPC

The LLC's Crypto Control function provides all the management and monitoring information required for proper operation of the LLC. This includes the information required to control the encryption of data to be transmitted from the SNC and the delivery of decrypted received data to the SNC.

Control of the SPC is passed through the LLC's Bypass function. The LLC monitors the flow of the SPC control information necessary for proper operation of the SPCs and radios. The LLC will also limit the number of bits that can be bypassed depending on the number of bits that have been encrypted and decrypted in a given time period. This bypass limit is a security feature of the device.

The LLC's Data Encryption/Decryption function provides the encryption, decryption, and integrity checking functions for all Network Packets (NPs) passing through the LLC. The LLC Integrity service can be enabled or disabled by the SNC on a per network basis. The 16-bit Integrity checksum is added to the NP data prior to its encryption, thus reducing the effective user bandwidth by two bytes per NP. Enabling the LLC Integrity function has negligible impact on LLC processing time. The contents of received NPs failing Integrity are never sent to the SNC, but the SNC is notified of the failure so that it can update statistics and perform corrective actions.

The LLC performs an error extension function to protect transmitted data against unauthorized modification. The error extension function guarantees that a modification of one bit of the input NP will result in multiple bits of the output NP being changed. Further, it guarantees that if an attacker changes a bit of the input NP, he does not know which bits of the output will be changed. This function is provided by default and is not selectable.

3A.6.4 Crypto Key Management

A Key Management Plan defines how keys are generated, distributed, and administered for the NILE network.

Crypto keys must be loaded into the front panel of the LLC, as described in paragraph 2.12 and Appendix B of the [\[LLC OPM\]](#). Keys are typically loaded from a Simple Key Loader (SKL) device or Data Transfer Device (DTD), which stores the keys in locations 0-63 of the specified network.

If the keys are loaded into the DTDs of all units at the same locations, then all SNCs will use the same Key Information. If the keys are loaded into the DTDs of each unit at different locations, the SNCs will need to use different Key Information to have the network operate correctly.

The DLP reports the Key Information to the SNC in the 'LLC Port Configuration Request' (303h) message. The SNC then sends the Key Information to the LLC in the 'LLC Configuration Request' (8100H) message.

The LLC constructs the encryption key on a packet-by-packet basis based on the NILE Address, NILE Network ID, Time Slot Number (TSN) specified by the SNC for that packet (which includes the Day of Week), and other device specific parameters. The LLC uses a two step encryption sequence to allow for the NILE Address to be explicitly included. If not explicitly included, the receiving LLC uses the Node ID supplied in the reception request by the SNC, which is from the ONCS.

Each day at midnight a ‘Key Management Request’ (8200H) message is automatically sent by the SNC to the LLC, which when the LLC DOW is 1-6 just causes the LLC to increment its DOW and resets the TOW to zero. When the DOW is 7, reception of the Key Management Request message causes a crypto key rollover, and the DOW is reset to 1, and the TOW is set to the TOW of the new key which should be 0. When a crypto key rollover occurs, all the keys in the currently used slots are zeroized and the LLC switches to use the next set of keys by incrementing the key location (if the location is 63, the next location is zero). A new set of keys can be loaded to replace the zeroized keys. The next weeks keys should always be loaded (when available) to ensure that a key rollover does not roll over to a location not containing a key, so as not to cause any loss of communication. Keys can be loaded at any time into any of the 64 key locations for each of the 8 networks, as long as the key is not being used.

3A.6.5 Crypto Time-of-Day (TOD)

There is no explicit TOD interface to the LLC. The LLC encrypts or decrypts the Network Packets passed to it in the data partition, using TSN information contained in the bypass partition of the messages sent over the SNC-to-LLC Interface or the LLC-to-SPC interface.

The Crypto Time-of-Day (TOD) bit-field is 32 bits long as shown in [Figure 3A.6-7](#), with the five most significant bits (28-32) always set to all zeros as padding. The remaining 27 least significant bits are the TSN, which comprises the Day Of Week (DOW) and the Time of Weekday (TOW).

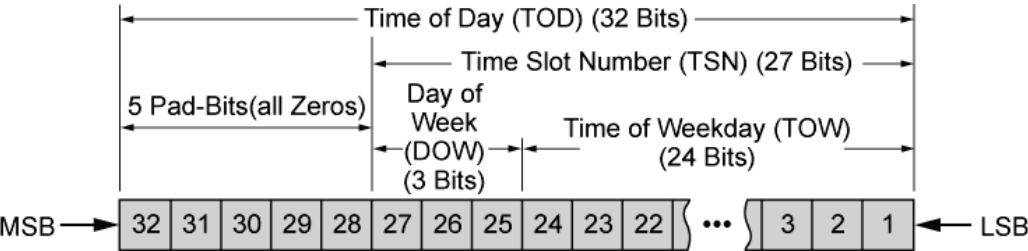


Figure 3A.6-7 Crypto TOD Format for time-related field

□ **DOW**

The DOW is contained in the three most significant bits (25-27) of the TSN. The DOW field value is common to all networks, having a value between 1 and 7, which is rolled over as previously detailed.

The LLC will reject a network packet for encryption if the DOW specified by the SNC does not match the internal DOW of the LLC. During LLC configuration, the current SN DOW is used to set the DOW of all LLCs.

During Operations, the LLC DOW of any newly configured LLC will be set by the SNC to the current SN DOW, as described in [3B.1.2 LLC Configuration](#).

□ **TOW**

The TOW is contained in the 24 least significant bits (1-24) of the TSN (see [Figure 3A.6-7](#)). TOW is measured as the number of Media Coding Frames (MCFs) since midnight where the value 0 means midnight. The actual maximum value used varies depending on the length of a MCF for a given media type.

Up to four separate networks can be connected to a single LLC, so the LLC keeps track of four separate TOWs, one for each network. The LLC will not encrypt data on a network if the DOWs do not match and the specified TOW is not greater than the TOW of the previously encrypted data on the same network. The TOW supplied by the SNC is always larger than the previously used value, except for the first value used after a rollover. When a daily rollover occurs, the TOW is reset to its minimum value of 0. Decryption does not require that the TSN is always larger than the previously used value. However, if an incorrect TSN is provided, the message will be decrypted incorrectly.

The LLC-7M does not have any limitations on the range of values for the TOW. The valid range of values for TOW in a Transmit NP Request is 0x000000 – 0xFFFFFFFF. The minimum value of TOW following a rollover is 0x000000; however due to the DOW change the SNC does not use the first timeslot of the day. The maximum TOW value for the last Transmit NP Request message of a ‘day’ is 0xFFFFFFFF. An LLC Error Report is generated when the maximum is reached and the LLC will no longer encrypt for that network until a DOW rollover occurs. This 24 bit maximum defines the most mini-slots that are possible per ‘day’, which equates to a minimum mini-slot or MCF duration of 5.15 milliseconds. The minimum MCF duration that an SPC can only be set to is 5.5ms and so the maximum value should never be reached. With

5.5ms the maximum value is 0xEF3A2. All current Link 22 media MCF durations are greater than this minimum and so this limit is never reached.

The LLC can generate the following TOD related Errors:

- A KIV_TSN_ERROR is reported if a Transmit NP Request TOW is less than or equal to the previously used TSN for the Network ID or if the DOW does not match the LLC's DOW value.

3A.7 LLC-to-SPC Interface

The LLC-to-SPC Interface enables the exchange of black (encrypted) data between the LLC and an SPC. The LLC has four separate interfaces using a single physical connector on the rear of the LLC-7M. Each interface provides a means for an SPC to communicate through the LLC to the SNC. The LLC-to-SPC Interface is fully defined in the [LLC IRS].

The LLC-to-SPC Interface carries black data to be transmitted, black data that has been received, and control and management information for the different media.

3A.7.1 Physical Interface

The LLC interfaces with up to four SPCs, each one having a separate serial connection, as shown in Figure 3A.7-1.

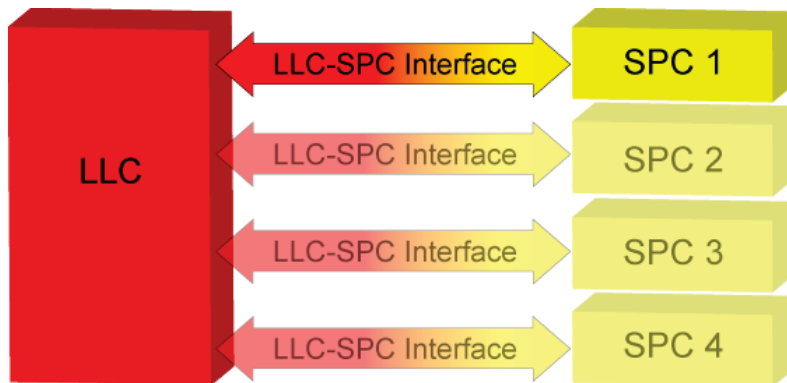


Figure 3A.7-1 Physical Interface between LLC and SPCs

The LLC-to-SPC Interfaces are implemented as balanced V24/V11 type (i.e., RS-422) Serial Interfaces. The serial format between LLC-to-SPC is a full duplex asynchronous format consisting of 1 start bit, 8 usable bits, no parity bit, and 1 stop bit. No higher level protocols for serial transport (e.g., loop mode, ACK/NACK, retransmissions, etc.) are supported, except as specified in the [LLC IRS] for LLC and SPC configuration and test modes.

Each serial interface in the LLC can be configured to operate at the following rates in bps: 19200, 28800, 38400, 57600, 115200, 230400, and 460800. The baud rate is set by an SNC-to-LLC message (the 'LLC Configuration Request' 8100H). The SNC is told by the DLP what baud rate the SPC is set at, as both the LLC and the SPC must

use the same rate to enable communications. The baud rate selected at the SPC must be high enough to support the data rate of the SPC.

The hardware interface supports the active signals shown in [Figure 3A.7-2](#). The LLC is considered the Data Terminating Equipment (DTE) and the SPC is considered the Data Communication Equipment (DCE).

Active Signals	DTE	DCE	Comments
Transmit Data (TxD)	Output	Input	Generated by the DTE for transmission of data to the DCE
Receive Data (RxD)	Input	Output	Generated by the DCE for the transmission of data to the DTE

Figure 3A.7-2 Active Signals Supported by the LLC Serial Interfaces

The connector for the LLC-to-SPC interface on the LLC chassis is a D38999/20WC35PN Circular Male Receptacle containing the 4 serial Interfaces, each interface using TxD and RxD interchange circuits as specified in the ISO 2110 standard. For the exact connector wiring, refer to the [\[LLC OPM\]](#).

3A.7.2 Functional Interface

The LLC-to-SPC Interface contains one functional interface, as shown in [Figure 3A.7-3](#). The data from the LLC contains control information in the Bypass partition and encrypted (Black) data for transmission in the Data Partition. The data from the SPC contains status information in the Bypass partition and received encrypted (Black) data in the Data Partition, for decryption by the LLC. The Crypto partition is always a null partition.

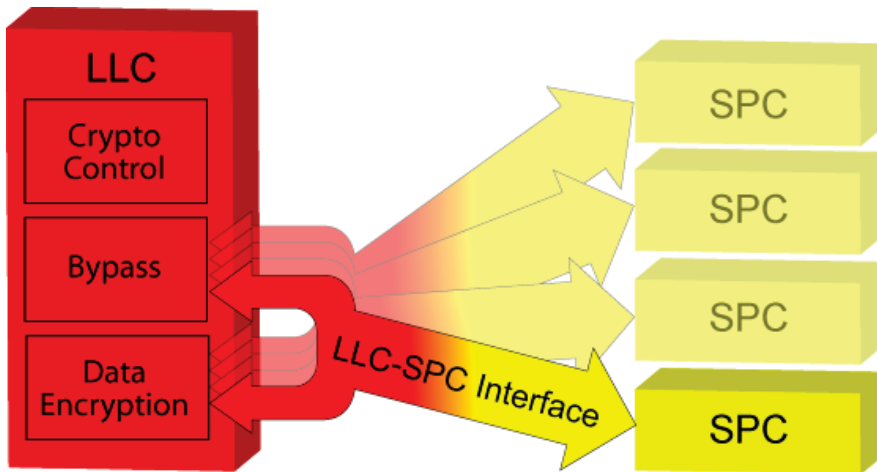


Figure 3A.7-3 LLC-to-SPC Functional Interface

3A.7.3 Message Definition

The structure of a LLC-to-SPC message is identical to the Serial Interface Message portion of the SNC-to-LLC Interface message structure defined in section 3A.5.3 Message Definition. It is also shown in Figure 3A.7-4. It should be noted that on this interface the Crypto partition is always a null partition.

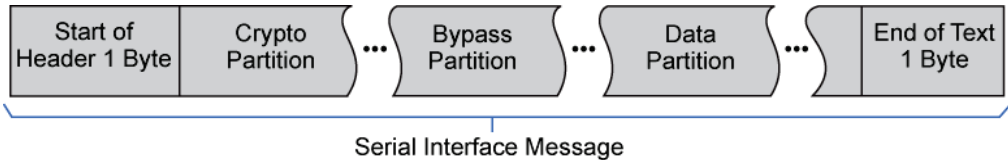


Figure 3A.7-4 LLC-to-SPC Message Structure

LLC-to-SPC serial interface communications use Big Endian byte format, and within a byte, the least-significant bit is transmitted first.

3A.7.4 LLC-to-SPC Messages

The messages the LLC sends to the SPC are as a direct result of the messages it receives from the SNC, and are listed in Figure 3A.7-5. The crypto partition is always empty for these messages. Only the ‘SPC Transmit Network Packet Request’ (0003H) message has a non-null data partition. For the first three messages in Figure 3A.7-5 the SNC sends the message to the LLC which sends it via the bypass partition to the SPC. For the last two messages the LLC receives the LLC version of the messages, the ‘LLC Transmit Network Packet Request’ (0303H) and the ‘LLC Receive Header Request’ (0404H) from the SNC. It then clears the crypto partition before sending them to the SPC as 0003H or 0004H messages respectively. Refer to section 3A.5.4 for SNC-to-LLC messages.

Message Name	Crypto: Bypass ID	Partitions			Protocol
		Crypto	Bypass	Data	
SPC Configuration Request	00C1H	null		null	SPC Control
SPC Status Request	0001H	null		null	
SPC Transmit Header Request	0002H	null		null	Transmission
SPC Transmit Network Packet Request	0003H	null			
SPC Receive Header Request	0004H	null		null	Reception

Figure 3A.7-5 LLC-to-SPC Messages

Figure 3A.7-5 and Figure 3A.7-6 show for each message the partitions that are not used and which have to be set as a null partition. Conversely where there is no null, the partition cannot be a null partition and must have the correct partition structure. The last column shows what protocol the message is part of.

3A.7.5 SPC-to-LLC Messages

The messages the SPC sends to the LLC are listed in Figure 3A.7-6. The crypto partition is always empty for these messages. Only the ‘SPC Receive Network Packet Response’ (00F3H) message has a non-null data partition. The LLC receives ‘SPC Receive Network Packet Response’ (00F3H) messages from the SPC, and fills the empty crypto partition before sending them to the SNC as ‘LLC Receive Network Packet Response’ (F5F3H) messages. Refer to the 3A.5.5 section for LLC-to-SNC messages. The last column shows what protocol the message is part of.

Message Name	Crypto: Bypass ID	Partitions			Protocol
		Crypto	Bypass	Data	
SPC Configuration Response	00E1H	null		null	SPC Status
SPC Status Response	00F1H	null		null	
SPC Error Report	00FFH	null		null	
SPC Alarm Message	00BBH	null		null	
SPC Transmit Response	00F2H	null		null	Transmission
SPC Reject Transmit Network Packet	00D3H	null		null	
SPC Receive Network Packet Response	00F3H	null			Reception
SPC Receive Response	00F4H	null		null	
SPC Receive Preamble Response	00F6H	null		null	

Figure 3A.7-6 SPC-to-LLC Messages

3A.7.6 Protocol

The protocols on the interface are detailed in Section 3C.14 of this chapter.

3A.8 SPC

The SPC functional architecture is shown in [Figure 3A.8-1](#).

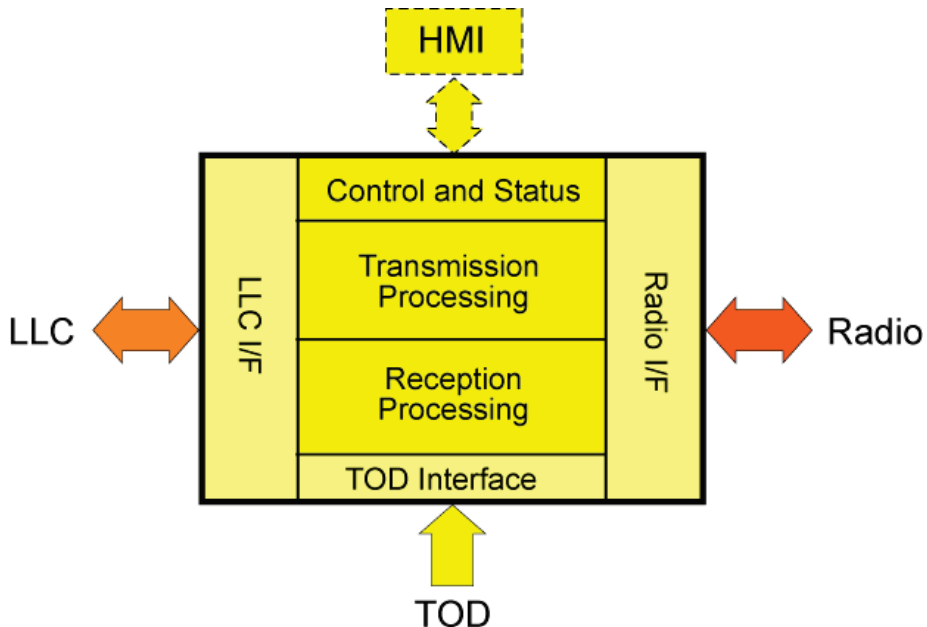


Figure 3A.8-1 SPC Functional Architecture

Each SPC has a serial interface to the LLC and an interface to its radio, which is dependent on the radio media type. Multiple SPCs may share the same TOD input. There may also be an optional HMI interface, to indicate configuration and status. This may consist of simple indicators or may be a more complex information display. The current HF FF and UHF FF SPCs are available in 19" rack mountable chassis. Some of the SPCs are implemented as a VME card, which means that they could be mounted in a suitably configured external VME backplane.

The function of the Link 22 SPC is to provide a Network Packet (NP) delivery service using Radio Frequency, operating on any of the following four media types.

- High Frequency - Fixed Frequency (HF FF) medium as defined in [STANAG 4539] - Annex D
- Ultra High Frequency - Fixed Frequency (UHF FF) medium as defined in [STANAG 4205] - Annex C
- High Frequency - Electronic Protection Mode (HF EPM) (slow frequency hopping) medium as defined in [STANAG 4444]
- Ultra High Frequency - Electronic Protection Mode (UHF EPM) (fast frequency hopping) medium as defined in [STANAG 4372] - Annex B - Chapter IV

A Link 22 SPC is required for each network/media that the unit is required to operate on. A single SPC may support more than one media, and a single unit may also contain more than one SPC.

3A.8.1 Functional Architecture

The SPCs functions and capabilities are media dependent. The functional architecture is illustrated in Figure 3A.8-2.

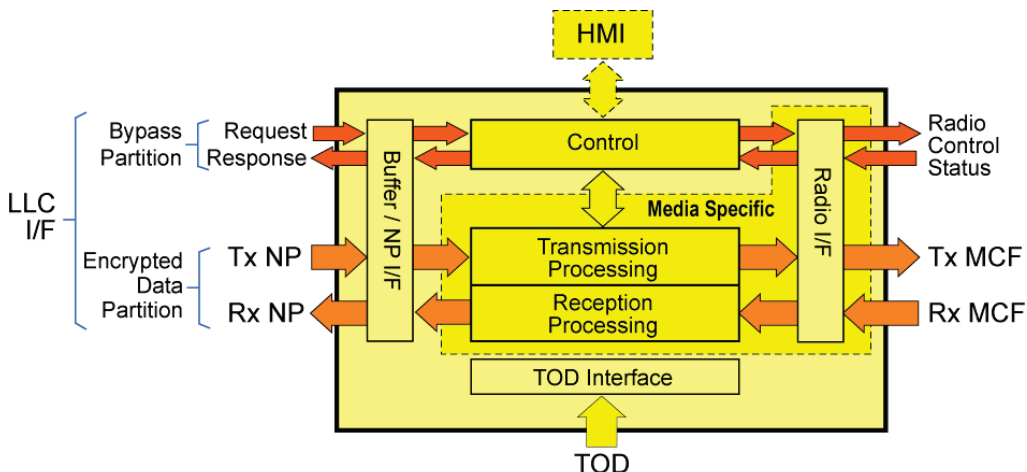


Figure 3A.8-2 SPC Functional Architecture

The following functions are provided by the SPC.

- Fragmentation and Reassembly – HF FF and UHF FF only
- Modulation and Demodulation (MODEM) – varies by media type, as defined in the [SPC SS] Appendices A-D
- Error Detection and Correction (EDAC) – varies by media type, as defined in the [SPC SS] Appendices A-D

The Fragmentation and Reassembly function is performed to communicate a Network Packet split across two or three MCFs. When a NP is fragmented into 2 MCFs, the first half of the NP is transmitted in the first MCF and the second half is transmitted in the next MCF. When a NP is fragmented into 3 MCFs, the first third of the NP is transmitted in the first MCF and the second third is transmitted in the next MCF and the last third of the NP in the third MCF. The Number of MCFs used is defined in the ‘SPC Configuration Request’ message. For EPM media, this value is always set to 1. When using fragmentation, if the reception or the decoding of one of the MCFs fails, the NP cannot be reassembled, and no NP is passed to the SNC.

3A.8.2 SPC - SNC/LLC Interface

The SPC communicates with the SNC through the LLC via a single bidirectional RS-422 serial data interface, as covered in section 3A.7.

3A.8.3 SPC - TOD Interface

The function of the Time of Day (TOD) interface is to provide the SPC with the time for synchronized operations on the media. The SPC has a single unidirectional interface with an external TOD Source. The Extended Have Quick format as specified in [STANAG 4430] is used by the SPC. The STANAG contains all the details (functional, physical, electrical, coding, etc.) of this format. However, any interface that provides the basic 1-PPS signal and Time Information messages, and that meets the SPC TOD requirements can be implemented as this is just a standardization issue and not an interoperability issue.

The Link 22 System requires that the TOD provided to the SPC is related to the Universal Time Coordinated (UTC) with accuracy better than or equal to ± 0.5 millisecond. The SPC synchronizes its transmission and reception operations to the supplied TOD.

The SPC monitors the TOD Interface and reports the TOD status (Enabled/Disabled), and the SPC's ability to transmit and/or receive in the <TOD Quality> field of the 'Status Response' (00F1) message, whenever the SPC sends the 'Status Response' (00F1) message. Changes to the TOD status are reported as they occur, no more than once a second.

The SPC monitors the accuracy of the TOD, based on Time Figure of Merit (TFOM) of the TOD or other accuracy information provided by the TOD interface, and its internal knowledge of its own timing delays, clock accuracy/drift and the time since it was last synchronized with the external TOD. If the time accuracy is equal to or worse than the value required for transmissions on the media (10 milliseconds for HF and 1 millisecond for UHF), the SPC disables transmissions to prevent possible jamming, and reports to the SNC that it is not able to transmit.

When an SPC receives a preamble it synchronizes the reception of NPs to the end of the preamble. If the TOD is inaccurate by an amount less than a media coding frame, and the SPC can synchronize to the preamble and have the correct media coding frame number, it can still receive. When the SPC stops attempting to receive is an implementation issue that does not affect interoperability. When reception stops due to TOD problems, the SPC reports to the SNC that it is not able to receive, and sets the SPC state to disabled.

3A.8.4 Optional HMI Interface

The Human Machine Interface (HMI) is an optional interface that implementers of an SPC may include for the monitoring of the SPC and radio. The HMI is an optional national implementation issue and is not described further in this document. All Link 22 required control of the SPC is performed by the SNC.

3A.8.5 SPC-to-Radio Interface

The SPC communicates with the Radio through the SPC-to-Radio Interface, as detailed in section [3A.9](#).

3A.8.6 Data Entities

The data entities handled by the SPC are listed below and are defined in the following subsections.

- [Network Packet \(NP\)](#)
- [Media Coding Frame \(MCF\)](#)

□ **Network Packet (NP)**

The NP represents the smallest unit of information passed by the LLC to the SPC and vice versa and are encrypted/decrypted by the LLC. The NPs, sent by the SNC for transmission on or received from the media, are neither modified nor interpreted by the SPC, but treated transparently.

The NP capacity is expressed in Media Coding Frames (MCFs) and in Bits.

- **MCFs:** The NPs can be spread out (Fragmented) over an integer number of MCFs (1, 2 or 3), as specified in the Number of MCF field received in the ‘Configuration Request’ (00C1) message. In the case of UHF EPM, the same NP may be transmitted multiple times (1,2 3, or 4), based on ‘SPC Initialization Parameters’ field received in the ‘Configuration Request’ (00C1) message
- **Bits:** The NP capacity is computed by the SPC based upon the configured media type, media setting number (also known as the SPC Initialization Parameters), and the fragmentation rate (Number of MCF)

□ **Media Coding Frame (MCF)**

An MCF represents the smallest unit of information which is exchanged by the radios. The SPC fragments a NP into an integer number of MCFs. The MCF duration (in milliseconds) is related to the selected media (fixed duration for a given media), as listed in [Figure 3A.8-3](#).

Media	MCF Duration (milliseconds)
HF FF	112.5
UHF FF	48.0
HF EPM	112.5
UHF EPM	<CN > Classified Number

Figure 3A.8-3 MCF Duration

The MCF is used to define the media timing, which is expressed as the number of MCFs since midnight. The MCF is the unit used to define all Link 22 Network Cycle Structures. Every timeslot is defined as a number of MCFs and the NCT is defined as the total number of MCFs.

The Modulation scheme and coding scheme (Reed Solomon (RS) or Convolutional (Conv)) used for a MCF varies for each media type and each media setting number, and are as shown in [Figure 3A.8-4](#). The resulting user capacity in bits of a MCF is also shown in the figure as the NP capacity when the fragmentation rate is 1. When the fragmentation rate is greater than 1, the NP is divided over 2 or 3 MCFs. However, the capacity of the MCF does not change.

Media	MSN	Modulation Scheme	Coding Scheme ¹	Network Packet (NP) Capacity in Bits ¹		
				Fragmentation Rate		
				1	2	3
HF FF	1	QPSK	RS (36,21)	168	336	504
	2	QPSK	RS (36,30)	240	480	720
	3	QPSK	RS (48,30)	240	480	720
	4	QPSK	RS (48,39)	312	624	936
	5	8PSK	RS (72,48)	384	768	1152
	6	8PSK	RS (72,57)	456	912	1368
UHF FF	1	16Kbps NRZ FM	RS (96,76)	608	1216	1824
HF EPM	1	QPSK	RS (36,30) / RS (24,21)	240 / 168	-	-
	2		RS (36,21) / RS (24,12)	168 / 96	-	-
	3		RS (24,21) / RS (16,12)	168 / 96	-	-
	4		RS (24,12) / N/A	96 / 0	-	-
UHF EPM	1	16Kbps NRZ FM	Conv 1/2, Rep 0	464	-	-
	2		Conv 1/2, Rep 1	464	-	-
	3		Conv 1/2, Rep 2	464	-	-
	4		Conv 1/2, Rep 3	464	-	-

Note: When LLC Integrity is enabled, the LLC uses the last 16 bits of the NP for an Integrity checksum. The SNC sends to and receives from the LLC, NPs that are 16 bits shorter than above, if non zero. However, the SPC will always receive NPs that are the size as stated in this table.

¹For HF EPM, two values are shown, the first is for a Regular NP and the second is for the Last NP

Figure 3A.8-4 Modulation & Coding Schemes, NP Capacity

3A.8.7 SPC System Capabilities

The SPC can queue up to 128 requests for transmission ('Transmit Header Request') and/or reception ('Receiver Header Request'), in any order or combination.

The SPC can queue at least 3 maximum size timeslots worth of data (Network Packets) for transmission at any instant.

The SPC will not send more than 4 messages per media coding frame to the LLC. This prevents the SPC from overloading the restricted bandwidth of the LLC bypass channel, which is shared by other networks using the same LLC. Normal this is not a problem, but when a group of rejected NPs, errors or alarms occur within a short period of time, if they were all sent immediately to the LLC this could affect the operation of the LLC and so the operation of the other networks using the LLC.

3A.9 SPC-to-Radio Interface

The function of the SPC-to-Radio interface is to connect the SPC to the Radio. It consists of two parts: the Control and Status Interface and the Data Interface.

The SPC-to-Radio Control and Status (C&S) Interface is an implementation issue depending upon the type of radio device connected to the SPC. However, the common mandatory capabilities and the desirable features are defined as follows.

The mandatory capabilities are as follows.

- **TX/RX Switching Control:** The SPC issues transmit and receive commands to the radio. The switching command timing takes into account the TX and RX attack and release times (the SPC has the knowledge of these radio delays)
- **Status/Alarm Report:** The radio is able to report to the SPC some basic information about its status (for example enabled/disabled) and about any alarm that may have occurred (for example Power Amplifier OFF). If the radio is disabled or has an alarm the SPC sends an 'Alarm Report' message to the SNC indicating Radio Failure. If the radio is disabled then the state of the SPC becomes disabled

The desirable features are as follows.

- **Abort Request:** The SPC should be able to request the radio to abort a transmission or reception request, after which the radio should go into the idle mode
- **Frequency Setting:** To allow the SPC (and thus the SNC) to remotely set up and change the frequency or frequency hopset
- **Power Setting:** To allow the SPC to remotely set up and change the transmitter power in order to support the Power management function handled by the SNC

The data interface provides data for transmission to the radio and receives data which the radio has received. The data interface is different for each media type and is specified in the applicable STANAGs. Each media type is considered in the following subsections.

□ **HF FF SPC-to-Radio Interface**

The HF FF SPC-to-Radio interface is composed of a Single Tone Baseband interface which is a common 300 - 3300 Hz single tone analogue signal interface, as described in [STANAG 4285] and Appendix A of the [SPC SS].

The Tx/Rx control is provided by a Press to Talk (PTT) line in accordance with the requirements of [STANAG 4285]. After the transmission of the last bit of a timeslot is completed, the SPC keeps the PTT line at the transmission level for another 4msec $\pm 10\%$, before dropping the signal, to allow time for the radio to complete transmission.

□ **UHF FF SPC-to-Radio Interface**

The UHF FF SPC-to-Radio interface is composed of a Non Return to Zero (NRZ) digital interface, as described in [STANAG 4205] and Appendix B of the [SPC SS]. While the SPC is not sending data to the radio, the output voltage from the SPC is held between +0.1V and -0.1V. The voltage output from the SPC is adjustable between $\pm 3V$ and $\pm 4V$.

After the transmission of the last bit of a timeslot is completed, the SPC keeps the transmitter keyline at the transmission level for another 500 μ sec $\pm 10\%$, before dropping the signal, to allow time for the radio to complete transmission.

□ **HF EPM SPC-to-Radio Interface**

The HF EPM SPC-to-Radio interface is composed of a Multi-tone Baseband interface is a raised cosine 300 - 3300 Hz multi-tone signal interface, as described in [STANAG 4444].

The HF EPM SPC uses the following subset of [STANAG 4444] Initial Network Parameters.

- Mode = TDMA
- CIE - COMSEC = External
- TIE - TRANSEC = Internal
- GT Index = 2

□ ***UHF EPM SPC-to-Radio Interface***

For the UHF EPM media, the SATURN Fast Frequency-Hopping radio is used to provide an Electronic Counter Measures resistance capability for the Link 22 data link. The SPC-to-Radio interface is composed of a digital data interface that is compliant with [STANAG 4372].

In addition to the common Control and Status interface requirements, the UHF EPM Control and Status has the following mandatory requirements, and desirable features.

■ ***Mandatory radio control***

The SPC is capable of: the following.

- Selection of SATURN TDMA Mode for Link 22 operation
- Setting of Net Number
- Selection of frequency hopping mode
- Timeslot Timing (Start signal/End signal)

■ ***Mandatory radio report handling***

The SPC is capable of using:

- The SATURN Radio provided clock signal indicating the SATURN Frame Timing as reference for the control and data exchange with the radio
- The SATURN Radio provided information about the short call synchronization process (short call detected, short call not detected, time)

■ ***Desirable features***

- Radio Status Outputs, the radio should report a measure of signal quality for both initial synchronization and after reception

3A.10 Radio Equipment

The Radio Equipment operates on the following four media types, and their characteristics and requirements are defined in the specified STANAGs.

- High Frequency - Fixed Frequency (HF FF) medium as defined in [STANAG 4539] - Annex D
- Ultra High Frequency - Fixed Frequency (UHF FF) medium as defined in [STANAG 4205] - Annex C
- High Frequency - Electronic Protection Mode (HF EPM) (slow frequency hopping) medium as defined in [STANAG 4444]
- Ultra High Frequency - Electronic Protection Mode (UHF EPM) (fast frequency hopping) medium as defined in [STANAG 4372] - Annex B - Chapter IV

For HF and UHF FF, the same radio used for Link 11 can generally be employed, if they include digital switching time. For UHF EPM SATURN capable radios are used.

This page is intentionally left blank.

Section B External Protocols

This section discusses the functions and protocols that may have external controls or visibility, and goes into the technical details that were not necessary for understanding from the operator's perspective given in Chapter 2. The following external protocols are discussed.

- SNC Initialization & Set-Up
- Network Initialization
- Orders
- Command Queuing
- SN Directory Maintenance
- DLP Request Management Info
- Network Control
- Late Network Entry (LNE)
- Closedown
- Monitoring and Statistics

3B.1 SNC Initialization & Set-Up

SNC Initialization is the process of initializing the SNC with Super Network information necessary for the preparation of the SNC prior to the start of Link 22 operations. This is accomplished by communications of Super Network OPTASK LINK (OLM) data and other unit specific information from the DLP to the SNC, and from the SNC to the LLC. Typically an operator would provide the OLM data to the DLP, and then request the start of the Link 22 initialization process, with no further operator action required, as shown in [Figure 3B.1-1](#). SNC initialization is composed of the following phases.

- Start of SNC Initialization
- LLC Configuration
- Super Network Directory Configuration
- End of SNC Initialization

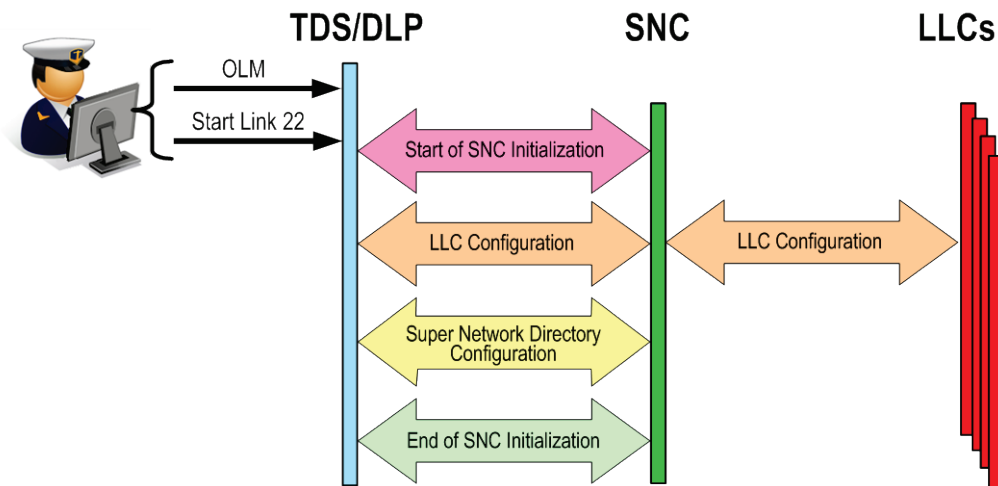


Figure 3B.1-1 SNC Initialization Phases

The phases are detailed in the following sub-sections, for normal initialization without errors. [Appendix B, Troubleshooting](#), covers initialization errors.

3B.1.1 Start of SNC Initialization

When the SNC executable starts running, it begins the SNC Initialization protocol by listening for a TCP/IP connection from the DLP. When the DLP attempts to establish this connection is a national implementation detail, for example it may be initiated by the operator, as shown above in [Figure 3B.1-1](#). After the TCP/IP connection between the DLP and SNC is made, the SNC sends its status to the DLP every 30 seconds, until the DLP responds. When the DLP receives the SNC's status, it knows that the SNC is working and ready to be initialized. After the DLP has processed the OLM data, and has received the 'SNC Status' (413h) message, it can send its first message to the SNC, which contains the Message Preparation Time (MPT) information, and is called a 'MPT Specification' (301h) message. The message flows are shown in [Figure 3B.1-2](#). The initialization figures in this section include status that may be displayed to the operator. Actual operator displays, if any, may differ.

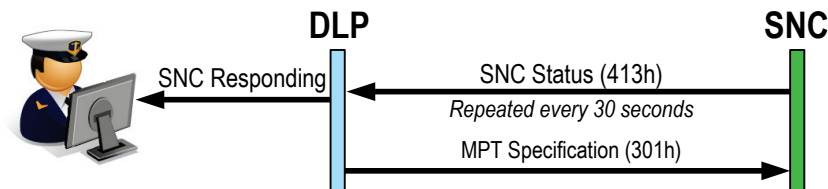


Figure 3B.1-2 Start of SNC Initialization

The 'MPT Specification' (301h) message specifies the following.

- Link 22 Address of the NU
- Time required for the DLP to prepare for the smallest timeslot (approximately 10 Tactical Message Words (TMW))
- Time required for the DLP to prepare for the largest possible timeslot (approximately 250 TMW)
- Whether or not the DLP wants to use the optional 'Optimized Receive Protocol'
- The BIT repetition rate
- The 'SN Day of Week (DOW)'
- The version of the DLP-SNC Interface the DLP wants to use
- Whether or not the DLP is capable of performing the SNMU and NMU functions

After the ‘MPT Specification’ (301h) message is correctly received, the SNC sends a ‘Built in Test’ (802h) message to the DLP (not shown in the figure), periodically at the BIT repetition rate specified in the MPT Specification.

Any time after the ‘MPT Specification’ (301h) message has been received, ‘Function Management Setup’ (335h) messages (not shown in the figure) may optionally be sent to the SNC to alter the default settings of the Function Management Switches. These are used to change the behavior of the SNC in response to network management orders, as discussed in section [3B.3 Orders](#).

The DLP-SNC Interface version is very important and is discussed in the following sub-section.

□ ***DLP-SNC Interface Version***

The SNC has a requirement for backward compatibility. This allows a DLP using an older definition of the DLP-SNC Interface to use the latest version of the SNC software. In this case, the SNC is able to use an older version of the message set to communicate with the DLP.

The SNC reports its SNC Version to the DLP in the ‘SNC Status’ (413h) message. The SNC Version consists of two parts: the major version number and the minor version number. Different major version numbers indicate an incompatibility between major SNC versions. The minor version number is used to identify SNC changes which are backward compatible with previous minor versions for the same major version. The version of the DLP-SNC Interface that the DLP will use is reported by the DLP to the SNC in the ‘MPT Specification’ (301h) message. The DLP must use the same major version number as its SNC, and must use a minor version number equal to or less than its SNC’s minor version number, as summarized in [Figure 3B.1-3](#).

Field	Compatibility	DLP Value Not Equal to SNC Value
Major Version Number	DLP and SNC must have the same value	Failure of SNC Initialization. SNC rejects 'MPT Specification' (301h) with a negative 'SNC C&S Acknowledgement' (421h)
Minor Version Number	DLP value must be less than or equal to SNC value	<i>DLP value > SNC value:</i> Failure of SNC Initialization. SNC rejects 'MPT Specification' (301h) with a negative 'SNC C&S Acknowledgement' (421h) <i>DLP value <= SNC value:</i> The SNC will communicate with the DLP at the version the DLP requested, and behave in the same way as an SNC of the requested version

Figure 3B.1-3 Version Number Compatibility

3B.1.2 LLC Configuration

After DLP receives the SNC's acknowledgement of proper reception of the 'MPT Specification' (301h) message, the DLP automatically continues with SNC initialization by starting the LLC Configuration phase, which consists of the following two steps.

- Connection to LLCs and Reset of Configurations
- Configuration of LLC's DOW and Ports

This determines whether the required LLCs can be accessed, and if so configures the LLCs as requested, ensuring that the internal LLC DOW is set to the current SN DOW.

❑ **Connection to LLCs and Reset of Configurations**

The DLP tells the SNC the number of LLCs to connect to, and the IP Address and port number of each LLC. To determine whether the required LLCs are available, the SNC attempts to connect to them using TCP. After a connection is established to an LLC, the SNC requests the LLC’s status. If the SNC gets a status response, the SNC knows that the LLC is available and responding to requests. The SNC sends a separate status request to each LLC. The LLC Status Response contains whether an LLC has any ports configured; which it may from previous use if all the networks were not previously closed down correctly. If there are any ports configured, the SNC configures the LLC with no ports configured, and checks that there are now no ports configured by sending another LLC Status Request. This configuration reset is shown in the shaded area in Figure 3B.1-4. This ensures that when this step completes there are no ports configured in all the LLCs, as this is necessary for the next step to set the DOW. The SNC informs the DLP of the results. The DLP updates its hardware status information which may be displayed to the operator. The message flows for this step are shown in Figure 3B.1-4.

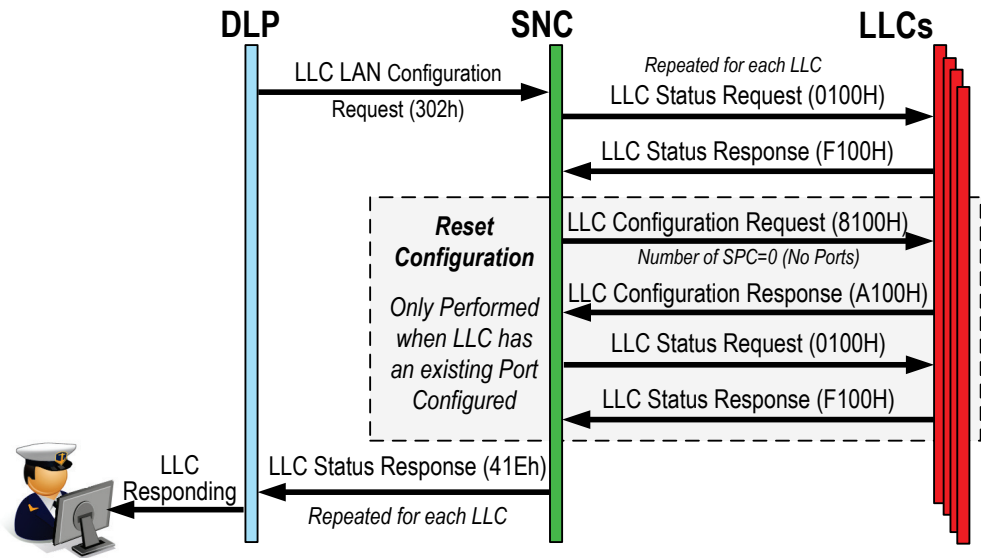


Figure 3B.1-4 Connect to LLCs and Reset Configurations

□ Configuration of LLC's DOW and Ports

The DOW in the LLC must match the SN DOW of the Link 22 system, which the DLP sent to the SNC in the 'MPT Specification' (301h) message. The LLC DOW can only be set to a specified value by using the Reset DOW Flag and the SN DOW fields in the LLC Configuration Request Message, which is only allowed when there are no ports already configured. In the previous step the SNC ensured that there are no ports configured. The SNC configures the LLC with the Reset DOW Flag field set to 1 and the SN DOW field set to the SN DOW, and at the same time configures the LLC ports as requested by the DLP in the 'LLC Port Configuration Request' (303h) message.

The LLC configuration sequence is a two-step process; first the SNC attempts to configure the LLC, and second the SNC requests the status of the LLC so that it can check that the LLC status matches the requested configuration. The SNC informs the DLP by sending a 'LLC Status Response' (41Eh) message. The DLP updates its hardware status information which may be displayed to the operator. The message flows for this step are shown in Figure 3B.1-5.

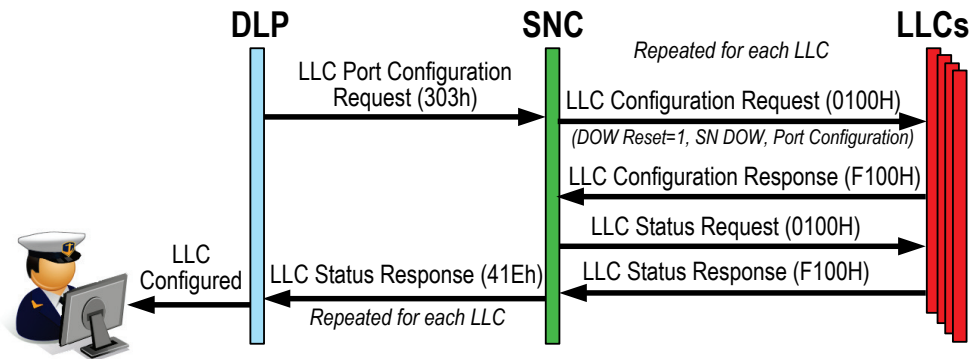


Figure 3B.1-5 Configuration of the LLC's DOW & Ports

3B.1.3 Super Network Directory Configuration

The Super Network Directory consists of two versions of the information, the OLM version and the current version. The configuration of the Super Network Directory consists of two parts to initialize these two versions. The first mandatory part is the entry of the information from the OLM which initializes the OLM version. Once complete the OLM version is copied to form a default current version. The second optional part is to initialize the current version of the Super Network Directory by replacing the default information with a newer version of the information. The newer version supplied by the DLP, for example might be the current version which the DLP received while previously participating as a member of the Super Network. These two parts of the initialization are detailed in the following sub-sections.

□ Super Network Directory OLM Version Initialization

Successful initialization requires that all NUs are provided with the same initial information. Each NU's DLP provides its SNC this initial information (version zero) through a set of messages that contain the information from the officially distributed OPTASK Link Message (OLM). The message flow is shown in [Figure 3B.1-6](#).

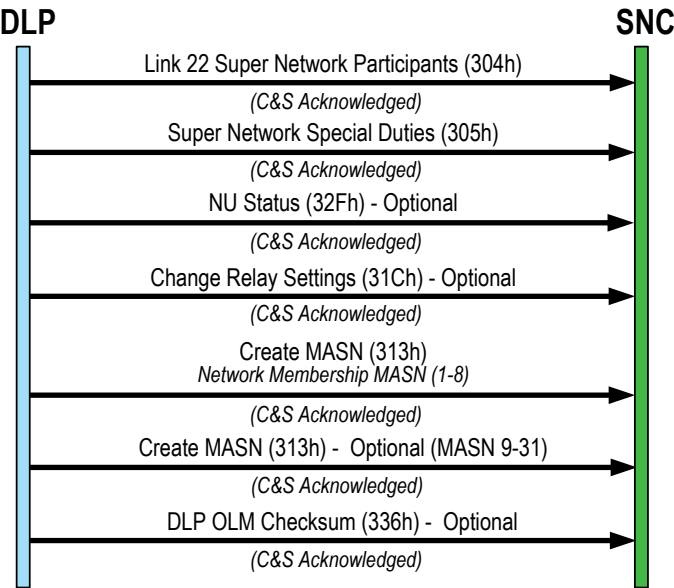


Figure 3B.1-6 Super Network Directory OLM Version Initialization

If the OPTASK Link Message assigned the NU a role for which its DLP is not capable, an ‘SNC Status’ (413h) message will be sent to the DLP reporting the role mismatch.

Figure 3B.1-7 lists the messages that are sent during this phase, indicates whether the message is mandatory or optional, and describes the content of the messages.

Message	Required	Description
Link 22 Super Network Participants (304h)	Mandatory	A list of Link 22 addresses in the Super Network
Super Network Special Duties (305h)	Mandatory	Link 22 Address of: <ul style="list-style-type: none"> ■ SNMU ■ Standby SNMU ■ NMU for each Network ■ Standby NMU for each Network
NU Status (32Fh)	Optional	Initial status of NUs (Default is Inactive)
Change Relay Setting (31Ch)	Optional	Initial relay settings of NUs (Default is Automatic)
Create MASN (313h) <i>One for each Network</i>	Mandatory	Link 22 Addresses of network members, as detailed in Appendix D, Section D.1 Super Network Level Data from the OLM
Create MASN (313h) <i>One for each non-Network MASN</i>	Optional	Link 22 Addresses of non-network MASN members
DLP OLM Checksum (336h)	Optional	Provides a checksum from the OLM in order to verify SN Directory data

Figure 3B.1-7 SN Directory OLM Version Initialization Messages

□ Super Network Directory Current Version Initialization

The current version of the Super Network Directory is initialized by default to be equal to the OLM version. At the time the NU is initialized, it is possible that the current Super Network Directory has changed from the original OLM settings, after the operations have been started. This can occur, for example, if the NU fails and needs to be restarted, or the NU starts late and updates are provided through an external channel. During SNC Initialization, the DLP can optionally provide a

complete newer version of any of the Super Network Directory components to the SNC (including the new version number). If the DLP does not supply the updates during SNC Initialization, the SNC will receive them automatically from the SNMU SNC, as detailed in section 3B.5 SN Directory Maintenance, which can consume significant bandwidth.

Figure 3B.1-8 shows the flow of messages between the DLP and SNC used to initialize the current version of the Super Network Directory components. These messages are the same as used in the initialization from the OLM, but are used to initialize the current version.

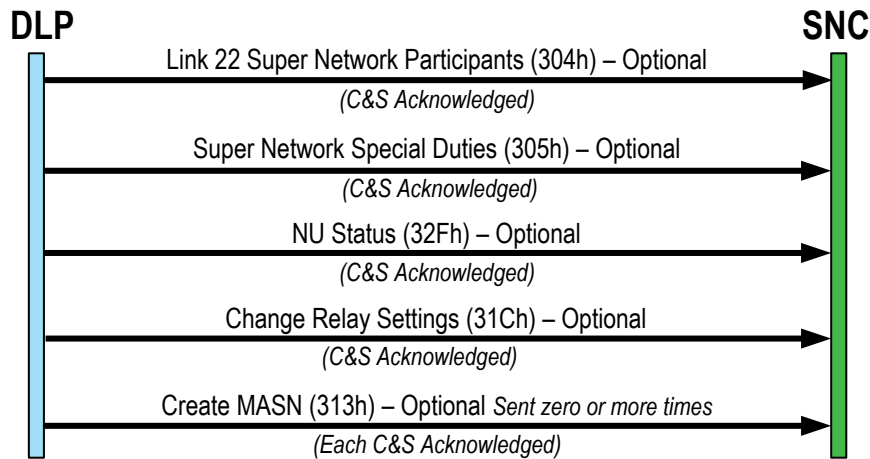


Figure 3B.1-8 Super Network Directory Current Version Initialization

Figure 3B.1-9 describes the messages that can be sent to initialize the current version of the Super Network Directory. All messages are optional, but if included, must be sent in the order shown, with a single message containing the complete contents of the newer version of a Super Network Directory component, except for the MASN component where there is a message for each MASN that is defined for the current version. When a message is received the contents of the Super Network Directory component are deleted and then replaced by the newer version. For the MASN component the deletion of the existing default OLM values occurs on reception of the first ‘Create MASN’ (313h) message.

If the ‘Super Network Special Duties’ (305h) message assigns the NU a management role for which the DLP is not capable, an ‘SNC Status’ (413h) message will be sent to the DLP reporting the role mismatch.

Category	Messages	Description
Address	Link 22 Super Network Participants (304h)	One message containing all the Link 22 Address of all the Super Network members at the specified version number, only sent when the Address version number is not the OLM version (zero).
Role	Super Network Special Duties (305h)	One message containing all the roles, only sent when the roles are different from the OLM roles.
Status	NU Status (32Fh)	One message containing the NU Status of all the Super Network members at the specified version number, only sent when the Status version number is not the OLM version (zero).
Relay	Change Relay Settings (31Ch)	One message containing the Relay settings of all the Super Network members at the specified version number, only sent when the Relay version number is not the OLM version (zero).
MASN	Create MASN (313h)	One message for each defined MASN, at the specified version number, only sent when the MASN version number is not the OLM version (zero).

Figure 3B.1-9 SN Directory Current Version Initialization Messages

3B.1.4 End of SNC Initialization

An ‘SNC Initialization Complete’ (32Ch) message is sent by the DLP to indicate that its initialization of the SNC is complete, and that the DLP will not send any more initialization messages to the SNC. The SNC’s positive acknowledgment of this message implies that the SNC is operational and ready for network initialization.

3B.2 Network Initialization

The goal of Network Initialization is for the SNC to accept the initial Network and Media parameters, as directed by the DLP (from the OLM). If Initialization with probing is required, this allows modifying and improving these parameters in order to better adapt to the current environmental conditions.

The Network Initialization protocol relies on the following.

- Successful SNC initialization
 - LLCs configured
 - LLC/SPC selected for each network
- Distribution of the same network information from the OLM to all NUs expected to participate in the network
 - Network ID
 - Media Type
 - Frequency/Hopset
 - Media Setting Number
 - Fragmentation Rate
 - LLC Integrity Flag (disabled during Probing)
 - DTDMA Flag (disabled during Probing)
 - Network Start Time

A separate Network Initialization message is provided to the SNC for each NILE network in the Link 22 Super Network.

Initial network members are specified in the MASN for the network. This allows for the inclusion of Receive-Only units. All NUs specified in the network MASN perform network initialization, including Receive-Only units.

If the LLC Integrity for the network is different than the value used to initialize the LLC during SNC Initialization, the port of the LLC will be reconfigured to use the different value.

Two types of network initialization procedures are available, as shown in [Figure 3B.2-1](#). The OLM specifies the network initialization type to be used for each network.

Initialization Type	Description	Uses
Short	Single MSN	Confidence in mission, media, area of deployment. Fast, straightforward initialization
Probing	Set of MSNs assessed	Topology and connectivity of participants uncertain. Slower, requires interaction with the NMU DLP Operator

Figure 3B.2-1 Network Initialization Types

It is expected that short initialization is the default selection, since the NMU can modify the parameters during operations.

Regardless of the type of initialization used, the SNC configures each required SPC through the attached LLC as shown in [Figure 3B.2-2](#), approximately 10 seconds prior to the start of the network. These steps are not shown in subsequent figures. The steps are the following.

- SNC requests the SPC status to ensure the SPC is enabled
- SNC configures the SPC per the parameters supplied by the DLP. If frequency and radio power are not controlled automatically, the Operator needs to ensure the correct settings
- SNC requests the SPC status again to check that the SPC configuration matches what the SNC requested. Radio Power and Frequency will not be checked if the SPC cannot automatically control them

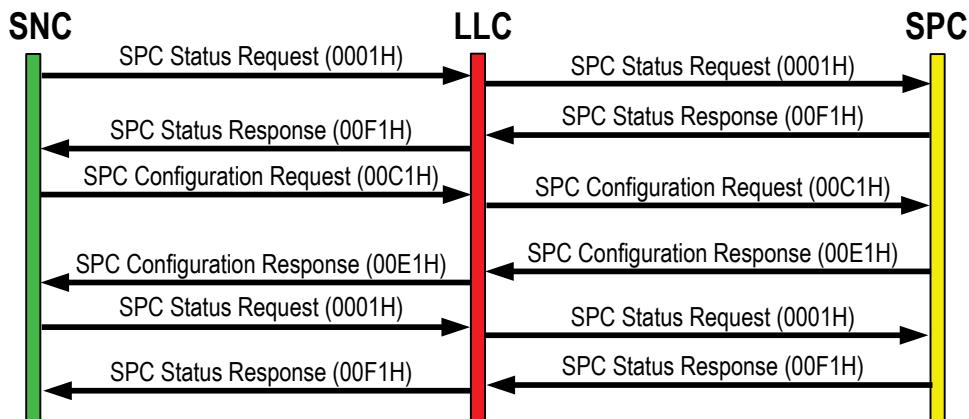


Figure 3B.2-2 SPC Configuration

Refer to Appendix B Troubleshooting for details of what happens if the configurations do not match.

The parameters used to initialize the SPC are listed below.

- Media Type
- Frequency/Hopset
- Media Setting Number (known as SPC Initialization Parameters in the [\[LLC IRS\]](#))
- Fragmentation Rate (known as Number of Media Coding Frames (MCF) in the LLC IRS)
- SPC Radio Power
- Time of Configuration (Not used. Set to FFFFF Hex)
- BIT/Loopback (Set to 0 (Normal))

When the DLP requests that the SNC probe multiple MSNs, the SNC initially configures the SPC to the first MSN supplied. All MSNs will be probed in order, as described in section [3B.2.2 Network Initialization with Channel Probing](#).

3B.2.1 Short Network Initialization

There are two forms of Short Network Initialization, depending on whether the NCS is calculated by the SNC, or supplied by the DLP.

- Network Parameters (SNC NCS)
- Network Parameters (DLP NCS)

□ Network Parameters (SNC NCS)

When the SNC is to calculate the NCS, the DLP supplies the media parameters and the following additional network parameters to the SNC.

- Access Delay Tolerance
- Efficiency
- For each NU that needs to transmit in the network
 - Channel Capacity Need
 - Channel Access Delay

Each SNC in the network calculates the same NCS based on the network parameters and the transmission needs of each NU, as described in [Section 3C.7 Network Cycle Structure Handling](#). Network connectivity is not taken into consideration for this computation. Each SNC reports the NCS to its DLP, initializes the SPC, and at network start time the NCS becomes operational. The SNC reports to its DLP that the network initialization is complete. This protocol is shown in [Figure 3B.2-3](#).

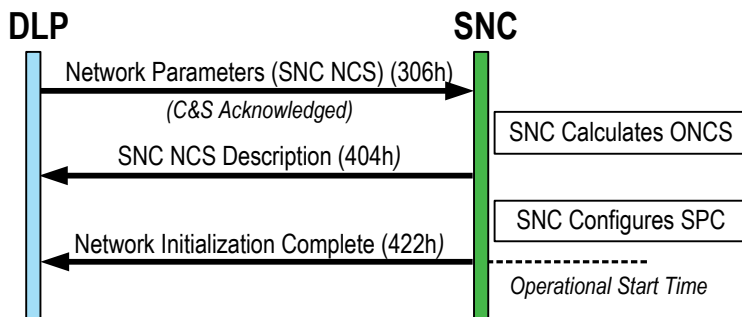


Figure 3B.2-3 Network Parameters (SNC NCS)

□ **Network Parameters (DLP NCS)**

When the DLP supplies the NCS, it also supplies the media parameters. Each timeslot in the defined NCS consists of the following.

- Timeslot Size (in minislots)
- Timeslot Owner (Link 22 Address, or 0 for a Priority Injection slot)

Each SNC accepts the NCS (if all values are consistent with defined constraints), initializes the SPC, and at network start time the NCS becomes operational. The SNC reports to its DLP that the network initialization is complete. This protocol is shown in Figure 3B.2-4.

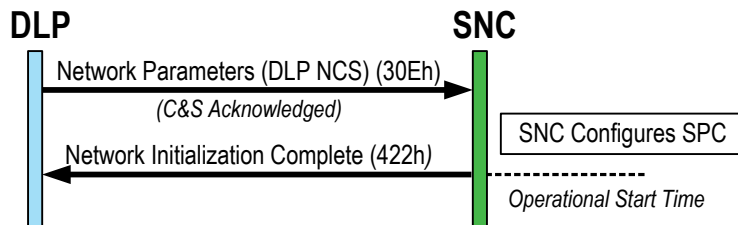


Figure 3B.2-4 Network Parameters (DLP NCS)

3B.2.2 Network Initialization with Channel Probing

Network Initialization with Channel Probing is used when there is little confidence in the environmental conditions, including Media Setting Numbers and network connectivity (list of participants and topology). Therefore, the SNC is requested to probe the channel in order to assess the channel, network connectivity quality (for the specified RF parameters), and optimize the NCS by taking into account connectivity information.

When Channel Probing is to be performed, the DLP supplies the media parameters and the following additional network parameters to the SNC.

- List of NUs (Link 22 Address for each NU)
- List of up to six MSNs to probe

Each SNC in the network initially configures the SPC with the first MSN. All MSNs will be probed in the order that the DLP supplied them. The probing NCS is fixed based on the following characteristics.

- NUs are sorted by their NILE Address
- Each NU participating in probing is assigned a single timeslot of size 5 Minislots
- Timeslots are in increasing order of the NU's 7-bit NILE Address
- No interrupt slots
- SPC Fragmentation Rate set to 1

The start time is calculated so that the first timeslot is the one assigned to the NMU. Because of this adjustment, the start time can be up to one NCT later than the start time in the received 'Network Parameters (Probing)' (307h) message.

At the start time, each SNC starts transmitting PROBING RECEPTION QUALITY (PRQ) technical messages in its timeslot. PRQ describes the quality of received transmissions from neighbor NUs. The quality figure is based upon the number of Network Packets (NP) received from neighbor NUs and the SPC provided error rate of the NP receptions.

The NU always sends its own PRQ message in the timeslot, and may also retransmit the PRQ messages received from its neighbors, if they fit into the timeslot, using the rules in [Figure 3B.2-5](#). This allows connectivity information to be communicated up to three legs away.

Condition	PRQ Messages in Timeslot
No neighbor PRQ messages received	Fill timeslot with own PRQ messages
Not all neighbor PRQ messages will fit in the timeslot	Own PRQ message Include only neighbor PRQ messages for the NUs that are not neighbors of the NMU and Standby NMU (if known). This helps to ensure that the NMU and Standby NMU receive the most PRQ information possible
Still not enough room for neighbor PRQ messages	Own PRQ message Randomly select neighbor PRQ messages to include in the timeslot

Figure 3B.2-5 Probing Timeslot Content Rules

[Figure 3B.2-6](#) shows an example of the PRQ messages that NU 1 might transmit in its timeslot for the network topology shown in the figure. NU 1's timeslot is large enough

for it to transmit its own PRQ message (PRQ NU 1), and retransmit all of its neighbors' PRQ messages (PRQ NU 2, PRQ NU 4, PRQ NU 5, and PRQ NU 6). After packing all of the neighbor PRQ messages, there is still room in the timeslot, so the NU fills the rest of the timeslot with a repeat of some of the PRQ messages.

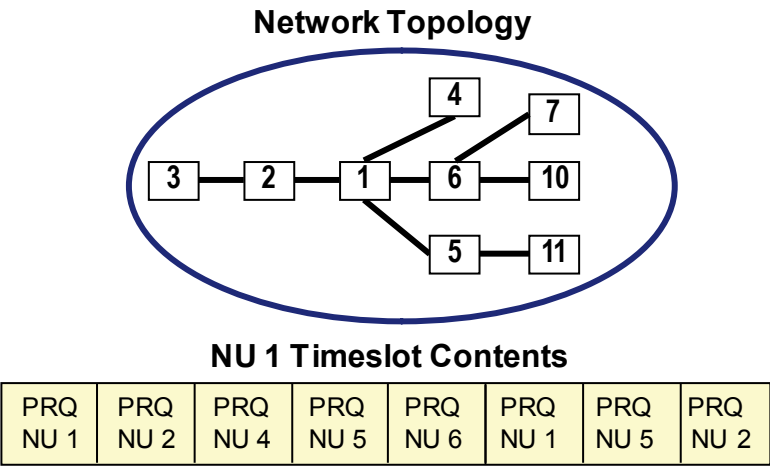


Figure 3B.2-6 PRQ Timeslot Usage

Each SNC builds a probing Connectivity Matrix from the PRQ data, reflecting the quality of links between NUs up to three legs away. This matrix is also used to initialize the connectivity learning process at the beginning of the Operational Network and therefore reduces the time to reach steady state. The PRQ values can be interpreted as described in [Figure 3B.2-7](#).

PRQ	Frequency	MSN	Meaning
0	Poor		Most of the preambles are not detected
1	Good	Not robust enough	Too many NPs do not pass the EDAC function.
2	Good	Robust enough	Most of the NPs are corrected by the EDAC function
3	Good	Very robust	Most of the NPs pass the EDAC function without any errors. A faster throughput MSN could be used if the current Network connectivity is good

Figure 3B.2-7 PRQ Interpretation

Ten NCTs of ‘PROBING RECEPTION QUALITY’ (5.6) technical messages are exchanged for each MSN. Each SNC then reports the probing results for the MSN to its DLP, including the following information.

- Gross Channel Throughput (bits per second)
- LRQ between each pair of NUs in the network
 - Up to three legs away for the NMU
 - Up to two legs away for all other NUs

One NCT is then used for the SNC to reconfigure the SPC for the next MSN. This is repeated for each MSN.

Each SNC informs its DLP when probing of all MSNs has ended. This part of the probing protocol is shown in [Figure 3B.2-8](#) for a single SNC; however all NUs in the network perform the probing. Multiple ‘PROBING RECEPTION QUALITY’ (5.6) technical messages are sent and received, and multiple ‘Probing Results’ (401h) messages may be sent at the end of each probed MSN, if the results do not fit into a single message.

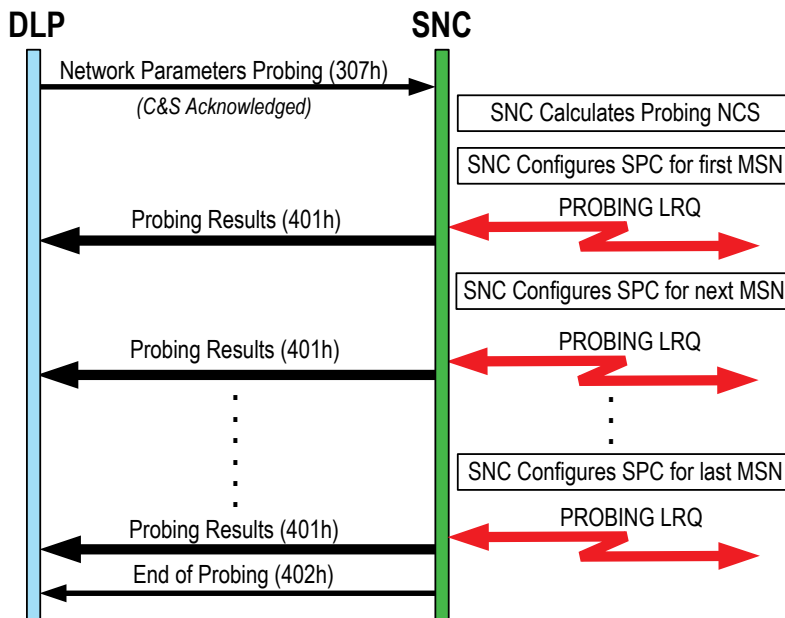


Figure 3B.2-8 Probing

After the end of probing, the last set of probed parameters continues to be used by each probing NU in the network. The NMU SNC starts transmitting ‘NMU ACTIVE’ (5.7) technical messages (not shown in the figure) to inform all other NUs that it is present and active. This prevents the Standby NMU from taking over the NMU role.

The DLP/Operator of the NMU will have the complete set of Connectivity, Link Quality measures, and throughput for each MSN. The DLP/Operator of the NMU has the following options.

- **Decides To Probe More Channels**
- **Accepts Probing Results**

These options are detailed in the following sub-sections. As soon as the NMU DLP responds to the SNCs with its choice, the NMU SNC stops transmitting the ‘NMU ACTIVE’ (5.7) technical message, in order to send additional required messages.

□ *Decides To Probe More Channels*

If the probing results indicate that no MSN leads to reasonable network performance, the DLP/Operator of the NMU can request a reprobe with new parameters, possibly including other MSNs, a new frequency, or a different list of NUs.

Note: Reprobing with a different frequency requires that all the radios being used allow the frequency setting to be controlled by the SPC.

The SNC of the NMU distributes the supplied network parameters to the NUs involved in the reprobing, which then respond back to the NMU indicating they are ready, and send the reprobe information to their DLPs. After at least 80% of the NUs respond, the NMU calculates a Network Start Time, and transmits it. Before the Network Start time, each SNC involved in the reprobe reconfigures its SPC to the provided media parameters, and then starts the new probing sequence at the specified time. The reprobe request and distribution is shown in [Figure 3B.2-9](#). The messages used to perform the actual probing are the same as the original probing, and are not included in this figure.

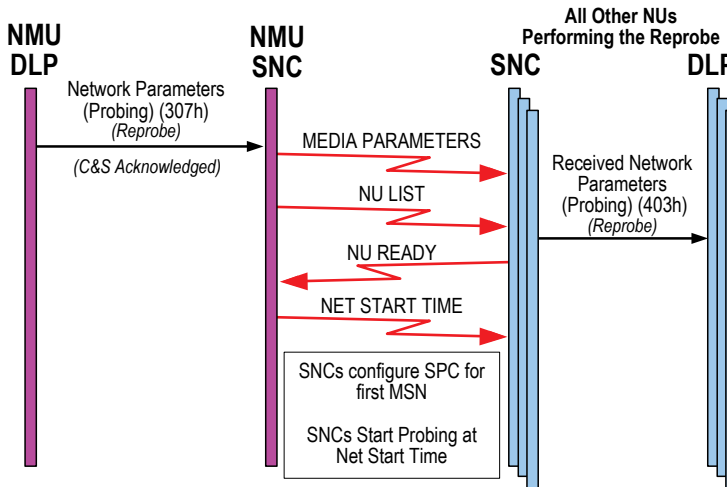


Figure 3B.2-9 Reprobng

The DLP can continue to request reprobng multiple times, until it is satisfied with the results.

❑ **Accepts Probing Results**

When the DLP/Operator of the NMU is satisfied with the probing results, it has to select which media parameters are to be used, including the DTDMA and LLC Integrity settings that were not used during probing.

The media setting is selected to achieve the lowest error rate for the highest data throughput.

The DLP/Operator of the NMU also decides how to provide the NCS for the network. The protocol continues with the following two stages.

- **NCS Definition**
- **Network Parameter Distribution**

These two stages are detailed in the following sub-sections.

■ **NCS Definition**

The NMU DLP has the same NCS choices as for short initialization, as shown in [Figure 3B.2-10](#), and they are described in the following two sub-sections. The selected media parameters are included with the NCS message.

NCS	DLP Supplied NCS Parameters	Message
Calculated by SNC	Access Delay Tolerance & Efficiency For each NU that needs to transmit in the network: <ul style="list-style-type: none">■ Channel Capacity Need■ Channel Access Delay	Operational NCS Request (30Bh)
Supplied by DLP	Timeslot Size (in minislots) Timeslot Owner (Link 22 Address, or 0 for a Priority Injection slot)	DLP NCS Description (30Dh)

Figure 3B.2-10 End of Probing NCS choices

◇ ***DLP Requests an NCS Calculated by the SNC***

If requested, the NMU SNC uses the supplied information to calculate the NCS. The SNC uses its Probing Connectivity Matrix to identify relay units, so that it can upgrade their Capacity Need and Access Delay values when computing the NCS. The SNC sends the NCS back to the DLP.

The DLP can do one of the following.

- Accept the NCS
- Supply different parameters for the SNC to calculate another NCS (for the same inputs, the SNC always produces the same results)
- Provide the NCS itself (as described in the next section)
- Reprobe

This protocol can be repeated until an NCS is determined. [Figure 3B.2-11](#) shows the case of the DLP accepting the SNC calculated NCS.

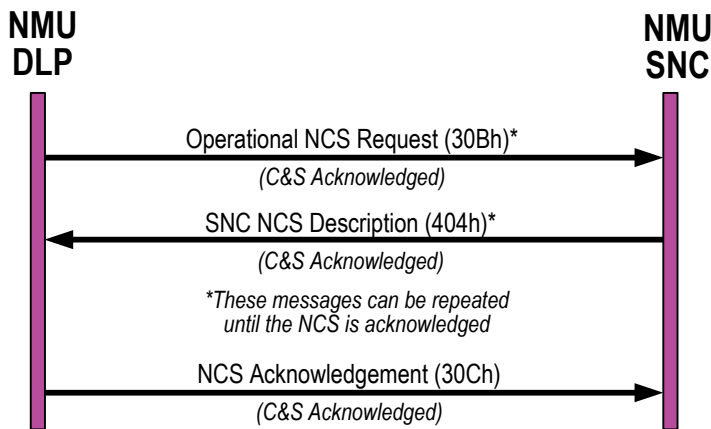


Figure 3B.2-11 DLP Requests SNC NCS after Probing

◇ **DLP Supplies the NCS**

The protocol used when the NMU DLP supplies the NCS itself after probing is complete, is shown in [Figure 3B.2-12](#).

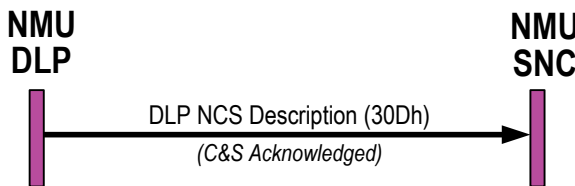


Figure 3B.2-12 DLP Provides NCS after Probing

■ **Network Parameter Distribution**

After the NCS calculation is accepted, or the NCS is supplied, the NMU SNC distributes the selected network parameters and the new NCS using the probing NCS and the last probed parameters. All other NU SNCs that were specified to be in the network send the received NCS and media parameters to their DLP, and respond back to the NMU SNC indicating they are ready. After at least 80% of the NUs respond, the NMU SNC calculates a Network Start Time, and transmits it. Before the Network Start time, each SNC in the network reconfigures its SPC to the provided media parameters. At the start time the SNC initializes the network and the NCS becomes operational. The SNC then informs its DLP that network initialization is completed,

and the network is operational. This protocol is shown in [Figure 3B.2-13](#), starting after the NCS has been determined.

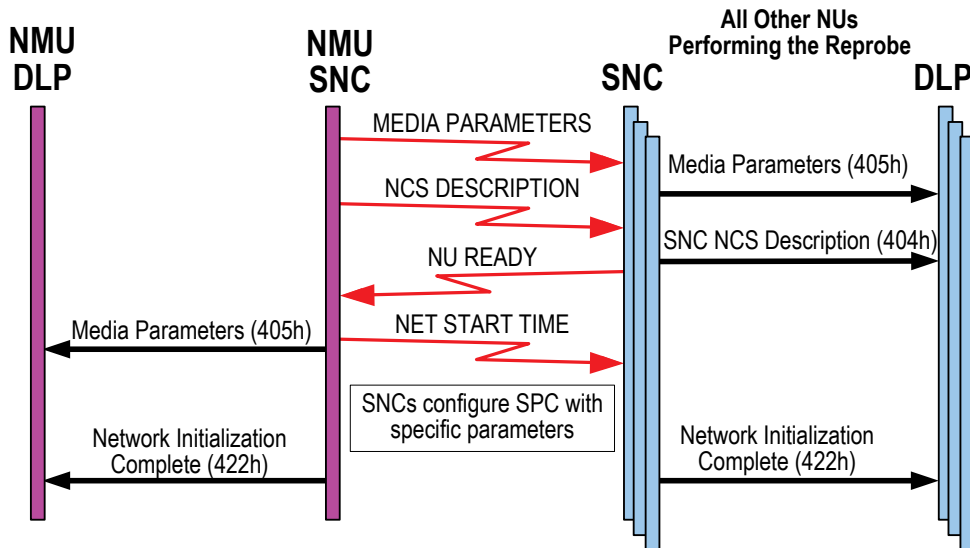


Figure 3B.2-13 Media Parameter Distribution after Probing

The SNC of the NMU also sends a NCT INFO technical message to all NUs in the Super Network, which contains the Network Cycle Time (NCT) information, so that all other NUs not in the network will know the NCT for the network. This is used to compute routing selection as detailed in section [3C.8 Relay & Routing](#) (but is not shown in the figure). A routing technique called flooding is used during the probing protocol by NUs to retransmit received technical messages, which increases the chance that all NUs will receive the necessary messages. The technical messages that are retransmitted using flooding are listed below.

- NMU ACTIVE
- MEDIA PARAMETER
- NCS DESCRIPTION
- NU LIST
- NU READY
- NET START TIME

3B.3 Orders

Network Management Orders are used by the SNMU or NMU to order other NUs to perform a specific function. The following topics are covered in this section.

- [Order Overview](#)
- [Function Management Switches](#)
- [Order Protocol](#)

3B.3.1 Order Overview

Orders contain the following information.

- Type of Order
- Addressing
 - A single NU
 - All Network members
 - All Super Network members
- Network ID
- Start and End Time
- Order Specific Parameter

Figure 3B.3-1 lists all the orders, the source and destination (Dest), and whether a Network ID, Start Time, End Time, and Order Specific Parameter are required, optional, or not applicable.

Order	Source	Dest	Network ID	Start Time	End Time	Order Specific
SN Closedown	SNMU	ALL	N/A	Required	N/A	N/A
NN Closedown	SNMU NMU	NMU Net	Required Required	Required Required	N/A N/A	N/A N/A
Leave Super Network	SNMU	NU	N/A	OPT	N/A	N/A
Leave Network	SNMU NMU	NU NU	Required Required	OPT OPT	N/A N/A	N/A N/A
Join an existing Network	SNMU	NU	Required	OPT	OPT	N/A
Assume SNMU Role	SNMU	NU	N/A	OPT	N/A	N/A
Assume Standby SNMU Role	SNMU	NU	N/A	OPT	N/A	N/A
Assume NMU Role	SNMU NMU	NU NU	Required Required	OPT OPT	N/A N/A	N/A N/A

Order	Source	Dest	Network ID	Start Time	End Time	Order Specific
Assume Standby NMU Role	SNMU NMU	NU NU	Required Required	OPT OPT	N/A N/A	N/A N/A
Insert LNE Slot	SNMU	NMU	Required	OPT	OPT	N/A
Remove LNE Slot	SNMU	NMU	Required	OPT	N/A	N/A
Radio Silence ON - SN - Single NU	SNMU	NU	N/A	OPT	OPT	N/A
Radio Silence ON - NILE Network - Single NU	SNMU NMU	NU NU	Required Required	OPT OPT	OPT OPT	N/A N/A
Radio Silence ON - Super Network	SNMU	ALL	N/A	OPT	OPT	N/A
Radio Silence ON - NILE Network	SNMU NMU	Net Net	Required Required	OPT OPT	OPT OPT	N/A N/A
Radio Silence OFF - SN - Single NU	SNMU	NU	N/A	OPT	N/A	N/A
Radio Silence OFF - NILE Network - Single NU	SNMU NMU	NU NU	Required Required	OPT OPT	N/A N/A	N/A N/A
Radio Silence OFF - Super Network	SNMU	ALL	N/A	OPT	N/A	N/A
Radio Silence OFF - NILE Network	SNMU NMU	Net Net	Required Required	OPT OPT	N/A N/A	N/A N/A
Initialize New Network (DLP NCS)	SNMU	Net	Required	Required	N/A	N/A
Initialize New Network (SNC NCS)	SNMU	Net	Required	Required	N/A	N/A
Initialize New Network (Probing)	SNMU	Net	Required	Required	N/A	N/A
Re-initialization (DLP NCS)	SNMU	NMU	Required	OPT	N/A	N/A
Re-initialization (SNC NCS)	SNMU	NMU	Required	OPT	N/A	N/A
Re-initialization (Media only)	SNMU	NMU	Required	OPT	N/A	N/A
Re-initialization (Probing)	SNMU	NMU	Required	OPT	N/A	N/A
Reconfiguration (DLP NCS)	SNMU	NMU	Required	OPT	N/A	N/A
Reconfiguration (SNC NCS)	SNMU	NMU	Required	OPT	N/A	N/A
Reconfiguration (DTDMA ON)	SNMU	NMU	Required	OPT	N/A	N/A
Reconfiguration (DTDMA OFF)	SNMU	NMU	Required	OPT	N/A	N/A

Order	Source	Dest	Network ID	Start Time	End Time	Order Specific
Key Management – Zeroize	SNMU	NU	N/A	N/A	N/A	N/A
Key Management – Load	SNMU	ALL	N/A	Required	N/A	N/A
Key Management – Rollover	SNMU	ALL	N/A	OPT	N/A	N/A
Radio Power Management	SNMU NMU	NU/Net NU/Net	Required	OPT	OPT	Required

Figure 3B.3-1 Orders

When an order requires network parameters, the parameters are sent in a separate network parameters message after the order. The network parameter message is a mandatory part of the order. The SNC waits until both the order and the network parameters message are received before processing the order. [Figure 3B.3-2](#) lists the orders and their corresponding network parameters message.

Order	Additional Message
Initialize New Network (DLP NCS)	Network Parameters (DLP NCS) (30Eh)
Initialize New Network (SNC NCS)	Network Parameters (SNC NCS) (306h)
Initialize New Network (Probing)	Network Parameters (Probing) (307h)
Re-initialization (DLP NCS)	Network Parameters (DLP NCS) (30Eh)
Re-initialization (SNC NCS)	Network Parameters (SNC NCS) (306h)
Re-initialization (Media only)	Network Parameters (DLP NCS) (30Eh) ¹
Re-initialization (Probing)	Network Parameters (Probing) (307h)
Reconfiguration (DLP NCS)	Network Parameters (DLP NCS) (30Eh) ²
Reconfiguration (SNC NCS)	Network Parameters (SNC NCS) (306h) ²
¹ For Re-initialization (Media only) only the media parameters of the 'Network Parameters (DLP NCS)' (30Eh) message are used; the NCS portion of the message is not used. ² For Reconfiguration orders only the NCS portion of the Network Parameters message is used, the media parameters in the message are not used.	

Figure 3B.3-2 Additional Input Messages For Each Order

When the SNC receives an order from the DLP, it validates the order. The SNC may reject an order for a number of reasons, some of which are listed below. The [\[SNC SS\]](#) provides more information on why the SNC may reject an order.

- SNC does not have the correct role to send the order
- Order conflicts with existing state of the network or system

- Order conflicts with existing orders or commands being processed
- Associated Network Parameters message was not received within 10 seconds
- Order and associated Network Parameters message are inconsistent (for example, order Start Time is not the same as Network Start Time in the additional message)
- Invalid field, for example:
 - Start time is less than 10 minutes in the future
 - Required field is not set
 - Unused field is set
 - Invalid addressing for order type

The SNC sends validated orders to the destination NUs, and waits for replies. The SNC reports each reply to the DLP in a 'Received Order Compliance' (429h) message. If a NU does not reply within 10 minutes, the originating SNC retransmits the order to those NUs that have not replied, if there is time left before the start time of the order, and only if the order has not already been retransmitted. If there is still no reply, the SNC informs the DLP of the timeout.

3B.3.2 Function Management Switches

Link 22 allows certain functions related to orders to be automated so that the SNC can take action without operator intervention. Two levels are identified for each order: compliance and execution of the order. The DLP can change any of these values as often as necessary by sending the 'Function Management Setup' (335h) message any time after the 'MPT Specification Message' (301h) has been acknowledged by the SNC, as shown in [Figure 3B.3-3](#). Because this message can be sent at any time, no other message is included in the figure.

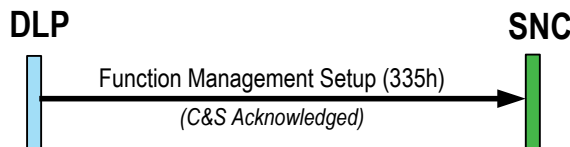


Figure 3B.3-3 Changing Function Management Switches

In other words, for every order there are two Function Management Switches.

- Automatic Compliance Switch (ACS)
 - Determines whether the SNC automatically sends the order compliance or not
- Automatic Perform Function Switch (APFS)
 - Determines whether the SNC automatically processes the order or not, after a positive compliance

The default ACS and APFS settings for each Order were shown in Chapter 2, [Figure 2C.2-6](#). Most functions are set to be performed automatically by the SNC, except those where it may be critical to have operator input/confirmation (such as SN Shutdown).

3B.3.3 Order Protocol

When an SNC receives a Network Management Order, the SNC sends the received order to the DLP, with all of the original order data, plus the following additional data.

- Information Only Flag
 - Indicates whether the order is addressed to this NU or not
- Originator
 - Link 22 Address of the NU that sent the order
- ACS/APFS
 - Current settings of the function management switches, so that the DLP knows what responses it needs to supply, if any

If the Information Only Flag indicates that the order is not addressed to this NU, the SNC and DLP take no further action. The DLP may inform the operator of the information it has received, but this is implementation dependent.

If the order is addressed to this NU, order compliance (for example, WILCO, CANTCO) is supplied by the DLP or SNC, depending on the ACS switch. For each received order, there is a corresponding message that is used to perform the order, as listed in [Figure 3B.3-4](#). After a WILCO, when APFS is OFF, the ordered DLP sends this message to the SNC. When APFS is ON, the SNC internally sends the message to itself.

Order	Source	Destination	Response to Received Order
SN Closedown	SNMU	ALL	Stop Communication (319h)
NN Closedown	SNMU NMU	NMU Net	Order (333h) - (NN Close Down) Stop Communication (319h)
Leave Super Network	SNMU	NU	NU Leave (31Ah) - (Leave All Networks)
Leave Network	SNMU NMU	NU NU	NU Leave (31Ah) - (Leave a Network) NU Leave (31Ah) - (Leave a Network)
Join an existing Network	SNMU	NU	Network Late Initialization Request (327h)
Assume SNMU Role	SNMU	NU	Role Change (31Bh)
Assume Standby SNMU Role	SNMU	NU	Role Change (31Bh)
Assume NMU Role	SNMU NMU	NU NU	Role Change (31Bh) Role Change (31Bh)
Assume Standby NMU Role	SNMU NMU	NU NU	Role Change (31Bh) Role Change (31Bh)
Insert LNE Slot	SNMU	NMU	Insert LNE Slot (32Ah)

Order	Source	Destination	Response to Received Order
Remove LNE Slot	SNMU	NMU	Remove LNE Slot (32Bh)
Radio Silence ON - SN - Single NU	SNMU	NU	Radio Silence (308h)
Radio Silence ON - NILE Network - Single NU	SNMU NMU	NU NU	Radio Silence (308h) Radio Silence (308h)
Radio Silence ON - Super Network	SNMU	ALL	Radio Silence (308h)
Radio Silence ON - NILE Network	SNMU NMU	Net Net	Radio Silence (308h) Radio Silence (308h)
Radio Silence OFF - SN - Single NU	SNMU	NU	Radio Silence (308h)
Radio Silence OFF - NILE Network - Single NU	SNMU NMU	NU NU	Radio Silence (308h) Radio Silence (308h)
Radio Silence OFF - Super Network	SNMU	ALL	Radio Silence (308h)
Radio Silence OFF - NILE Network	SNMU NMU	Net Net	Radio Silence (308h) Radio Silence (308h)
Initialize New Network (DLP NCS)	SNMU	Net	Network Parameters (DLP NCS) (30Eh)
Initialize New Network (SNC NCS)	SNMU	Net	Network Parameters (SNC NCS) (306h)
Initialize New Network (Probing)	SNMU	Net	Network Parameters (Probing) (307h)
Re-initialization (DLP NCS)	SNMU	NMU	Network Parameters (DLP NCS) (30Eh)
Re-initialization (SNC NCS)	SNMU	NMU	Network Parameters (SNC NCS) (306h)
Re-initialization (Media only)	SNMU	NMU	Change Media Parameters (30Fh)
Re-initialization (Probing)	SNMU	NMU	Network Parameters (Probing) (307h)
Reconfiguration (DLP NCS)	SNMU	NMU	Network Reconfiguration Request (DLP NCS) (310h)
Reconfiguration (SNC NCS)	SNMU	NMU	Network Reconfiguration Request (SNC NCS) (329h)
Reconfiguration (DTDMA ON)	SNMU	NMU	DLP DTDMA Change (311h)
Reconfiguration (DTDMA OFF)	SNMU	NMU	DLP DTDMA Change (311h)
Key Management – Zeroize	SNMU	NU	Key-Zeroization Request (321h)
Key Management – Load	SNMU	ALL	No Function performed by the SNC
Key Management – Rollover	SNMU	ALL	Key-Rollover Request (320h)
Radio Power Management	SNMU NMU	NU/Net NU/Net	SPC Radio Power Request (32Dh) SPC Radio Power Request (32Dh)

Figure 3B.3-4 DLP-to-SNC Interface Message used for each Order

□ ***SNC Processes Order Automatically***

When the ordered SNC is set to automatically comply and process the order, the SNC sends a WILCO to the originating SNC, and internally sends itself the command for the order and processes it. This internal command is shown with a loop arrow in the figure. An example of this protocol is shown in [Figure 3B.3-5](#), for an order from the SNMU.

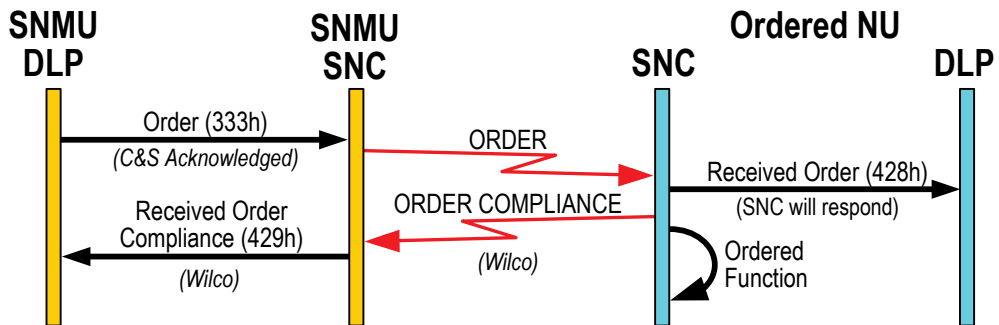


Figure 3B.3-5 Automatic Order Protocol Flow

□ **DLP Responds to Order**

When the ordered SNC is not set to automatically comply with or process the order, the SNC informs the originating SNC that the order was received, and the DLP is processing it, if there is time to send it before the DLP responds.

The DLP and/or operator must decide whether the NU can comply or not and, after the decision is made, the DLP informs the SNC of the decision, and the SNC sends the decision to the originating SNC. If the DLP 'WILCO'ed the order, the DLP then sends the message to perform the function to the SNC, and the SNC processes it. An example of this protocol is shown in [Figure 3B.3-6](#) for an order from the NMU.

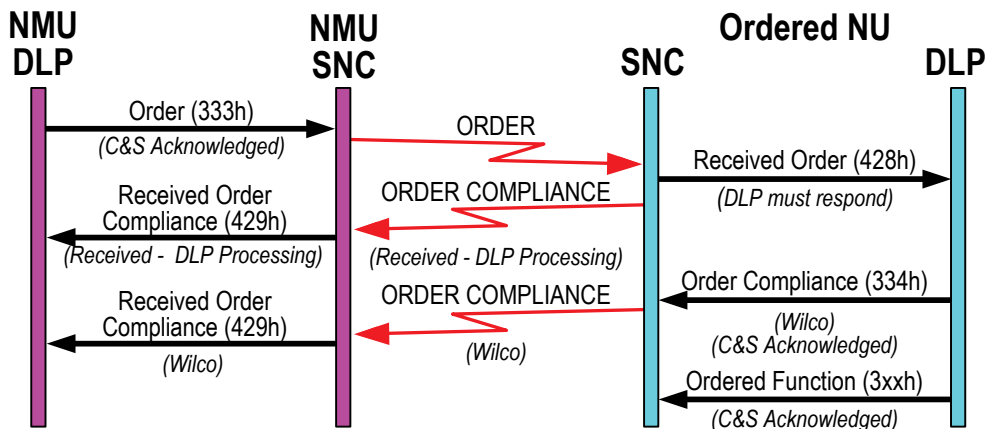


Figure 3B.3-6 Non-Automatic Order Protocol Flow

Multiple transmissions of the ORDER COMPLIANCE technical message by the ordered NU only occur when the events are separated in time. The multiple messages keep the order originator informed of the order progress when the protocol takes longer to complete. If the protocol completes quickly, so that multiple ORDER COMPLIANCE technical messages would be queued before being transmitted, only the last one is sent.

□ **Other ACS/APFS Combinations**

Some orders default to ACS off, and APFS on. In this case, the DLP must accept the order, and then the SNC automatically processes the order without further exchange from the DLP, as shown in [Figure 3B.3-7](#).

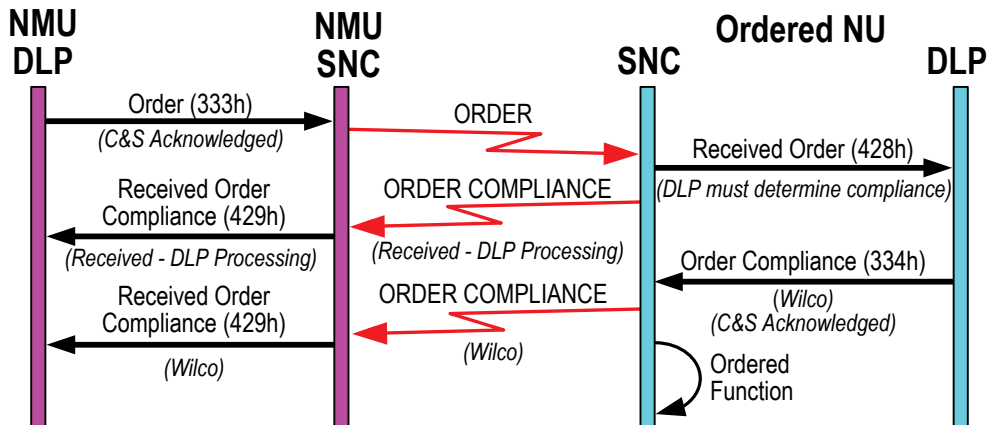


Figure 3B.3-7 ACS=Off, APFS=On Order Protocol Flow

Although possible, it is not likely that APFS would be off when ACS is on. This would mean that the SNC automatically sends a WILCO for the order, but then waits for the DLP to send the message to perform the function.

□ ***Orders with an Additional Message***

When an order requires additional data, extra technical messages are sent with the order, and after the SNC receives all of the related messages, it sends the received order and an extra related message to the DLP. These extra messages are listed in [Figure 3B.3-8](#).

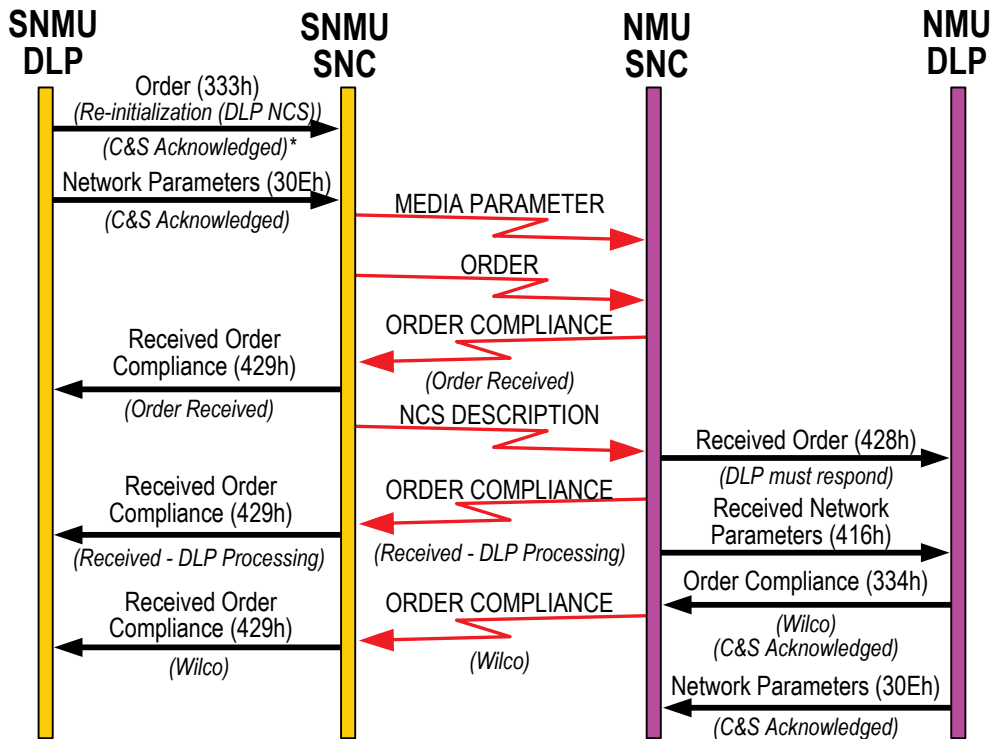
Order	Technical Messages	Additional Message upon Reception of Order
Initialize New Network (DLP NCS)	MEDIA PARAMETER NCS DESCRIPTION	Received Network Parameters (DLP NCS) (416h)
Initialize New Network (SNC NCS)	MEDIA PARAMETER NCS NEEDS	Received Network Parameters (SNC NCS) (42Ah)
Initialize New Network (Probing)	MEDIA PARAMETER NU LIST	Received Network Parameters (Probing) (403h)
Re-initialization (DLP NCS)	MEDIA PARAMETER NCS DESCRIPTION	Received Network Parameters (DLP NCS) (416h)
Re-initialization (SNC NCS)	MEDIA PARAMETER NCS NEEDS	Received Network Parameters (SNC NCS) (42Ah)
Re-initialization (Media only)	MEDIA PARAMETER	Received Network Parameters (DLP NCS) (416h)
Re-initialization (Probing)	MEDIA PARAMETER NU LIST	Received Network Parameters (Probing) (403h)
Reconfiguration (DLP NCS)	NCS DESCRIPTION	Received Network Parameters (DLP NCS) (416h)
Reconfiguration (SNC NCS)	NCS NEEDS	Received Network Parameters (SNC NCS) (42Ah)

Figure 3B.3-8 Additional Messages for Each Order

The bundle of technical messages may be received in any order. When the SNC of the receiving NU receives the ORDER technical message, and is still waiting for additional related messages, the SNC informs the originating SNC that the order was received, and no retransmissions of the order are necessary. If the SNC does not receive all of the associated technical messages within 2 minutes, it requests the information by sending a RETRANSMISSION REQUEST technical message to the originating SNC. If after 10 minutes all of the information has not been received by the ordered SNC, it discards the order and does not send any WILCO or CANTCO response.

The SNC sends the received order and associated message to its DLP only after it receives all necessary information. An example of a Re-initialization (DLP NCS)

order from the SNMU to the NMU, with ACS and APFS off at the NMU, is shown in Figure 3B.3-9.



* 'C&S Acknowledgement' not sent until after 'Network Parameters' message is received

Figure 3B.3-9 Example of Order with Additional Parameters (Non-Automatic)

3B.4 Command Queuing

Messages that are far enough in the future are not processed immediately. Instead, they are queued and processed closer to the start time for the message. This allows the commands to be cancelled, and helps to prevent potential inconsistent commands from being performed. This section covers the following topics.

- Queuing Commands
- Queue Processing
- Cancelling Commands

3B.4.1 Queuing Commands

The messages listed in [Figure 3B.4-1](#) all have a start time which can be in the future. If the message is more than 20 minutes in the future, the receiving SNC will put the message on a queue, if it does not conflict with messages already on the queue or being processed. At 20 minutes prior to the start time, the message is “activated”: it is removed from the queue, protocol processing is performed, and the message is transmitted as necessary.

Message Name	Number
Network Parameters (SNC NCS)	306h
Network Parameters (Probing)	307h
Radio Silence	308h
Network Parameters (DLP NCS)	30Eh
Change Media Parameters	30Fh
Network Reconfiguration Request (DLP NCS)	310h
DLP DTDMA Change	311h
Create MASN	313h
Modify MASN	314h
Delete MASN	315h
Stop Communication	319h
NU Leave	31Ah
Role Change	31Bh
Change Relay Settings	31Ch
Key-Rollover Request	320h
Network Late Initialization Request	327h
Network Reconfiguration Request (SNC NCS)	329h
Insert LNE Slot	32Ah
Remove LNE Slot	32Bh
SPC Radio Power Request	32Dh
Order	333h

Figure 3B.4-1 Messages that can be queued by the SNC

3B.4.2 Queue Processing

The SNC performs the following validation of messages it receives from the DLP.

- Is the message valid – does NU Role allow the command, are the fields valid? For example, it validates the following
 - Media parameters validity
 - NCS validity, with the media parameters in the received command (if any) or in the queued commands that alter media
 - Link22 address existence
- Does the command overlap any queued commands of the same kind in its activation window (20 minutes before the command start time up to the command start time)? These types of overlapping commands are rejected
- Is the command consistent with the current SNC status and the queue content? Ensures that the new command will not introduce an inconsistency and that the queue is not already inconsistent, due to previous item cancellations. Checks include the following
 - Already queued items with Start Time earlier than the new command are checked against each other to make sure the queue is coherent before the new insertion
 - The new item is checked against the affected element status against all the queue entries to make sure the new insertion produces no incoherencies (for instance, a NN Closedown of a non-existing network or a MASN modification for a deleted MASN will be rejected)

If any of the validation fails, the SNC rejects the message and informs the DLP with a negative ‘SNC C&S Acknowledgement’ (421h) message, indicating the reason for rejection.

At activation time (20 minutes before start time), the SNC processes the queued command, which includes any necessary transmissions to other NUs, and marks it as “being processed”. Internally, the SNC leaves the command on the queue at this point. The command can no longer be cancelled, and is not sent to the DLP upon request of queued messages. It remains on the internal SNC queue so that the SNC can still use it for further checks when queuing other commands. At the command start time, the command is removed from the queue, since it has been executed.

Most orders or commands are not affected by ones already in the queue. [Figure 3B.4-2](#) lists which messages can be rejected due to queued messages.

Order or Command Message	Restrictions
Re-initialization (All Types)	No two events for the same network within 20 minutes
Reconfiguration (DLP NCS)	
Reconfiguration (SNC NCS)	
Relay Setting	No two events for the same unit within 20 minutes
Insert LNE	No two events for the same network within 20 minutes
Remove LNE	No two events for the same network within 20 minutes
Role Change	No two events for the same role within 20 minutes
NU Leave Stop Communications	No two events for the same unit on the same network within 20 minutes

Figure 3B.4-2 Restrictions when queuing Orders or Commands

3B.4.3 Cancelling Commands

Queuing of messages allows the operator (through the DLP) to cancel any of the messages that are still on the queue, prior to activation. The operator can request a list of the messages that are on the queue, as discussed in Chapter 2, section [2C.2.2 Advanced NU Management](#). When a queued message is to be cancelled, the DLP sends the original message to the SNC with the Message Variant field set to Cancel. The contents of the message are used to identify the message on the queue that is to be cancelled. The SNC will delete the message from the queue that matches the message input, if any, and inform the DLP of the results of the request. This protocol is shown in [Figure 3B.4-3](#).

When an ‘Order’ (333h) message with an associated network parameters message is queued, the network parameters are stored with the Order on the queue, not as a separately queued message. Only the Order needs to be sent to cancel it. When an order is cancelled, any associated network parameter information is automatically deleted by the SNC.

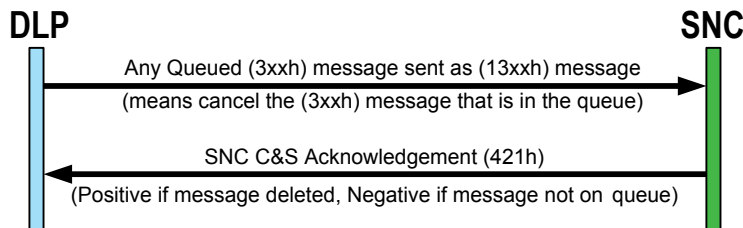


Figure 3B.4-3 Cancelling of Queued Command and Status Message

3B.5 SN Directory Maintenance

Every unit in the Super Network maintains its own copy of the Super Network (SN) Directory. The SN Directory consists of the following components.

- Address
 - 15-bit Link 22 Address of every unit
 - 7-bit NILE Address of every unit
- MASN
 - MASN Membership
- Role
 - SNMU
 - Standby SNMU
 - NMU for each Network
 - Standby NMU for each Network
- Status
 - NU Status of every unit at Super Network level
- Relay
 - NU Relay Setting of every unit at Super Network level

For each component, every SNC stores the OLM values supplied by the DLP during initialization, as detailed in section [3B.1.3 Super Network Directory Configuration](#). Every SNC also maintains the current version of all the components which by default is initialized to be the OLM version. The current version of the Address, MASN, Status, and Relay components, are identified by a version number. The current Role component does not have a version number.

Ideally every unit in the Super Network should have the same SN Directory. The SNC of the SNMU maintains the master SN Directory, and distributes all changes. Each SNC uses the version numbers to automatically detect and solve inconsistencies in the Address, MASN, Status, and Relay components. Roles are distributed whenever they change and periodically after the first change has occurred.

This section contains the following subsections.

- [SN Directory Components](#)
- [SN Directory Maintenance](#)

3B.5.1 SN Directory Components

This section discusses the details of each of the following SN Directory components, and describes how they are changed. Radio Silence is included, as it affects NU Status.

- Address
- MASN
- Role
- Status
- Relay

□ Address

Every unit is assigned a unique 15-bit Link 22 Address, as detailed in [2B.2.3 NILE Unit Parameters](#). To save bandwidth when communicating address information, the Link 22 Address is mapped to a 7-bit NILE Address. The NILE Address only uses the values in the range 1-125 decimal. Values 0, 126 and 127 are not used.

NILE Addresses normally start at 1, but can be configured to start with a higher number by setting the Lowest Allocatable NILE Address in the OLM to a different value. This allows different Super Networks to be configured with different subsets of NILE Addresses, to avoid NILE Address conflicts if two or more Super Networks are merged together.

During SNC Initialization, the DLP sends the Lowest Allocatable NILE Address, and the list of Link 22 addresses, as provided in the OLM, using the ‘Link 22 Super Network Participants’ (304h) message. The first unit listed in the message is assigned a NILE Address equal to the Lowest Allocatable NILE Address. The next unit in the message is assigned the next NILE Address, which is repeated for all subsequent units in the message. [Figure 3B.5-1](#) shows an example of address allocation with five units. The SNC stores this mapping of Link 22 Address to NILE Address in the SN Directory. It is important that the mapping is the exactly the same on every unit, and so the order of the units in the message supplied by the DLP must be the same as in the OLM.

'Link 22 Super Network Participants' (304h) message	NILE Address
Lowest Allocatable NILE Address = 10	
Number of NUs = 5	
Link 22 Address 00100	10
Link 22 Address 00500	11
Link 22 Address 00400	12
Link 22 Address 00200	13
Link 22 Address 00300	14

Figure 3B.5-1 Link 22 to NILE Address Mapping Example

When the DLP of the SNMU needs to add a unit that is not a member of the Super Network (in other words, the unit does not already have a NILE Address), it requests its SNC to allocate a NILE Address by sending a 'NILE Address Allocation Request' (31Fh) message, as shown in [Figure 3B.5-2](#).

If the message is valid, the SNC allocates the next available NILE address and replies with a 'NILE Address Allocated' (40Fh) message, which indicates the version number associated with the change. The SNMU SNC sends the DIRECTORY ADDRESS technical message to inform all other units of the change to the Address component of the SN Directory, and all other units inform their DLPs with the 'NILE Address Allocated' (40Fh) message.

If the number of available NILE addresses drops below ten, the SNC of the SNMU and the SNC of the Standby SNMU send to their DLP a 'NILE Address Availability' (410h) message indicating the number of free addresses left.

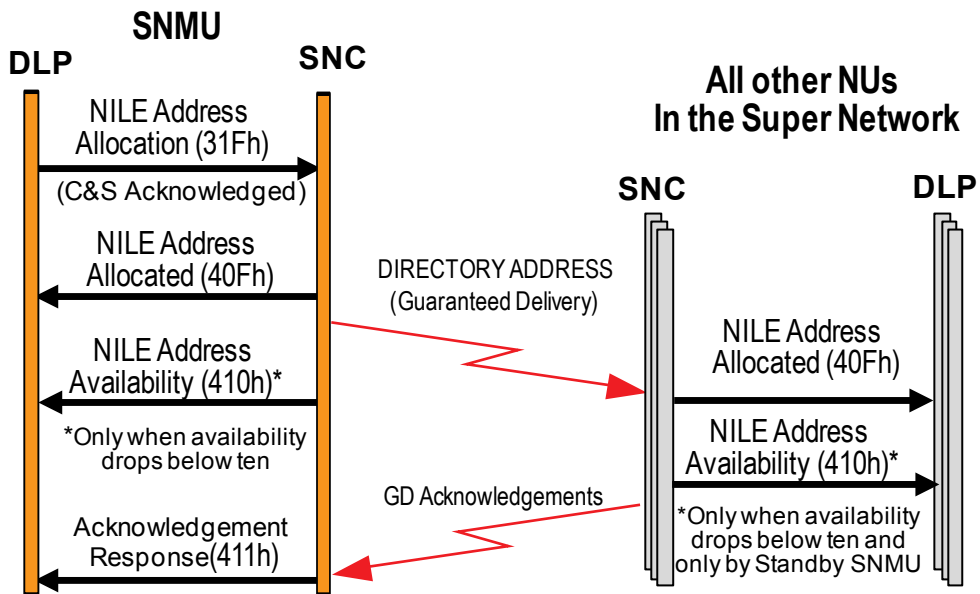


Figure 3B.5-2 NILE Address Allocation

□ MASN

A MASN is a logical group of units which is used to minimize the size of Service Headers when addressing messages to multiple units. Two types of MASNs are defined.

- Tactical MASNs
 - Assigned initially by the OLM and then modified by the SNMU Operator
 - Used to address tactical messages
- Technical MASNs
 - Statically defined
 - Used to address technical messages

MASNs reduce the bandwidth used when addressing a group of units, and are used to ensure the users received the data, especially in a dispersed and congested environment. A MASN is not defined to segregate or restrict data. The MASN concept is similar, but not the same as, a Link 16 Network Participation Group (NPG).

The NPG works as a destination address, but also as a receiving filter because of the need to maximize the use of the channel.

There are 32 tactical MASNs numbered 0-31. MASNs 1–8 are defined as the network membership MASNs for networks 0–7. During SNC initialization, each DLP sends all the predefined MASNs in the OLM to its SNC, using the ‘Create MASN’ (313h) message, as detailed in [Section 3B.1.3 Super Network Directory Configuration](#). MASNs 1-8 are mandatory for all the defined Networks, and are defined by the OLM network membership as detailed in Appendix B, section [B.1.2 Determining Network Membership](#).

Tactical MASNs 0 and 9-31 can include any subset of Super Network units and do not need to be members of the same network.

During Link 22 operations, the DLP of the SNMU can instruct its SNC to change the tactical MASN composition. All changes are required to be sent 10 minutes in advance of their indicated TOD, because the changes are generated sequentially based on TOD for each individual MASN. The DLP of the SNMU can make the following changes, by sending the associated message to its SNC.

- A new MASN may be created, using ‘Create MASN’ (313h) message
- An existing MASN may be modified by adding or removing unit(s), using ‘Modify MASN’ (314h) message
- An existing MASN may be deleted using ‘Delete MASN’ (315h) message

The SNC of the SNMU sends the MASN CREATE, MASN MODIFY, MASN DELETE, or MASN COMPACT technical message to inform all other units of the change to the MASN component of the SN Directory. The MASN COMPACT technical message is used instead of MASN CREATE or MASN MODIFY when the size of the message is less than the non-compact version.

The message flows are shown in [Figure 3B.5-3](#).

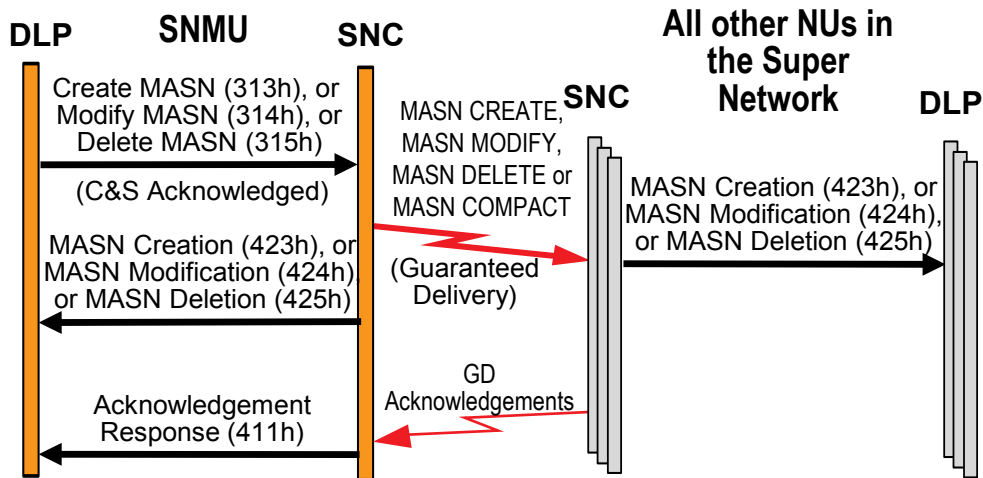


Figure 3B.5-3 MASN Change Distribution

Technical MASNs are predefined within the SNC and [Figure 3B.5-4](#) details the meaning of the Technical MASNs.

MASN ID	Technical Destination Address Set
0	SNMU and Standby SNMU
1-8	All units in Network #0-7, respectively
9-16	NMU and Standby NMU for Network #0-7, respectively
17	SNMU
18	NU Performance MASN - SNMU and Standby SNMU plus the NMU and Standby NMU for all networks of which the source unit is a member
19-31	Unused

Figure 3B.5-4 Technical MASNs

The SNC initializes the list of units in the technical MASNs during SNC Initialization upon receipt of the ‘Super Network Special Duties’ (305h) message and ‘Create MASN’ (313h) messages for the defined Networks. It updates the technical MASNs during operation, when it receives role change information and network membership MASN changes.

□ **Role**

Certain units within the Super Network have special duties, which are called Roles. The initial allocation of these Roles is defined during network planning. The special Roles at the Super Network level are as follows.

- Super Network Management Unit (SNMU)
- Standby SNMU
- Network Management Unit (NMU), one for each Network
- Standby Network Management Unit (NMU), one for each Network

Role changes can be planned or unplanned during operations.

■ **Planned Changes**

Planned role changes can be ordered by the SNMU. Planned role changes that just affect the network role units (NMU or Standby NMU) can be ordered by the NMU of a Network. The DLP of the SNMU or the NMU informs its SNC of role changes using a 'Role Change' (31Bh) message, which the SNC uses to update its SN Directory.

After the ordered new SNMU has agreed to become the SNMU (WILCO to the order), the SNMU notifies everyone of the change. [Figure 3B.5-5](#) describes the message flow for the SNMU notifying everyone that there will be a new SNMU at the specified time.

The SNC notifies its DLP of role changes using a 'Role Status' (40Dh) message.

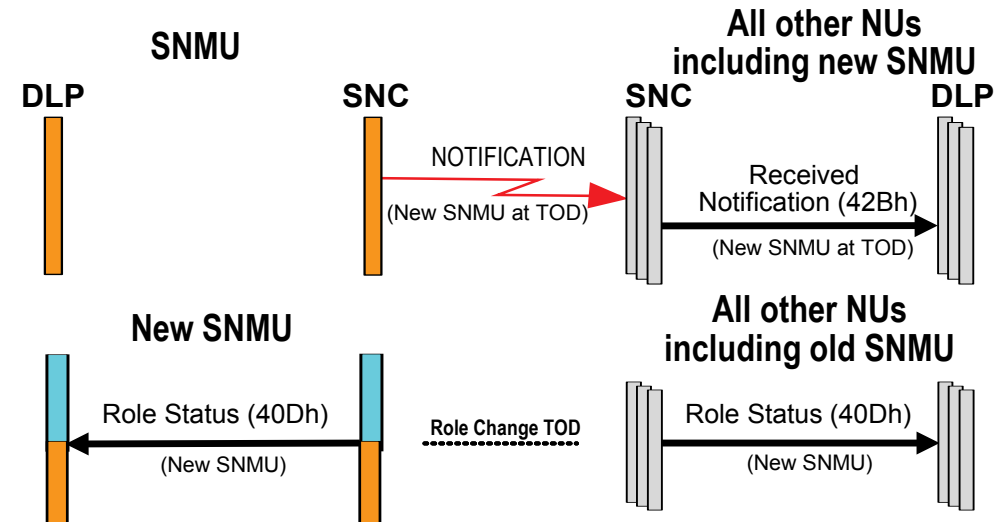


Figure 3B.5-5 Notification of Planned Role Change

■ **Unplanned Changes**

The SNC of a unit with a role monitors the received messages and provides the DLP with an update when a change is detected, using the ‘Role Status’ (40Dh) message, which contains all the current known roles.

If the primary role (SNMU or NMU) is lost, and the standby SNC is set in automatic mode, it automatically assumes the primary role and notifies everyone.

The DLP can control whether the SNC of a Standby unit automatically takes over the primary role when communication is lost, or whether it only notifies the DLP of the detected loss. This behavior can be defined in the OLM. The DLP sends the ‘Role Takeover Control’ (331h) message to its SNC, setting the message fields as indicated in [Figure 3B.8-6](#). By default, the SNC of the standby does not automatically assume the primary role when a loss is detected.

Field	Range	Explanation
SNC Role Automatic Takeover Flag	0/1	When set to 1 indicates that automatic takeover by the SNC is enabled, when zero it is disabled
Role Loss Timeout	2-15	The number of minutes that the SNC should wait before declaring the loss of the primary role

Figure 3B.5-6 Role Takeover Control Message Information

The SNC of each unit continuously monitors the received traffic. If the SNC detects conditions that may affect the reliability of loss detection, it temporarily disables the automatic takeover. The SNC of the Standby SNMU or Standby NMU can only automatically take over the role if all the following conditions are true.

- The Standby can exchange messages with at least one neighbor
- TOD input, LLCs and SPCs are fully functional

The SNC notifies the DLP of changes using the ‘SNC Status’ (413h) indicating if the Status is Enabled or Disabled for the Super Network or any individual Network upon change.

If both units performing SNMU and Standby SNMU are lost, any unit can assume the role of SNMU, by the DLP sending a ‘Role Change’ (31Bh) message to its SNC. The new SNMU must then nominate a new Standby SNMU.

In order to ensure periodic traffic between units, each SNC generates HEARTBEAT technical messages with a frequency of thirty seconds for role units and two minutes for all other units.

The SNC of the acting SNMU periodically (every 300 seconds) sends the complete list of roles, to ensure that all NUs have the same view. This allows recovery and provides the information to ‘receive only’ or ‘radio silent’ units that cannot request it.

□ **Status**

The Status component consists of the NU Status of every NU in the Super Network. There is a Version Number for the Status component. The following subcomponents of the Status component are discussed.

- NU Status
- Radio Silence

■ **NU Status**

Every unit has a NU Status within the Super Network, as defined in [Figure 3B.5-7](#).

NU Status	Definition
Active	Any unit that has timeslots assigned, and is able to transmit and receive
Radio Silent	Any unit that has timeslots assigned, but by choice or order is not allowed to transmit. It is able to receive, but not send and acknowledge messages. It may break the 'Radio Silence' status and inject messages upon request of its own DLP
Receive Only	Any unit that has NO timeslots assigned. It is able to receive.
Inactive	Any unit currently not part of the Super Network (Failure, Maintenance, etc.) with or without timeslots assigned

Figure 3B.5-7 NU Status Definition

Every 60 seconds, each DLP receives a ‘NU Data’ (606h) message from its SNC, which contains information about the last time a message was received from each unit, and its distance from each unit in the Super Network. The SNMU DLP can use this message to assess when a unit should be considered Inactive.

When becoming active in any Network, the SNC generates the NU PERFORMANCE technical message, and continues to send it periodically every 20 minutes. This message is distributed to the SNMU and Standby SNMU and the NMU and Standby NMU of the networks where the unit is active, and is the main source used by the SNC of the SNMU to detect changes in the network and Super Network status of each unit. When receiving this technical message, the SNC sends ‘NU Performance Data’ (427h) messages to its DLP, which is described in section [2C.2.3 NU Performance Data](#) subsection.

The state transitions between the NU Status values, the source of the transition (whether the SNC can determine the change or only the DLP can) and the cause of the transition are listed in [Figure 3B.5-8](#).

Current State	New State	Source	Cause of Transition Between States at the SNMU
Inactive	Active	SNC	Reception of NU Performance technical message from the unit
Inactive	Receive Only	DLP	No information is transmitted by the unit so can only be externally defined. This is the case when a unit performs LNE and no capacity is assigned
Inactive	Radio Silence	DLP	No information is transmitted by the unit so can only be externally defined. This is the case when a unit initializes in Radio Silence mode
Active	Inactive	SNC	When a unit leaves the Super Network in a controlled manner (either because it decides to itself or is ordered to by the SNMU)
Active	Receive Only	SNC	When a unit is not included in a new NCS when it previously was due to a Reconfiguration or Re-Initialization of the network
Active	Radio Silence	SNC	Reception of NOTIFICATION Technical messages
Receive Only	Inactive	DLP	No information is transmitted by the unit so can only be externally defined, based also on 'NU Data' (606h)
Receive Only	Active	SNC	Reception of NU Performance technical message from the unit
Receive Only	Radio Silence	DLP	External addition confirmation required
Radio Silence	Inactive	DLP	No information is transmitted by the unit so can only be externally defined, based also on 'NU Data' (606h)
Radio Silence	Active	SNC	Reception of NU Performance technical message from the unit
Radio Silence	Receive Only	SNC	When a unit is not included in a new NCS when it previously was due to a Reconfiguration or Re-Initialization of the network

Figure 3B.5-8 Causes of Transitions between States

What might happen when a unit has an incorrect status is listed in [Figure 3B.5-9](#).

Incorrect State	Correct State	Possible Issues
Inactive	Active Receive Only Radio Silent	Unit may not receive messages that need to be relayed to it
Active Receive Only Radio Silent	Inactive	Bandwidth may be wasted trying to communicate with the unit
Active	Radio Silent Receive Only	Other units will not receive responses from the unit that the units may be waiting for
Receive Only	Active	The unit may not be assigned any NCS capacity, and thus may not be able to transmit

Figure 3B.5-9 Possible Issues Due To Temporary Incorrect NU Status

If the DLP of the SNMU knows or detects that a NU has changed state in the Super Network, and the SNC may not know, the DLP of the SNMU can instruct its SNC to modify the Status of that unit with a ‘NU Status’ (32Fh) message, as shown in [Figure 3B.5-10](#). The SNMU SNC sends the NU STATUS technical message to all units to inform them of the change to the Status component of the SN Directory.

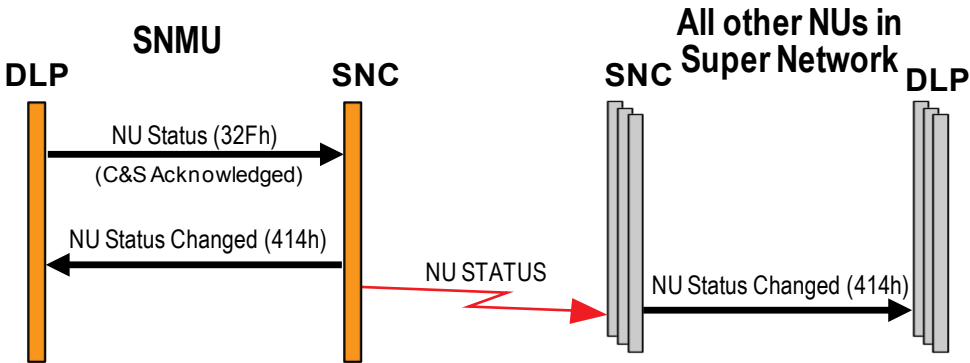


Figure 3B.5-10 NU Status

■ **Radio Silence**

Each unit can be radio silent on a Network or in the Super Network. A Network or the entire Super Network can also be Radio Silent, but a unit’s NU Status is only affected by individual unit radio silence changes. If the entire Super Network is Radio Silent the SNMU does not change every NU Status to Radio Silent. Changes to the Radio

Silence Status of an individual unit can be initiated by the SNMU in any Network or Super Network, or by the NMU for its network, by sending an ‘Order’ (333h) message. The DLP of any unit can also initiate its own change locally, using ‘Radio Silence’ (308h) message. Radio Silence can be immediate or in the future. When ordered in the future, the ten minutes rule applies to allow enough time for notifying all other units of the planned changes. When the change is immediate, all the other units may not be notified of the changes. [Figure 3B.5-11](#) depicts the protocol flow when a unit changes to radio silence for a predetermined amount of time. The SNC of the unit changing to or from radio silence informs all other units of the change by sending the NOTIFICATION technical message.

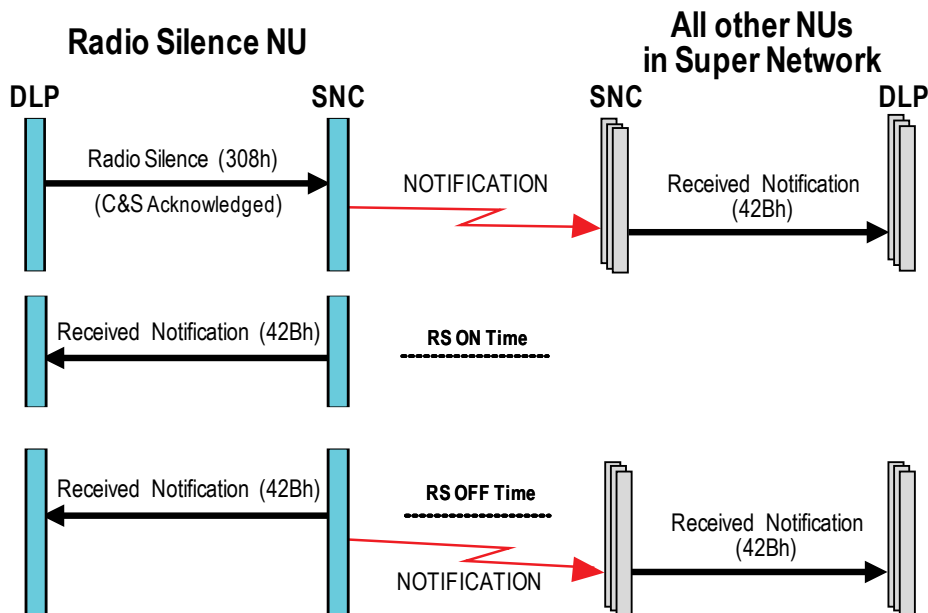


Figure 3B.5-11 Radio Silence protocol

The Radio Silent order is sent by the DLP of the SNMU or NMU to the SNC using an ‘Order’ (333h) message. The allowed combinations and the addressing mechanism are shown in [Figure 3B.5-12](#).

Role	All Units in the SN	All Units in a Network	Single Unit in the SN	Single Unit in a Network
SNMU Order	Totalcast	Network Membership MASN	Unit	Unit
NMU Order	Not Allowed	Network Membership MASN	Not Allowed	Unit

Figure 3B.5-12 Radio Silence Order

The SNC of the unit being ordered Radio Silent applies all requests based on the time of the request. This allows the SNC to accept multiple requests from SNMU, NMU and local DLP, which may be received and be valid at different TODs. The SNC enters Radio Silence at the earliest TOD of any request and exits at the latest TOD of all requests.

If the unit is Radio Silent in the Super Network, the SNMU updates the unit's NU Status to Radio Silent, and sends a NU STATUS technical message to all units to inform them of the change to the Status component of the SN Directory.

Radio Silence of critical units may generate fragmented Super Networks. The SNMU may need to ensure the Radio Silent unit always receives messages. In the case when relay is required, the SNMU needs to use 'Link Quality Status' (328h) as described in [3C.8 Relay & Routing](#).

Tactically, before going Radio Silent in the Super Network, the last PLI should have the Network Participation Status Indicator set to conditional radio silence, so that receiving units know that reporting responsibility for the unit's tracks has to be determined.

□ **Relay**

The Relay component contains the Relay Setting of each NU. There is a Version Number for the Relay component. Every unit has a Relay Setting defined within the Super Network, which can be set as indicated in [Figure 3B.5-13](#) and can influence Relay Traffic flow, as described in [3C.8 Relay & Routing](#).

Value	Explanation
Automatic	A unit determines the need for relay based on internal protocol calculations
Preferred	Tie-breaker rule, in case two or more units are equal
Inhibited	The unit shall not perform relay

Figure 3B.5-13 Relay Setting Values

If the Relay Setting of a unit is not included in the OLM, it defaults to Automatic. The DLP of the SNMU can change it by sending the 'Change Relay Setting' (31Ch) message, as shown in [Figure 3B.5-14](#). The SNMU SNC sends the RELAY SETTING technical message to all units to inform them of the change to the Relay component of the SN Directory and the current version number.

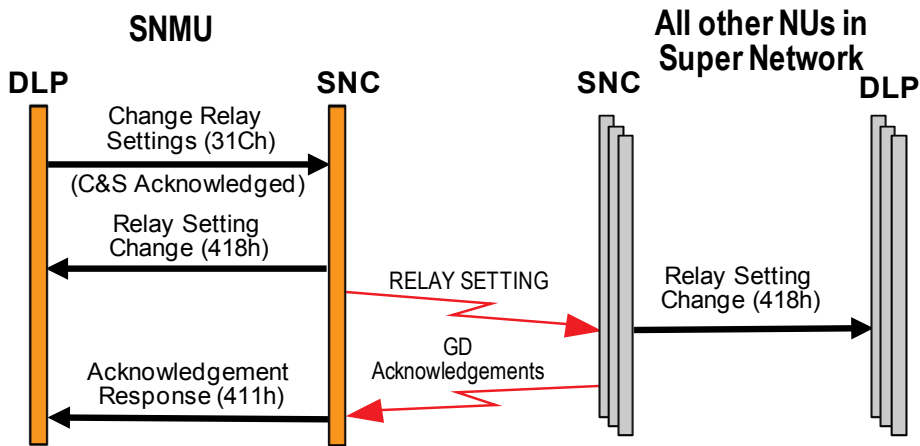


Figure 3B.5-14 Relay Setting

3B.5.2 SN Directory Maintenance

The Address, MASN, Relay, and Status components of the SN Directory are maintained by use of version numbers. The Role component is maintained without the use of a version number. Every SNC stores the original OLM version of the components as version number zero which is never changed, unless it is found to be in error. Every SNC also stores the current version of the components. The SNC of the SNMU maintains the master copy of the OLM version and the current version. All changes to the current version are distributed to the other SNCs using technical messages, containing either the complete component at the current version or the change from the current version, whichever uses the least bandwidth. If the SNC receives from the SNMU a component with a version number that is not equal to the version number of the local current component, the SNC replaces the current component and version number with that received from the SNMU. The following features are described below.

- Version Numbers
- SNC Request for SN Directory
- DLP Request for SN Directory Update
- SNMU DLP Request to send SN Directory Update
- LNE NU SN Directory Update from Support Unit
- Role Component Maintenance

□ Version Numbers

All SN Directory changes are traced using version numbers, except for Role Changes. Each component has a separate internal 32-bit version number. The SNC provides the version number to the DLP with the complete component whenever there is a change to a component. In order to save bandwidth, the SNC uses a limited numbers of bits to transmit the Version Number in any technical message, as detailed in [Figure 3B.5-15](#).

The SNC of the SNMU maintains the current version number for each component. When any unit requests realignment (requests the current version), the SNMU sends either the complete component at the current version or the change from the OLM version, whichever uses the least bandwidth. The requesting SNC then uses either the OLM version of the component and the changes supplied to form the current version, or if the complete component is received replaces its current version with that supplied.

In the case of LNE, the OLM or the current version of the component are sent directly by the Supporting Unit.

SN Directory Component	Version Number Range in Technical Messages	COMMENT
ADDRESS	0 3-125	<ul style="list-style-type: none"> Value 0 always indicates OLM Information 7-bit version number, values 3-125, as the maximum additions is 123, from 2 the minimum number of units in a SN to 125 the maximum. The values in the range (1 to the number of units in the OLM plus the lowest allocatable NILE Address minus 1) are not used, as when a NU is added the version number is set equal to the added unit's NILE Address
MASN	0 1-255	<ul style="list-style-type: none"> Value 0 always indicates OLM Information Cyclic value 1-255, is the 8-bit conversion of the internal version number
RELAY	0 1-255	<ul style="list-style-type: none"> Value 0 always indicates OLM Information. Cyclic value 1-255, is the 8-bit conversion of the internal version number
STATUS	0 1-255	<ul style="list-style-type: none"> Value 0 always indicates OLM Information. Cyclic value 1-255, is the 8-bit conversion of the internal version number

Figure 3B.5-15 Version Number

When the internal version number is transmitted in a technical message, it needs to be converted to fit the available number of bits. The Address component has a maximum value of 125, the maximum number of NUs in a Super Network. For the other components, the range is 1 to 255. There is no need for conversion if the internal value is 0 to 255. If the number is 256 or larger, the SNC converts it to a cyclic number in the range 1 to 255, using the following formula, considering that the value 0 always represents the OLM version.

$$\text{Technical Message Value} = ((\text{Internal Value} - 1) \text{ MOD } 255) + 1$$

Figure 3B.5-16 shows examples of conversion. When a request for realignment is received, the SNC of the SNMU will convert the value from external to internal.

Internal Value	0	1	2	...	255	256	257	258	...	510	511	...	765	766	...
Technical Message Value	0	1	2	...	255	1	2	3	...	255	1	...	255	1	...

Figure 3B.5-16 Conversion of Version Number from Internal value

Once the SNMU makes any change to the Address, MASN, Status, or Relay components of the SN Directory, the SNC of the SNMU automatically starts transmitting a DIRECTORY STATUS technical message with a periodicity of ten minutes. This message contains the version number value and checksum of each component. When any SNC receives the message, it checks the version number of each of its components against those received, and when the same version compares the checksum to the calculated value.

□ SNC Request for SN Directory Realignment

Whenever the SNC of any unit detects an inconsistency in its SN Directory based on the version numbers or checksums in the received DIRECTORY STATUS message, it automatically sends a DIRECTORY REQUEST technical message to the SNMU, indicating its internal version numbers. When the SNC of the SNMU receives the message, it compares the received request for each component with its internal values, and responds with a set of messages as shown in [Figure 3B.5-17](#).

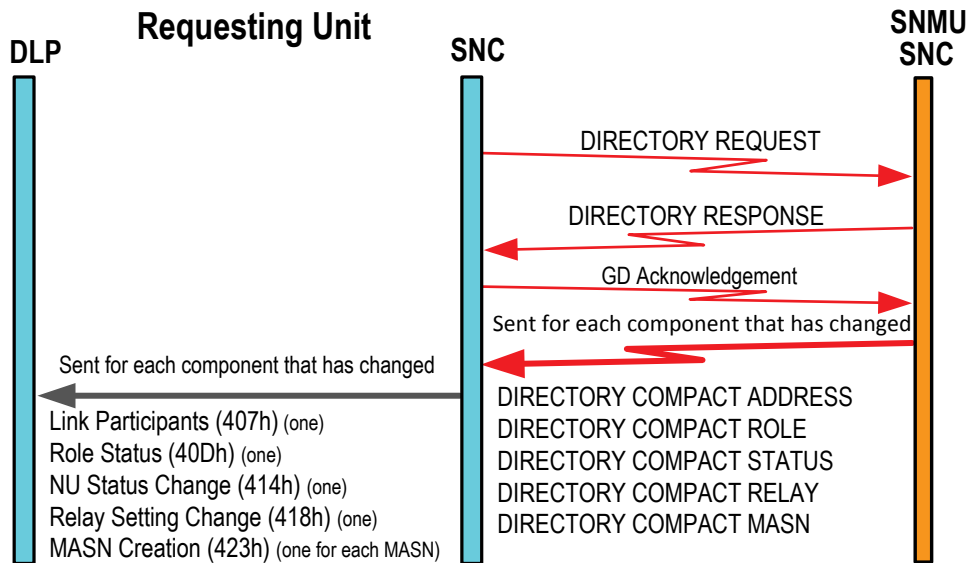


Figure 3B.5-17 SN Directory Update requested from SNMU

A **DIRECTORY RESPONSE** technical message is generated to indicate which technical messages are to be expected, if any.

If no **DIRECTORY RESPONSE** technical message is received after ten minutes, a new request is sent.

If a **DIRECTORY RESPONSE** technical message is received but some of the technical messages are still missing after ten minutes, the SNC of the requesting unit will send a modified **DIRECTORY REQUEST** technical message requesting only the messages not received.

[Figure 3B.5-18](#) provides details of the fields involved in the **DIRECTORY RESPONSE** technical message.

Value	Usage
Version Number (for Address, MASN, Status and Relay)	Version number of each Component in external representation, based on the internal SNMU version number. If changes have occurred, messages are expected
Role Changes Flag	Indicates if Role changes occurred and therefore a message is expected
Totalcast Flag	Indicates if Totalcast or Point-to-Point is involved
Destination	NILE address of the Destination if the above flag is set to Point-to-Point
Address Messages Mask	Indicates the list of expected Address messages to be received
MASN Messages Mask	Indicates the list of expected MASN messages to be received
OLM Flag	Indicates whether updates to the OLM Address or MASN components were requested and only if set are the next two fields included
OLM Address Messages Mask	Indicates the list of expected OLM Address messages to be received
OLM MASN Messages Mask	Indicates the list of expected OLM MASN messages to be received

Figure 3B.5-18 DIRECTORY RESPONSE relevant fields

□ **DLP Request for SN Directory Update**

If the DLP of a unit determines that the SN Directory is not the latest version (or other reason, such as recovery after failure), the DLP can request the SN Directory updates from the master copy held by the SNMU, as shown in [Figure 3B.5-19](#).

This activates the same protocol that is used when the SNC makes the request, as discussed in the previous section “[SNC Request for SN Directory](#)”. The SNMU replies by sending a DIRECTORY RESPONSE technical message addressed point-to-point. This message tells the SNC of the requesting unit what the current status of the SN Directory is and therefore what updates to expect.

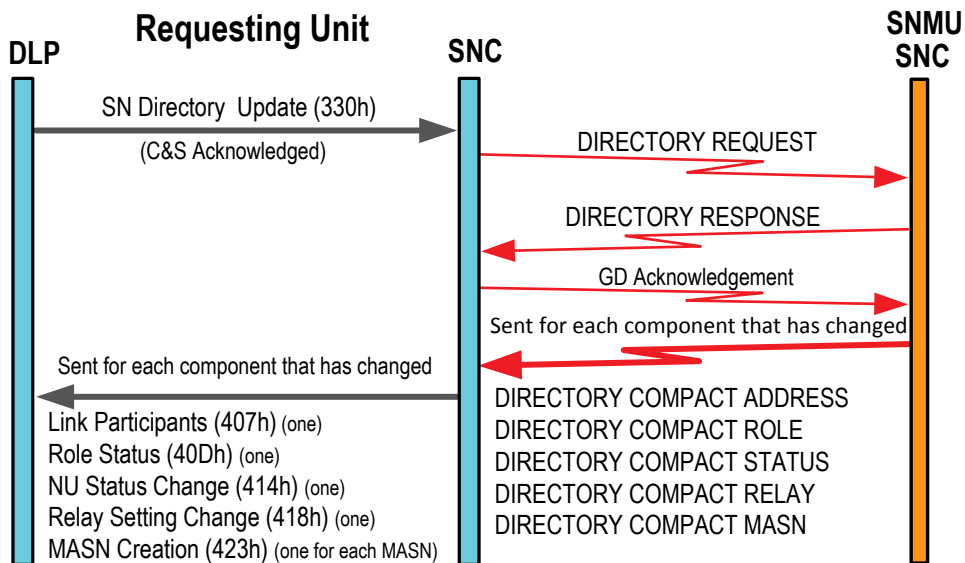


Figure 3B.5-19 DLP Request for SN Directory Update from the SNMU

❑ **SNMU DLP Request to send SN Directory Update**

The DLP of the SNMU can instruct its SNC to supply SN Directory updates to other units, by sending a ‘Notify SN Directory’ (32Eh) message to its SNC. The DLP indicates whether the notification is limited to a single unit or all units in the Super Network. [Figure 3B.5-20](#) shows the message flows when the DLP request was for all units in the Super Network.

The SNMU DLP may want to perform this action in the following circumstances.

- Re-send recent changes that have not been acknowledged by an NU
- Send the complete picture to a Silent Join LNE unit

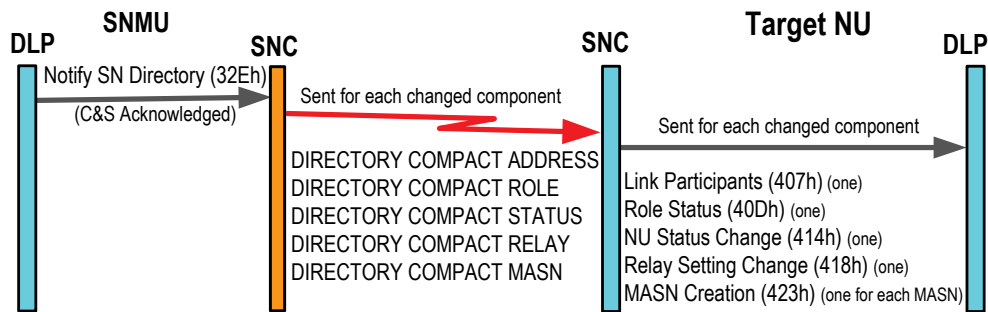


Figure 3B.5-20 SN Directory Update Notification from SNMU

❑ **LNE NU SN Directory Update from Support Unit**

If the LNE unit is not active on any network, the Supporting Unit (SU) always first sends a DIRECTORY RESPONSE technical message to inform the LNE SNC of the state of the SN Directory so that it knows what updates to expect, using the same protocol indicated when the message is received by the SNMU. The SNC of the SU sends a NU ROLES technical message if requested in the LNE REQUEST message.

❑ **Role Component Maintenance**

Once the SNMU makes a change to the Roles, the SNC of the SNMU automatically starts transmitting a NU ROLES technical message with a periodicity of ten minutes. When the SNC receives this message, it updates its internally held roles, and informs the DLP of the new role by sending a ‘Role Status’ (40Dh) message.

3B.6 DLP Request Management Info

The DLP Request Management Info protocol allows the DLP to request some of the data internally stored and maintained by the SNC, once SNC Initialization is complete. When the DLP determines that management information is needed, it sends a 'DLP Request Management Info' (312h) message to the SNC, specifying which type of data it requires from the SNC. The SNC returns the requested information in a set of messages. The DLP can request the following information.

- Request for Connectivity Data
- Request for Link Participants
- Request for Media Parameters
- Request for SN Directory Components
- Request for List of Queued Messages
- Request for Network Information
- Request for Congestion Indexes
- Request for NU Capabilities
- Request for C&S Messages

The response to each individual type of request is detailed in the following sections. For each individual request, when no response messages will be provided, an 'SNC Status' (413h) message will be sent to notify the DLP of the lack of information.

The DLP can also request the SNC to provide the selected information periodically, by setting the Periodic Reporting Flag and specifying the desired period.

The DLP can request the SNC to stop periodic transmissions, for the selected information by setting the Periodic Reporting Flag and specifying a period of zero, or for all information by setting the Reset All Periodic Reporting Flag.

When there are multiple requests, there is only one 'SNC C&S Acknowledgement' (421h) message.

3B.6.1 Request for Connectivity Data

In response to a request for connectivity information, the SNC sends a set of ‘Connectivity Information (LRQ)’ (602h) messages and also a set of ‘Connectivity Information (LCD)’ (607h) messages. The LRQ messages contain the connectivity up to two legs, while the LCD messages contain the connectivity for the third leg. The two messages are complimentary. Both messages are sent to the DLP for all defined networks, regardless of which networks the unit is a member of, as connectivity information can be received for networks the unit is not a member of, as detailed in Section 3C.8 Relay & Routing. This could result in a large amount of information that would then be split into a number of messages to reduce the size of each message. If the unit is not operational on any network, an ‘SNC Status’ (413h) message is sent with SNC Status field set to 4 (“SNC Warning”) and the text field set to “312h request for Connectivity Info, All networks are Inactive”. This message flow is shown in Figure 3B.6-1.

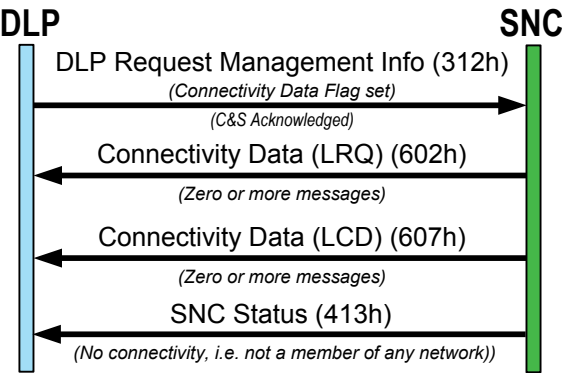


Figure 3B.6-1 DLP Request Management Info – Connectivity Data

3B.6.2 Request for Link Participants

In response to a request for Link Participants, the SNC sends a ‘Link Participants’ (407h) message listing the Super Network members, and if there are operational networks a second ‘Link Participants’ (407h) message listing the NILE Network members. This message flow is shown in [Figure 3B.6-2](#).

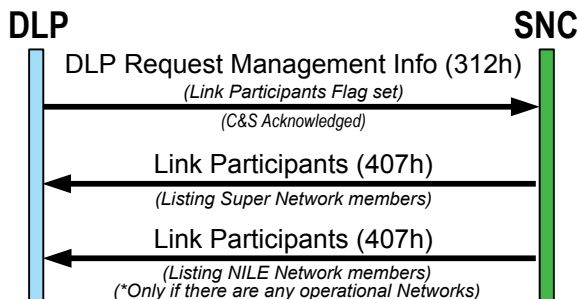


Figure 3B.6-2 DLP Request Management Info – Link Participants

3B.6.3 Request for Media Parameters

In response to a request for Media Parameters the SNC sends one ‘Media Parameters’ (405h) message for each operational network the unit is a member of. If the unit is not operational on any network an ‘SNC Status’ (413h) message is sent, with SNC Status field set to 4 (“SNC Warning”) and the text field set to “312h request for Media Parameters, All networks are Inactive”. This message flow is shown in [Figure 3B.6-3](#).

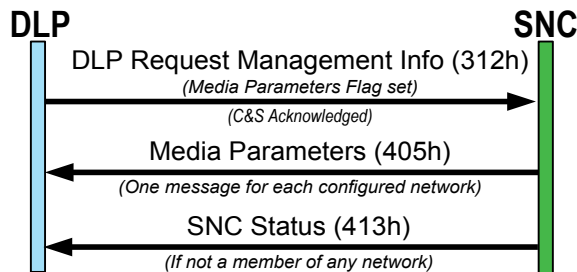


Figure 3B.6-3 DLP Request Management Info – Media Parameters

3B.6.4 Request for SN Directory Components

The DLP supplies whether it wants the OLM or the current SN Directory version when it requests the SN Directory Components. There is a flag to indicate whether each of the components is required to be sent. The SNC sends a set of messages that contain the required components for either the OLM or the current version of the SN Directory as shown in [Figure 3B.6-4](#).

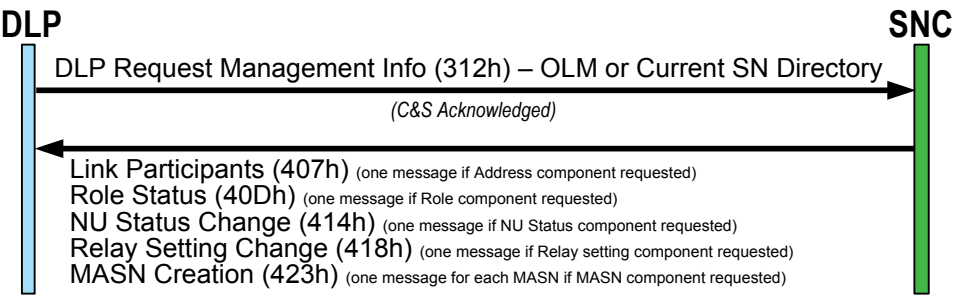


Figure 3B.6-4 DLP Request Management Info – SN Directory Components

There is a message for each component that is requested, except for the MASN component for which there is a message for each defined MASN, as detailed in [Section 3B.5 SN Directory Maintenance](#).

3B.6.5 Request for List of Queued Messages

As detailed in Section 3B.4 [Command Queuing](#), the SNC internally stores messages when the time of activation is more than 20 minutes in the future. The DLP can request this list at any time. In response to a management request for a list of the queued messages the SNC sends any (zero or more) messages that are waiting to be processed (those messages with a start time in the future and have not yet started to be processed) back to the DLP, setting the Message Variant field to the value 2. If there are no queued messages to be returned, an ‘SNC Status’ (413h) message is sent with SNC Status field set to 5 (“SNC Info”) and the text field set to “312h request, No Queued Messages”. This message flow is shown in [Figure 3B.6-5](#).

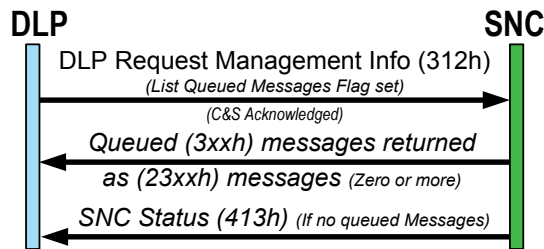


Figure 3B.6-5 DLP Request Management Info – List Queued Messages

3B.6.6 Request for Network Information

In response to a request for Network Information the SNC sends a ‘Network Information’ (42Dh) message, one for each network that the NU is operating on (status of Active, Receive-Only for Radio silent). If there are no operational networks, an ‘SNC Status’ (413h) message is sent with SNC Status field set to 4 (“SNC Warning”) and the text field set to “312h request for Network Information, All networks are Inactive”. This message flow is shown in [Figure 3B.6-6](#).

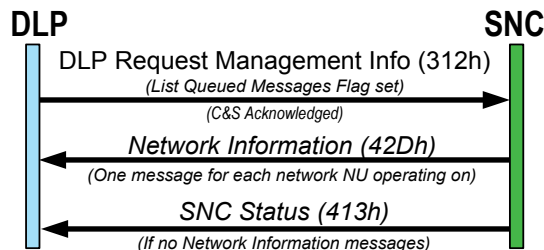


Figure 3B.6-6 DLP Request Management Info – Network Information

3B.6.7 Request for Congestion Indexes

In response to a request for congestion Indexes, the SNC sends a ‘Network Congestion Indexes’ (42Eh) message for each operational network. The message contains the congestion indexes for each network member. If there are no operational networks, an ‘SNC Status’ (413h) message is sent with SNC Status field set to 4 (“SNC Warning”) and the text field set to “312h request for Congestion Indexes, All networks are Inactive”. This message flow is shown in [Figure 3B.6-7](#).

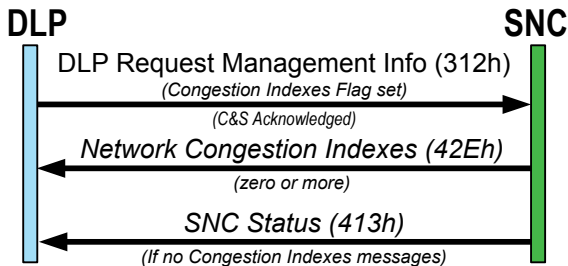


Figure 3B.6-7 DLP Request Management Info – Congestion Indexes

3B.6.8 Request for NU Capabilities

In response to a request for NU Capabilities, the SNC sends a ‘NU Capabilities’ (42Fh) message reporting SNC version and SNMU/NMU capabilities for own unit and for each unit from which the SNC CAPABILITIES technical message has been received. This message flow is show in [Figure 3B.6-8](#).

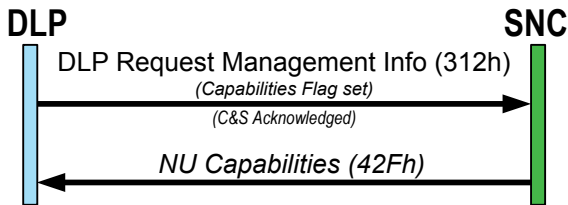


Figure 3B.6-8 DLP Request Management Info – Capabilities

3B.6.9 Request for C&S Messages

In response to a request for a Control & Status Message, the SNC sends one for the following response messages, depending on DLP selection, setting its Message Variant field to the value 4:

- an ‘MPT specification’ (301h) message, with the current Super Network Day Of Week and the currently used Smallest and Largest Message Preparation Time
- an ‘LLC LAN Configuration’ (302h) message describing the current configuration and reporting for each LLC the current LLC Internal Day Of Week
- a ‘Role Takeover Control’ (331h) message with the current takeover settings
- a set of ‘Link Quality Status’ (328h) messages reporting all connectivity overrides issued by the DLP; if the DLP has issued no overrides an ‘SNC Status’ (413h) message is sent with SNC Status field set to 5 (“SNC Info”) and the text field set to “312h request, No connectivity override info”
- a set of ‘Function Management Setup’ (335h) messages with the current settings

If the requested C&S message is not handled, an ‘SNC Status’ (413h) message is sent with SNC Status field set to 4 (“SNC Warning”) and the text field set to “312h request for C&S message not handled”. This message flow is show in [Figure 3B.6-9](#).

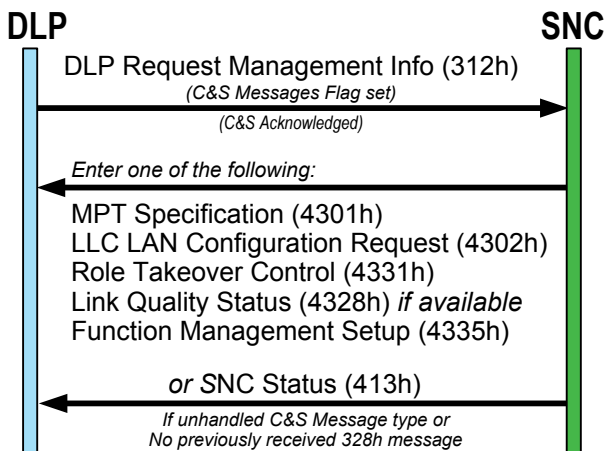


Figure 3B.6-9 DLP Request Management Info – C&S Messages

3B.7 Network Control

After a network has been initialized, the DLP of the NMU has the responsibility for control of that network. The NMU achieves this by managing a network's parameters. If the SNMU requires changes to the network (and it is not the NMU), it uses the Order protocol described in section [3B.3 Orders](#) to send an order to the NMU to change the network's parameters, and supplies the new parameters to the NMU.

The network control protocols include the following.

- [DTDMA Change](#)
- [Reconfiguration](#)
- [Re-Initialization](#)
- [New Network Initialization](#)
- [Power Management](#)

The network parameters consist of the following.

- DTDMA Flag
- Media Segment Parameters
 - Media Type
 - Frequency / Frequency Hopset
 - Media Setting Number (Waveform)
 - Fragmentation Rate
 - LLC Integrity Flag
 - SPC Radio Power
- Network Cycle Structure
 - Provided by the DLP
 - Calculated by the SNC

The DLP of the NMU must also provide which network it is controlling and when (start time) to perform the change.

[Figure 3B.7-1](#) summarizes the types of network changes that can be made, and the messages used to initiate the change at the NMU. The messages used to change the ONCS include the ability to change the DTDMA Flag at the same time, if desired.

Change	SNMU Order	NMU Message
DTDMA Flag	Reconfiguration (DTDMA ON) Reconfiguration (DTDMA OFF)	DLP DTDMA Change (311h)
ONCS	Reconfiguration (DLP NCS) Reconfiguration (SNC NCS)	Network Reconfiguration Request (DLP NCS) (310h) Network Reconfiguration Request (SNC NCS) (329h)
Media Parameters	Re-initialization (Media only)	Change Media Parameters (30Fh)
Media Parameters and ONCS	Re-initialization (DLP NCS) Re-initialization (SNC NCS) Re-initialization (Probing)	Network Parameters (DLP NCS) (30Eh) Network Parameters (SNC NCS) (306h) Network Parameters (Probing) (307h)
SPC Radio Power	SPC Radio Power Request (32Dh) (not an order)	SPC Radio Power Request (32Dh)

Figure 3B.7-1 DLP Network Control Changes

3B.7.1 DTDMA Change

Figure 3B.7-2 shows the protocol used to change just the DTDMA Flag in a network. The change is shown coming from the DLP, but could also have been initiated by an order from the SNMU. The time the change is to occur is supplied to the NMU SNC, but the message sent by the NMU SNC to the other NUs in the network does not have a time in it. Therefore, the NMU SNC will transmit the change at the time specified.

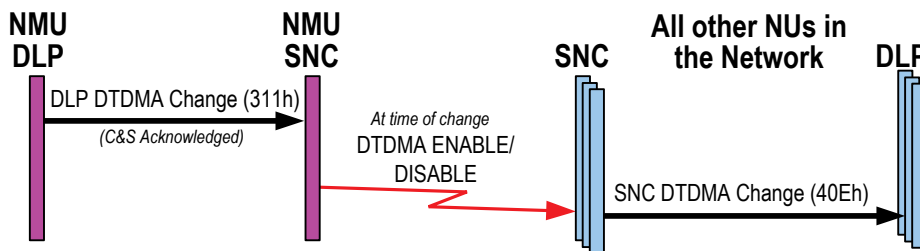


Figure 3B.7-2 DTDMA Change

3B.7.2 Reconfiguration

The purpose of the Network Reconfiguration is to restructure the ONCS to optimize the performance of a Network. This can be the case when units join or leave the network, when connectivity changes affect relay flow, and also when traffic profiles change among the different units. DTDMA can be enabled or disabled at the same time. These changes do not require a reconfiguration of the LLC and/or the SPC, so the changes occur seamlessly. As during initialization, the DLP can provide the NCS, or request that the SNC calculate the NCS from parameters supplied by the DLP.

When the DLP provides the NCS, the following data is provided to the NMU SNC.

- Network ID
- Network Start Time
- DTDMA setting
- For each defined timeslot in the ONCS
 - Timeslot Size (in minislots)
 - Timeslot Owner (Link 22 Address, or 0 for a Priority Injection slot)

The beginning of the reconfiguration protocol for the DLP provided NCS is shown in [Figure 3B.7-3](#).

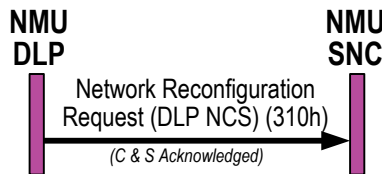


Figure 3B.7-3 Start of Reconfiguration with DLP ONCS

When the SNC is to calculate the NCS, the DLP supplies the following network parameters to the NMU SNC.

- Network ID
- Network Start Time
- DTDMA setting
- Access Delay Tolerance
- Efficiency
- For each NU that needs to transmit in the network
 - Channel Capacity Need
 - Channel Access Delay

The SNC uses the supplied parameters to calculate an NCS. The SNC sends the NCS to the DLP for approval. The DLP can perform one of the following actions.

- Accept the NCS
- Supply different parameters for the SNC to calculate another NCS (For the same inputs, the SNC always produces the same results)

The beginning of the reconfiguration protocol for the SNC-calculated NCS is shown in [Figure 3B.7-4](#), with the DLP accepting the NCS computed by the SNC. If the protocol started with an order from the SNMU that was automatically performed by the NMU SNC, no NCS Acknowledgement from the DLP is expected.

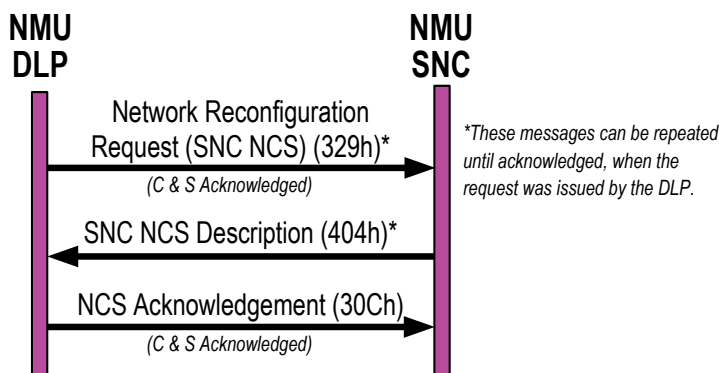


Figure 3B.7-4 Start of Reconfiguration with SNC Calculated ONCS

After the NCS calculation is accepted the NMU SNC distributes the information to the other NUs in the network. The receiving NUs send an acknowledgement back to the NMU SNC, and inform their DLP of the reconfiguration. All NUs in the network start using the new NCS at the specified Network Start Time, or immediately if received late, and the NCS becomes the new ONCS. This protocol is shown in [Figure 3B.7-5](#).

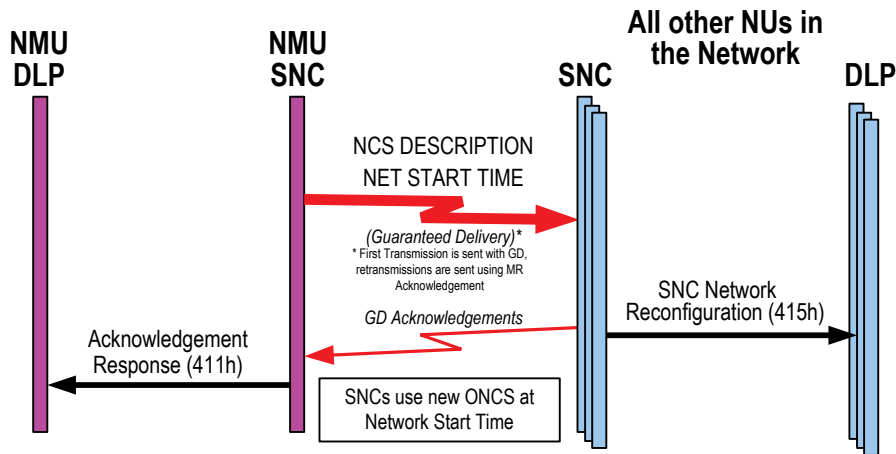


Figure 3B.7-5 Distribution of Reconfiguration parameters

The NMU SNC also sends a NCT INFO technical message, which contains the network cycle time (NCT) information, to all NUs in the Super Network so that all other NUs not in the network will know the NCT for the network. This is used to compute routing selection as detailed in [section 3C.8 Relay & Routing](#) and it is not shown in the figure.

3B.7.3 Re-Initialization

The purpose of the Network Re-Initialization is to optimize the performance of a network by modifying the network's media parameters, and optionally, by also modifying the ONCS at the same time. This can be used when changes in environmental conditions may require different settings and/or a different frequency. These changes require a reconfiguration of the LLC and/or the SPC, so transmissions and receptions are suspended for approximately 5-10 seconds.

There are three types of re-initialization available.

- [Media Parameter Change](#)
- [Short Re-Initialization](#)
- [Re-initialization with Probing](#)

Note that some SPCs can automatically change media type, while others cannot. Issues regarding changes to media type are covered in [Appendix B](#).

□ **Media Parameter Change**

Media parameters (does not affect the ONCS) can be changed, using a ‘Media Parameter Change’ (30Fh) message. The second column in [Figure 3B.7-6](#) indicates which media parameters can be changed for each media type using this protocol. All other parameters that have more than one value, including media type, must be changed by performing one of the other re-initialization protocols that include an NCS change. Note that media type change is not a requirement of the SPC and may not be supported automatically by some manufacturers.

Media Type	Parameters not affecting ONCS. Media Parameter Change can only modify these parameters	Parameters affecting ONCS	Parameters with only one value
HF FF	MSN Frequency LLC Integrity SPC Radio Power	Fragmentation Rate	
UHF FF	Frequency LLC Integrity SPC Radio Power	Fragmentation Rate	MSN
HF EPM	MSN Frequency Hopset LLC Integrity SPC Radio Power		Fragmentation Rate
UHF EPM	Frequency Hopset LLC Integrity SPC Radio Power	MSN (Repetition Rate)	Fragmentation Rate

Figure 3B.7-6 Media Parameter Change Parameters

All of the media parameters are included in the message. Those that are not being changed are set to their current values, except SPC Radio Power, which is set to zero if it is not being changed because each NU may be using a different radio power. The NMU DLP can specify the time of the change, or allow the NMU SNC to calculate

the earliest time the change can be applied, taking into consideration the delay for SNC message distribution in the Network and the reconfiguration time of the LLC/SPC. The SNC sets the time of activation to 15 times the NCT, if the time is not specified by the DLP. The NMU SNC distributes the changes to all NUs in the network. The receiving NUs send an acknowledgement back to the NMU SNC, and inform their DLP of the change. If SPC Radio Power is being changed, each NU follows the protocol in section [3B.7.5 Power Management](#). All NUs in the network stop transmissions and receptions 10 seconds before the Network Start Time to reconfigure the LLC/SPC. This protocol is shown in [Figure 3B.7-7](#), excluding the protocol used to change the SPC Radio Power.

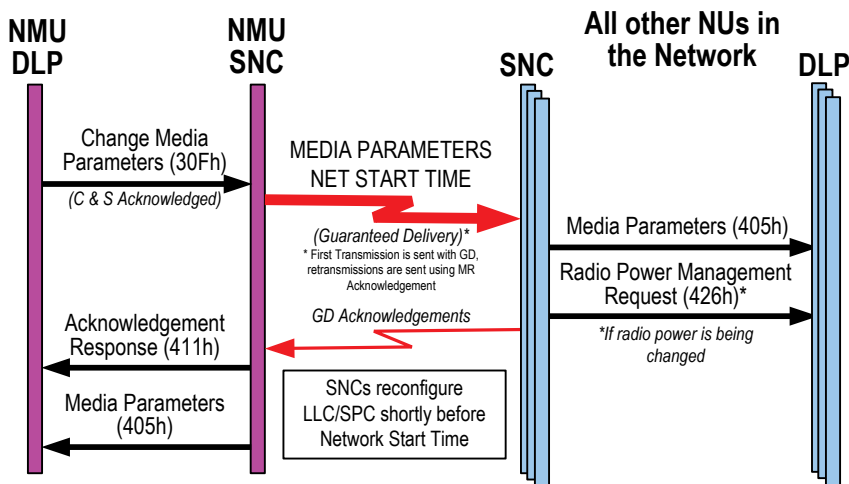


Figure 3B.7-7 Media Parameter Change

□ **Short Re-Initialization**

If both the media parameters and the ONCS need to be changed, and probing is not required, a short re-initialization can be performed. The short re-initialization protocol allows the ONCS and media parameters to be changed at the same time. This requires a reconfiguration of the LLC and/or SPC. As for reconfiguration, either the DLP can supply the new NCS, or the DLP can request that the SNC calculate the NCS. The following parameters are included in both cases.

- Network ID
- Start Time
- Media Type
- Frequency/Hopset
- MSN
- Fragmentation rate
- DTDMA
- LLC Integrity
- SPC Radio Power

When the DLP provides the NCS, the following NCS data is provided to the NMU SNC for each defined timeslot in the NCS.

- Timeslot Size (in minislots)
- Timeslot Owner (Link 22 Address, or 0 for a Priority Injection slot)

The beginning of the short re-initialization protocol using the DLP provided NCS is shown in [Figure 3B.7-8](#).

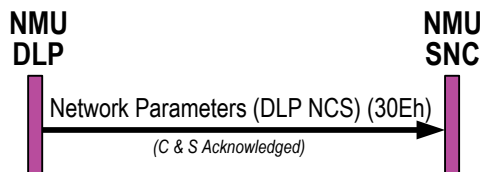


Figure 3B.7-8 Start of Short Re-initialization with DLP NCS

When the SNC is to calculate the NCS, the DLP supplies the following NCS parameters to the NMU SNC.

- Access Delay Tolerance
- Efficiency
- For each NU that needs to transmit in the network
 - Channel Capacity Need
 - Channel Access Delay

The SNC uses the supplied parameters to calculate an NCS. The SNC sends the NCS to the DLP for approval. The DLP can perform one of the following actions.

- Accept the NCS
- Supply different parameters for the SNC to calculate another NCS (For the same inputs, the SNC always produces the same results)

The beginning of the short re-initialization protocol for the SNC calculated NCS is shown in [Figure 3B.7-9](#), with the DLP accepting the NCS returned by the SNC. When the protocol starts with an order from the SNMU, the SNMU includes the NCS NEEDS technical message in the messages it sends to the NMU, and then the NMU calculates the NCS. If the order is automatically performed by the NMU SNC, no NCS Acknowledgement from the DLP is expected.

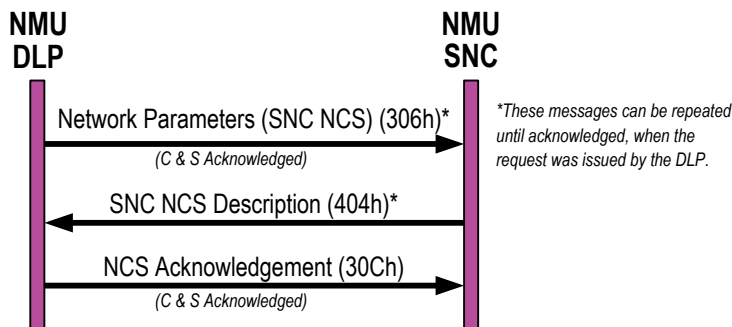


Figure 3B.7-9 Start of Short Re-initialization with SNC Calculated ONCS

After the NCS calculation is accepted the NMU SNC distributes the information to the other NUs in the network. The receiving NUs send an acknowledgement back to the NMU SNC, and inform their DLP of the short re-initialization. If SPC Radio Power is being changed, each NU follows the protocol discussed in [section 3B.7.5 Power Management](#). All NUs in the network reconfigure the LLC/SPC shortly before the Network Start Time, and initializes the network. If a new NCS was supplied this becomes the new ONCS. This protocol is shown in [Figure 3B.7-10](#), excluding the protocol used to change the SPC Radio Power.

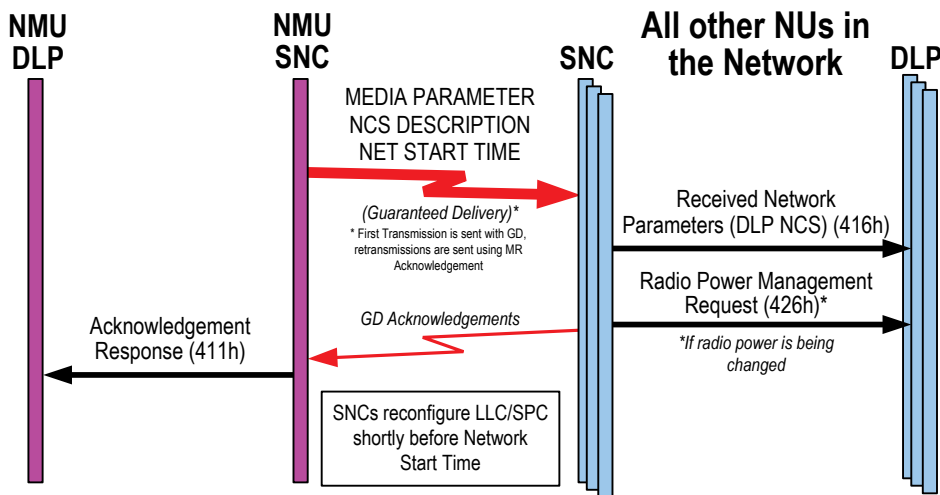


Figure 3B.7-10 Distribution of Short Re-initialization parameters

The NMU SNC also sends a NCT INFO technical message to all NUs in the Super Network, which contains the network cycle time (NCT) information, so that all other NUs not in the network will know the NCT for the network. This is used to compute routing selection as detailed in Section 3C.8 [Relay & Routing](#) and it is not shown in the figure.

□ **Re-initialization with Probing**

If propagation conditions are not known, a re-initialization with probing can be performed. This allows both the media parameters and the ONCS to be changed. The following parameters are specified.

- Network ID
- Probing Start Time
- Media Type
- Frequency/Hopset
- MSN
- SPC Radio Power
- Each Network NU's Link 22 Address

The NMU SNC distributes the information to the other NUs in the network. The receiving NUs send an acknowledgement back to the NMU SNC, and inform their DLP of the probing re-initialization. If SPC Radio Power is being changed, each NU

follows the protocol described in section 3B.7.5 [Power Management](#). All NUs in the network stop transmissions and receptions 10 seconds before the Network Start Time to reconfigure the LLC/SPC, and then perform the probing as described in Section 3B.2.2 [Network Initialization with Channel Probing](#). This protocol is shown in Figure 3B.7-11, excluding the probing protocol and the protocol used to change the SPC Radio Power.

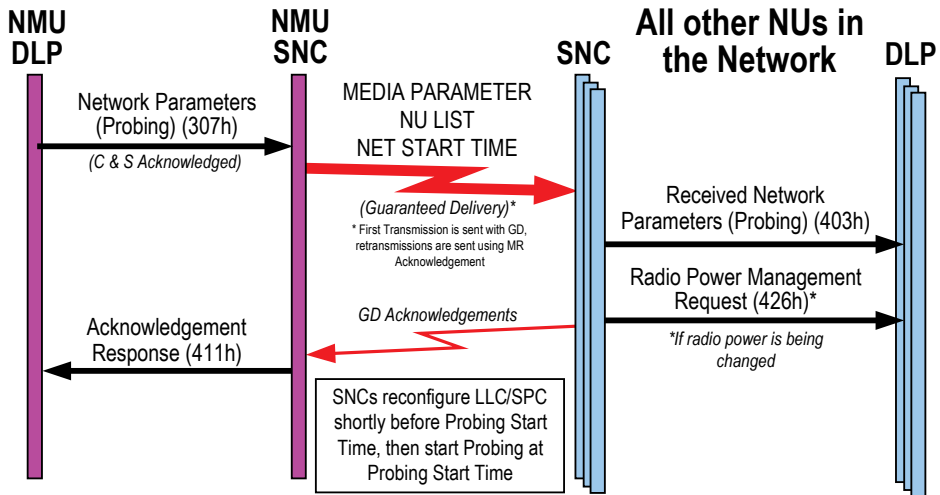


Figure 3B.7-11 Re-initialization with Probing

3B.7.4 New Network Initialization

The creation of a new network (not specified in the OPTASK Link Message), is managed exclusively by the SNMU and involves the following steps.

- Creation of the New Network Membership MASN
- Distribution of the New Network Order
- Assignment of NMU and Standby NMU roles
- Initialization of the New Network

The DLP of the SNMU should not assign the NMU or Standby NMU until it knows which NUs comply with the new network order, as some of the units may not have the required hardware (LLC/SPC/Radio) to activate the new network. The order to initialize a new network requires a response from the DLP operators of the involved

NUs, because the unit may have to leave another active network to be able provide the hardware necessary to join the new network.

A new network may be created by splitting one or more active networks.

□ **Creation of the New Network Membership MASN**

The DLP of the SNMU must first indicate which NUs are going to be in the new network by creating the MASN (if not yet created) for the new network, as described in Section 3B.5 SN Directory Maintenance. The MASN needs to be created and be operational before the new network order is distributed because the SNMU addresses the message to the MASN so that all members of the new network can receive the message.

□ **Distribution of the New Network Order**

The DLP of the SNMU sends one of the three Initialize New Network orders and the associated network parameters message to its SNC. The choices are the same as for initializing a network during SNC Initialization.

- Initialize New Network (DLP NCS): SNMU DLP supplies the NCS
- Initialize New Network (SNC NCS): SNMU DLP supplies the needs of the NUs, and the NMU SNC calculate the NCS
- Initialize New Network (Probing): NMU DLP decides how to supply the NCS

The SNMU SNC then sends the corresponding messages to the NUs defined by the network membership MASN. The receiving NUs send the information to their DLPs. Figure 3B.7-12 summarizes the messages involved.

Order	DLP->SNC message sent with Order	Technical messages sent with ORDER	SNC->DLP message sent with received Order
Initialize New Network (DLP NCS)	Network Parameters (DLP NCS) (30Eh)	MEDIA PARAMETERS NCS DESCRIPTION	Received Network Parameters (DLP NCS) (416h)
Initialize New Network (SNC NCS)	Network Parameters (SNC NCS) (306h)	MEDIA PARAMETERS NCS NEEDS	Received Network Parameters (SNC NCS) (42Ah)
Initialize New Network (Probing)	Network Parameters (Probing) (307h)	MEDIA PARAMETERS NU LIST	Received Network Parameters (Probing) (403h)

Figure 3B.7-12 Messages Involved in Initializing a New Network

❑ **Assignment of NMU and Standby NMU roles**

After the DLP of the SNMU knows which NUs have responded with a WILCO to the order, the DLP assigns a NMU and Standby NMU for the new network members, as described in section [3B.5 SN Directory Maintenance](#). The new NMU and Standby NMU notify all other NUs of their role.

If probing initialization is to be used for the new network, the SNMU must assign the NMU before probing starts, because the probing protocol needs an NMU. When probing is not used, and the start time of the new network is close, the SNMU is likely to wait to assign the NMU and Standby NMU until after the new network is initialized, because the units the SNMU is trying to send the order to may already have shut down on their only network to prepare to initialize the new network.

If after 15 minutes of assigning the NMU no Standby NMU is assigned by the SNMU, the DLP of the NMU is responsible for assigning a Standby NMU.

❑ **Initialization of the New Network**

Each DLP initializes the new network by performing the steps listed in [Figure 3B.7-13](#).

Step	Message
Shutdown existing network, if necessary	NU Leave (31Ah)
Configure new LLC, if needed	LLC LAN Configuration Request (302h)
Assign SPC for the new network	LLC Port Configuration Request (303h)
Initialize the network	<i>One of the following corresponding to the order</i> Network Parameters (DLP NCS) (30Eh) Network Parameters (SNC NCS) (306h) Network Parameters (Probing) (307h)

Figure 3B.7-13 New Network Initialization Steps

A DLP may need to use equipment for the new network that is being used by one of its current networks. If this is the case, the DLP must first shut down on the existing network prior to the new network start time allowing enough time for any operator interaction (such as manual retuning of the radio to the new frequency). The new network must be mapped to a LLC port even if the DLP is re-using a port, because the network number is different.

At the specified time, all the new network members that replied with a WILCO initialize the new network. The sequence is exactly the same as if it was initializing the network from the information in the OLM, as described in section [3B.2 Network Initialization](#).

3B.7.5 Power Management

A NU can adjust its own Radio Power, or the SNMU and NMU can order a NU or all NUs in a network to adjust their Radio Power. Radio Power can also be changed for all NUs in a network during a re-initialization. Some Radios or national procedures may not allow for automatic change.

The radio transmission power used by a NU on a network is adjusted by the NU's DLP sending the SNC a 'SPC Radio Power Request' (32Dh) message with the required power level and optionally a start time. This may be performed when determined by the DLP, by the DLP in response to an order from the SNMU or NMU of the network, or as requested by network re-initialization. If a network re-initialization is about to start and there is not enough time to complete the power change before the re-initialization must start, then the Radio Power change will not be performed until the re-initialization is completed. The SNC requests the SPC to change its radio power, and then informs the DLP whether or not the operation was successful, and what the radio power is set to. This protocol is shown in Figure 3B.7-14.

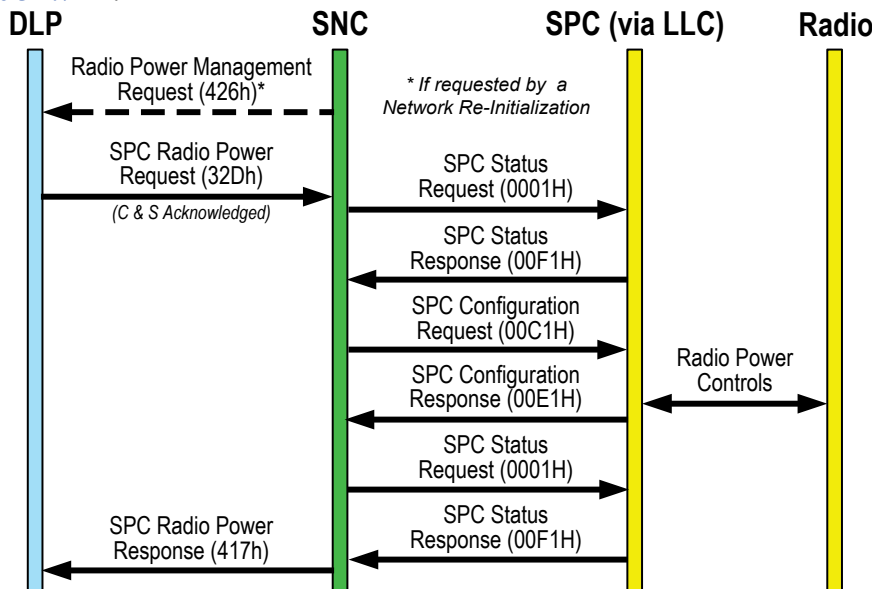


Figure 3B.7-14 Adjustment of Own SPC Radio Power

□ **SNMU/NMU Radio Power Management Order**

When the DLP of the SNMU or the NMU of a network needs to change the radio power level of a single NU or all NUs in a network it sends a Radio Power Management Order to the NU or to all the NUs in the network membership MASN. The DLP sends to its SNC an 'Order' (333h) message containing the required radio power level. The SNMU or NMU SNC sends the order technical message to the NU or all network members. The receiving NU sends an order compliance back to the SNMU or NMU SNC, which informs its DLP by sending a 'Received Order Compliance' (429h) message. The SNC of the addressed NU sends a 'Received Order' (428h) message to its DLP, which uses the protocol shown in [Figure 3B.7-14](#) to adjust its radio power, if it complies.

An example of the Radio Power Management Order protocol from the SNMU to all network members, with automatic order processing turned off, is shown in [Figure 3B.7-15](#).

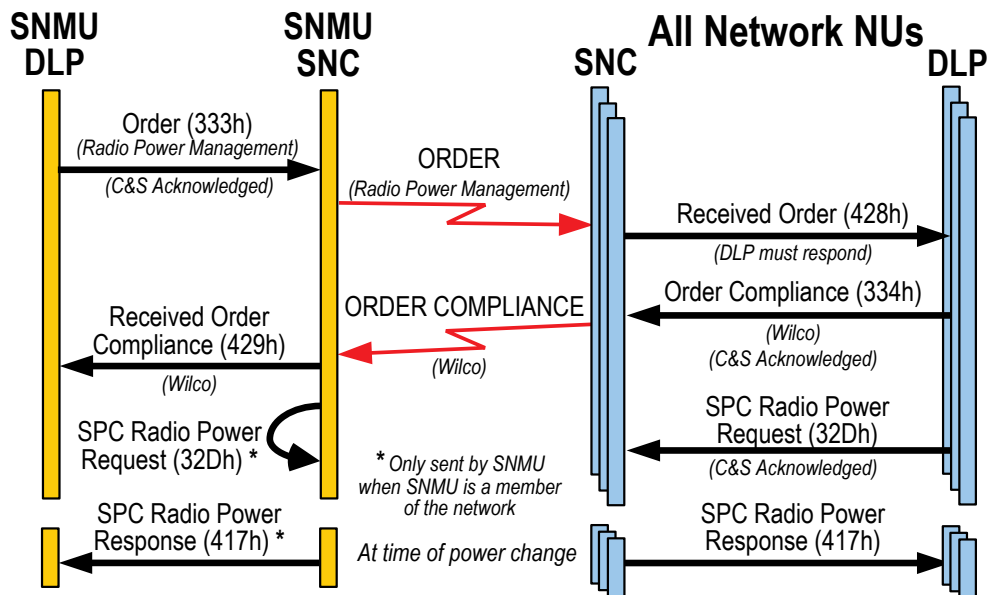


Figure 3B.7-15 SNMU Orders all Network Members to Change Radio Power

□ ***SPCs that Cannot Control Radio Power***

If the SPC or Radio does not implement radio power control, the SPC sets the SPC Radio Power field to zero whenever it sends the SPC→SNC ‘SPC Status Response’ (00F1H) message. The SNC will then set the SPC Radio Power field to zero in all SNC→SPC ‘SPC Configuration Request’ (00C1H) messages, which tells the SPC to not attempt to change the radio power. In the case of a radio power change, the SNC will not send anything to the SPC. The SNC will report back to the DLP that the radio power was successfully changed to the requested value, since the SNC stores the received value. The power will then need to be manually changed.

3B.8 Late Network Entry (LNE)

After a network has been started, units that have not yet initialized on that network can join the network by initiating a protocol called Late Network Entry (LNE). LNE supports the following.

- Units not yet initialized on any network
- Units already initialized on another network
- Units joining only to listen – no transmission capacity requested during LNE, receive-only after LNE is complete
- Units silently joining, without making any transmissions
- Receive-only units already in a network, requesting transmission capacity

From the point of view of the DLP Operator, only two selections are available using the ‘Network Late Initialization Request’ (327h) message. In the first case, the SNC determines which specific protocol to follow. In the second case, Silent Join is mandated.

- SNC to determine whether Inactive or Active join be performed
- DLP specifies that Silent Join LNE be performed

The sequence depends on the current status of the unit and the status it wants to achieve within the network. The different types of LNE are listed in [Figure 3B.8-1](#).

LNE Type	Usage
Inactive Join (IJ)	Unit does not have a NILE Address, or NU has a NILE Address but is inactive in the Super Network, or NU is a Receive Only unit in the network (it wants Transmission Capacity)
Active Join (AJ)	NU has a NILE Address, and NU is Active (Tx & Rx) in at least one existing network
Silent Join (SJ)	Unit may or may not have a NILE Address, and the unit wants to Receive from the network, unknown to the rest of the SN

Figure 3B.8-1 LNE Types

Note that a unit can only perform one IJ LNE at a time. After successfully joining the first network, it performs AJ LNE if it wants to join another network. [Figure 3B.8-2](#) shows the high level phases that each form of LNE completes for a successful join and indicates the similar phases across the different forms of LNE. The shaded box indicates that those operations are performed by the Supporting Unit (SU) and not by the LNE unit itself.

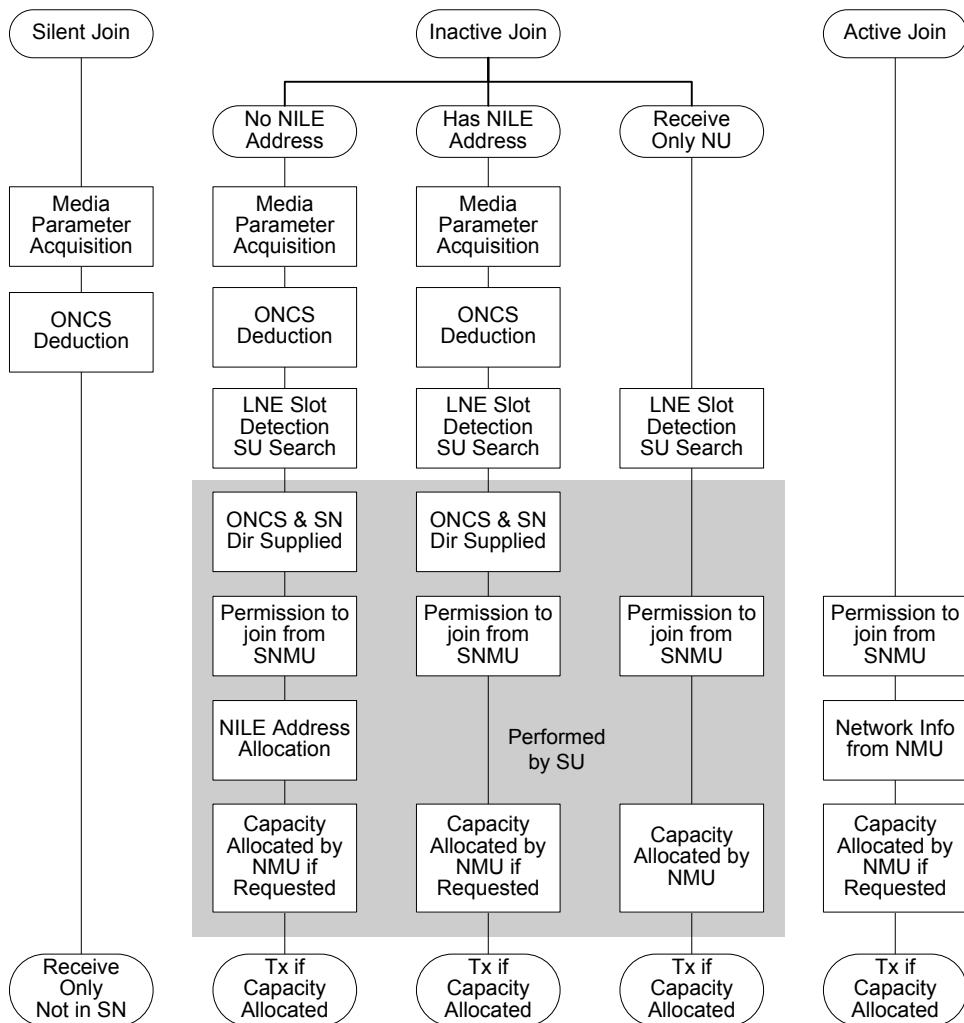


Figure 3B.8-2 The Different Forms of LNE and their Common Phases

Note a unit being “Receive Only Not in the SN” at the end of Silent Join is not the same as being a “Receive Only NU”. Both Inactive Join and Active Join require SNMU permission to join the network. If the NU is already in the network membership MASN, permission has already been granted. If capacity is requested, the NMU is asked for transmission capacity if the NU is not already in the ONCS. The

Silent Join requires no transmissions. The LNE transmissions are summarized in [Figure 3B.8-3](#).

LNE Type	LNE Transmissions
Inactive Join (IJ)	LNE Slot is inserted into the ONCS. LNE unit transmits only in the LNE Slot during the LNE process. IJ unit communicates with a Supporting Unit (SU). SU transmits requests to SNMU and NMU, and reports results back to the IJ unit, unless the unit is already defined in both the MASN and the ONCS
Active Join (AJ)	AJ unit transmits requests to SNMU and NMU itself
Silent Join (SJ)	No transmissions are made

Figure 3B.8-3 LNE Transmissions

The DLP of any LNE unit wanting to join must know some of the network parameters, such as the network number and crypto parameters, all of which are contained in the OPTASK Link message. Media Parameter Acquisition (MPA) is the first phase of the IJ and SJ process and also requires media type and frequency. Knowledge of other network parameters such as Media Setting Number, LLC Integrity, and Fragmentation Rate, although not mandatory, could allow the MPA protocol to complete more quickly, instead of making the unit cycle through all possible combinations.

The LNE unit will need to assign a LLC and SPC for the network to be joined, if they were not previously assigned. The LLC is included in the 'LLC LAN Configuration Request' (302h) message, and the SPC is assigned to the network in the 'LLC Port Configuration Request' (303h) message. These messages are normally sent during SNC Initialization (see section [3B.1 SNC Initialization & Set-Up](#)), but can be sent at any time to include a new LLC or SPC, as summarized in [Figure 3B.8-4](#).

Current State	LLC/SPC Initialization Required
Not yet initialized	Perform SNC Initialization & Set-Up, and include the LLC and SPC to be used for the network being joined, in the 'LLC LAN Configuration Request' (302h) and 'LLC Port Configuration Request' (303h) messages
LLC not initialized	'LLC LAN Configuration Request' (302h) – include only the new LLC 'LLC Port Configuration Request' (303h) – include all SPCs
SPC not initialized	'LLC Port Configuration Request' (303h) – include all SPCs
LLC and SPC already initialized	No additional LLC/SPC configurations are required

Figure 3B.8-4 LNE LLC/SPC Initialization

The current LLC DOW must be supplied in the ‘LLC LAN Configuration Request’ (302h) message, and the crypto keys must be loaded into the LLC in the location supplied in the ‘LLC Port Configuration Request’ (303h) message. Refer to section [3B.1.2 LLC Configuration](#), for special considerations when the LLC DOW is unknown.

All SPCs connected to the LLC must be included in the ‘LLC Port Configuration Request’ (303h) message, including those already in use and the new SPC to be used for the LNE network.

If the DLP does not specify Silent Join, the SNC determines whether it needs to use Inactive Join or Active Join. If the SNC can use Active Join, the SNC does not perform the Media Parameter Acquisition steps, and instead just informs the DLP in the ‘LNE Status’ (409h) message that Active Join is being used. The DLP would then instruct the SNC to continue with the LNE protocol by sending a ‘DLP LNE Request’ (316h) message. The request indicates the unit’s capacity requirements, if any. This protocol is shown in [Figure 3B.8-5](#).

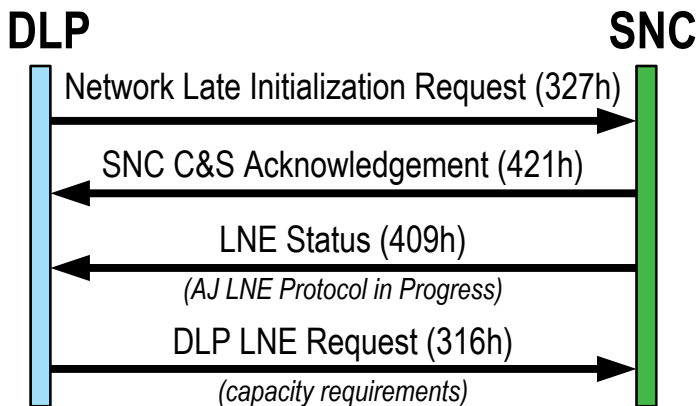


Figure 3B.8-5 DLP-SNC Beginning of AJ LNE Protocol

3B.8.1 Media Parameter Acquisition

The first phase of IJ and SJ LNE is for the LNE unit to determine the media parameters of the network by sequencing through the possible variations based on the DLP supplied parameters until successful, as detailed in [Figure 3B.8-6](#). Receive-only IJ NUs do not perform this phase, as they are already listening on the network.

Parameter	Source of Parameter
Network ID	Must be supplied by the LNE operator
Day of Week	LLC must already be set to the correct DOW
Crypto Key	LLC must already be loaded with the correct crypto key
Media Type	Must be supplied by the LNE operator
Frequency	Must be supplied by the LNE operator
Media Setting Number (MSN)	LNE operator must list between one and six MSNs to try The SNC will try each MSN
Fragmentation Rate	Optionally supplied by the LNE operator If not supplied, the SNC will try all valid Fragmentation Rates
LLC Integrity	Optionally supplied by the LNE operator If not supplied, the SNC will try both LLC Integrity Enabled and LLC Integrity Disabled

Figure 3B.8-6 LNE Media Parameters

The SNC attempts different valid combinations of MSN, Fragmentation Rate, and LLC Integrity based on what the DLP supplies, until it either finds the correct values, or fails. In the case of HF FF, the SNC sorts certain MSNs (1 before 2, 3 before 4, and 5 before 6) to ensure the strongest waveform is checked first. The SNC listens using a random number of minislots close to maximum size timeslots so that it is more likely to receive a network packet. The SNC will continue to listen for up to two maximum length NCTs, or until it receives enough good or bad network packets to determine the results. The SNC reports the results of listening to each MSN, and then reports the success or failure to the DLP, including the media parameters if successful.

□ HF FF, UHF FF, HF EPM Media Parameter Acquisition

Figure 3B.8-7 shows the logic the SNC uses during the Media Parameter Acquisition Phase for all media types (except UHF EPM), assuming that the Fragmentation Rate and LLC Integrity are unknown, in which case the SNC starts with LLC Integrity enabled and Fragmentation Rate of 1. The green box indicates the successful completion of this phase, while the light red boxes represent areas where failure can occur.

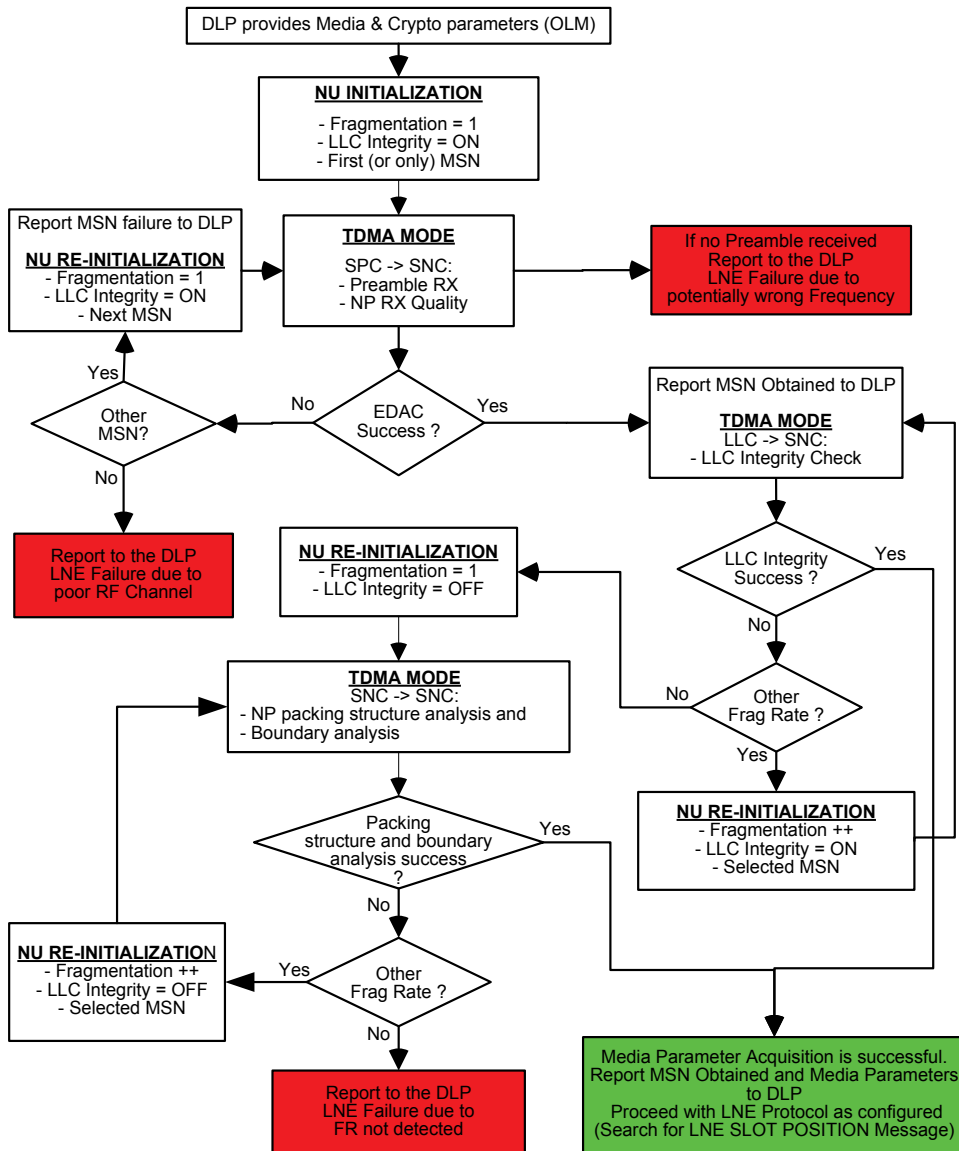


Figure 3B.8-7 Media Parameter Acquisition

Figure 3B.8-8 summarizes the contents of the flow diagram. The parameters are listed in the order they are determined, and a description of the analysis the SNC performs for each parameter is included. Thresholds used to declare a parameter detected or to decide to try the next possible value are also reported.

Parameter	Condition for Detection	Action upon failure
Frequency	At least <u>one</u> preamble (Initial Training sequences for HF EPM) is found	LNE Failure reported to DLP – wrong frequency. DLP can restart LNE with a different frequency
MSN	Network Packets containing at least <u>5</u> Media Coding Frames are received with EDAC success	If at least <u>20</u> Media Coding Frames were received, give up and try next MSN. If no more MSNs, LNE Failure reported to DLP – Wrong MSN or bad RF conditions. DLP can restart LNE, possibly with different MSNs
Fragmentation Rate, with LLC Integrity Enabled	At least <u>94%</u> of Network Packets pass decryption	If at least <u>50</u> Media Coding Frames were received, give up and try next Frag Rate. If no more Frag Rates, try LLC Integrity Disabled
Fragmentation Rate, with LLC Integrity Disabled	At least <u>94%</u> of decrypted Network Packets pass SNC analysis of correct NP packing structure and timeslot boundaries	If at least <u>100</u> Media Coding Frames were received, give up and try next Frag Rate. If no more Frag Rates, LNE Failure is reported to the DLP – Unable to Detect Fragmentation Rate
LLC Integrity	Set while determining Fragmentation Rate	

Figure 3B.8-8 Media Parameter Acquisition Description

A LNE Failure could also be caused by an incorrect Crypto Key or Day of Week in the LLC.

□ UHF EPM Media Parameter Acquisition

UHF EPM has one defined waveform, and four different repetition rates. The Media Setting Number is converted to the repetition rate for UHF EPM using Figure 3B.8-9. A repetition rate of zero indicates that a transmitted Network Packet is not repeated. The DLP can supply the known repetition rate, or a list of repetition rates to try.

Media Setting Number	Repetition Rate
1	0
2	1
3	2
4	3

Figure 3B.8-9 MSN to Repetition Rate Conversion

Figure 3B.8-10 shows the logic the SNC uses during the Media Parameter Acquisition Phase for UHF EPM, again assuming that the Fragmentation Rate and LLC Integrity are unknown. The green box indicates the successful completion of this phase, while the light red box represents where a failure can occur.

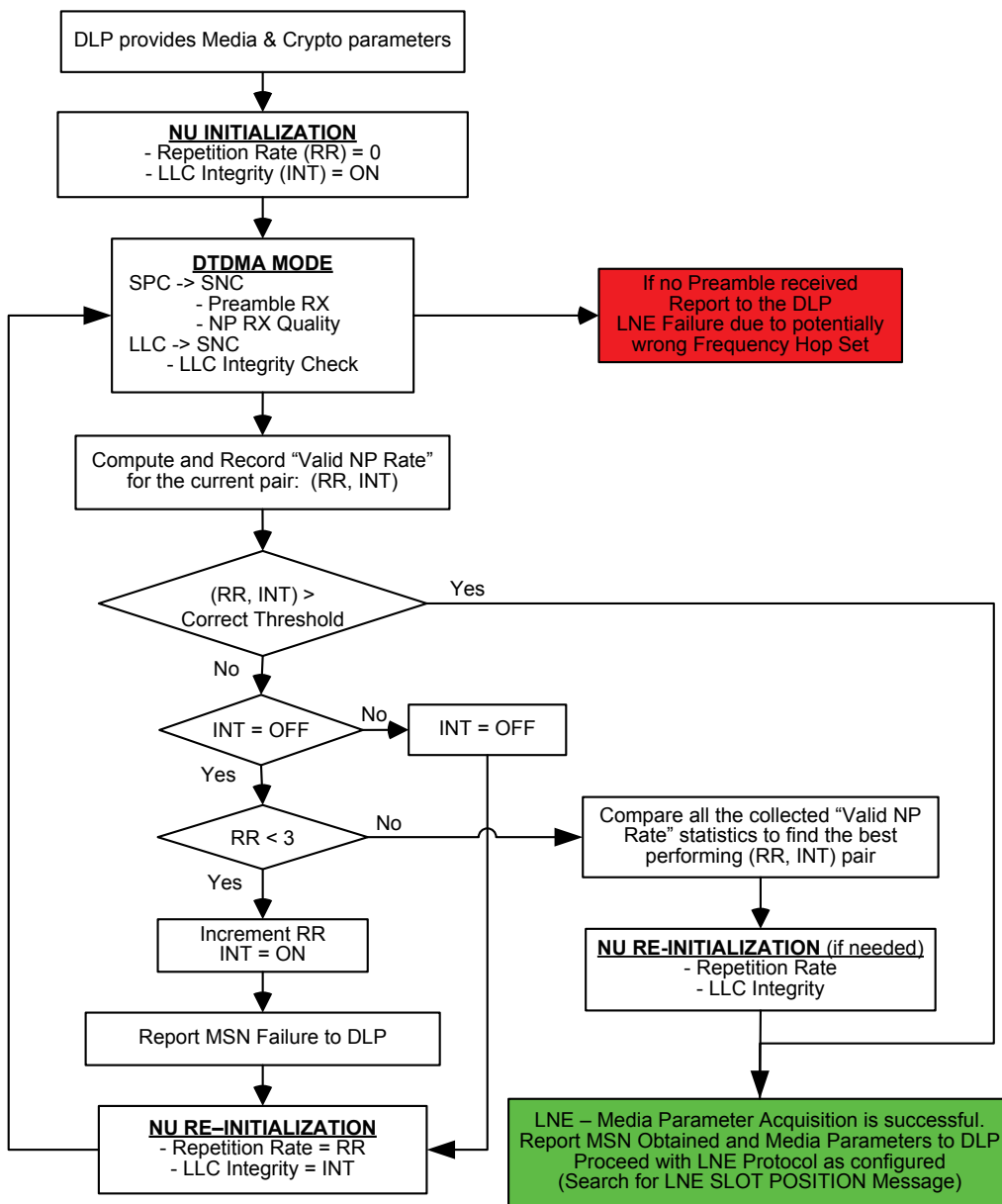


Figure 3B.8-10 UHF EPM Media Parameter Acquisition

Two different Valid NP Rate thresholds checks are made, one to determine the correct repetition rate, and the other to determine the correct LLC Integrity value. Repetition rates 0-3 are tried in order, swapping LLC Integrity for each rate, until the LLC Integrity Threshold is met, at which point the LLC Integrity setting is known, and is not changed anymore.

Figure 3B.8-11 summarizes the contents of the UHF EPM flow diagram, including the reporting thresholds used to determine repetition rate and LLC Integrity.

Parameter	Condition for Detection	Action upon failure
Frequency	At least <u>one</u> preamble is found	LNE Failure reported to DLP – wrong frequency. DLP can restart LNE with a different frequency
Repetition Rate	Network Packets containing at least <u>40</u> Media Coding Frames are received with EDAC success.	Try LLC Integrity Disabled, if Enabled was tried, otherwise try next RR.
LLC Integrity	At least <u>98%</u> of Network Packets pass decryption	If no more RRs, the best performing parameters pair is chosen

Figure 3B.8-11 UHF EPM Media Parameter Acquisition Description

□ **Beginning of the DLP-SNC LNE Protocol - Summary**

The flow of messages between the DLP and the SNC during the initial portion of the LNE protocol is shown in Figure 3B.8-12, for IJ or SJ LNE trying two MSNs. The SNC keeps the DLP informed of the ongoing status of LNE by sending ‘LNE Status’ (409h) messages to the DLP. The DLP knows the SNC completed the Media Parameter Acquisition phase when it receives either a ‘LNE Status’ (409h) message indicating Parameters Obtained, or a ‘LNE Failure’ (40Ah) message (not shown).

After the SNC informs the DLP of the acquired media parameters, the IJ DLP instructs the SNC to continue with the LNE protocol by sending a ‘DLP LNE Request’ (316h) message. The request indicates the unit’s capacity requirements, if any. This is not sent by a Silent Join unit.

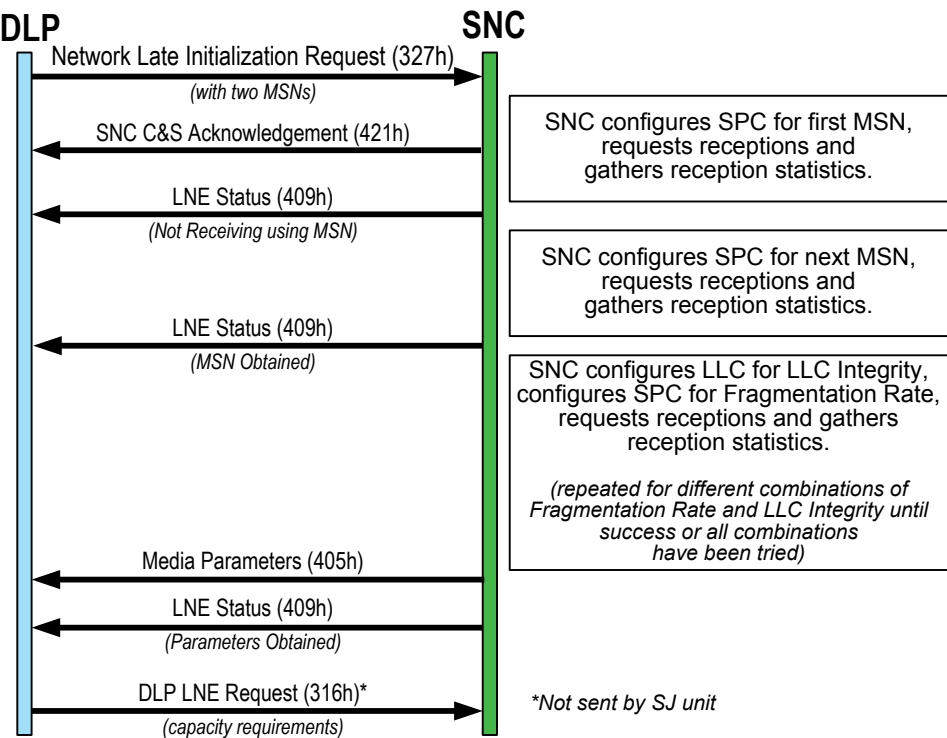


Figure 3B.8-12 DLP-SNC Media Parameter Acquisition Protocol

3B.8.2 ONCS Deduction

Throughout the execution of the LNE protocol, the IJ or SJ LNE unit collects information about the ONCS.

- The SPC reports Preambles or Short NPs, which help to identify timeslot boundaries
- The LLC can identify the NU using the slot when Explicit Source Identification is used in the NP header

Once the boundaries of a timeslot and the owner of a timeslot are known, the LNE unit can receive and process the tactical and technical messages transmitted in the timeslots owned by its RF neighbors.

The IJ or SJ LNE unit performs two algorithms on the collected information in order to reconstruct an NCS as similar to the actual ONCS as possible.

- Autocorrelation, based on the computation of the NCT as the distance between the absolute maximum and the first local maximum of the autocorrelation function, generated from the collected preambles
- Pattern Matching, based on the search for a pattern of data which is repeated every NCT

If a potential NCT is determined (it can be a multiple of the actual NCT), an NCS is produced using information about the identified NUs. If some preambles were not received and thus invalid timeslots were produced that were larger than allowed, they are split into multiple smaller timeslots; if a timeslot owner was not identified because Explicit Source Identification was not used, a default owner is assigned. If an LNE SLOT POSITION technical message (see the following section) reporting the actual NCT is received, the computed NCS is trimmed, if necessary, before applying LNE SLOT information.

After this stage the Silent Join LNE protocol is complete. The SJ unit can receive traffic on the network, and start to supply Tactical information to its DLP. The SJ unit will not actively participate in network management activities, however if it receives reconfiguration or re-initialization information it will be able to implement them just as though it was a member of the network, thereby maintaining reception on the network as it changes. Any received information about any other networks in the Super Network could be used to provide quicker access to those networks if additional LNE is required.

3B.8.3 LNE Slot

Successful Inactive Join requires that a LNE Slot is inserted into the ONCS. The NMU SNC inserts the LNE slot when requested by the NMU operator (e.g. when an IJ unit is expected), or when ordered by the SNMU. All or part of an existing slot is used as the LNE slot. The LNE Slot may occur every NCT, or it may be available only on a periodic multiple of the NCT, based on the Repetition Rate. The NMU SNC calculates the location of the LNE Slot, using the following criteria.

- Select unassigned minislots first
- If no unassigned slots exist, select the slot with the lowest reported capacity utilization
- If there is a tie, select a slot from the NU with the most assigned capacity
- If there is still a tie, use a random selection
- The allowable size of the LNE slot is the same as described for a Priority Injection slot (see [Figure 2B.4-6 Valid Timeslot Sizes](#))
- The LNE Slot must not take all of a unit's transmission capacity away
- The LNE Slot must not cross timeslot boundaries

The Network Cycle Time, LNE Slot position, and repetition rate are transmitted within the LNE SLOT POSITION technical message, which is distributed across the network by all network members.

Successful decryption requires that the source of the received message is known. An IJ or SJ LNE unit does not know who is transmitting, so only messages that use the Explicit Source Identification can be decrypted. The Explicit Source Identification is used when space permits, and is always used in the first NP of every timeslot when a LNE Slot has been inserted into the ONCS. If possible, the LNE SLOT POSITION technical message is inserted into the first Network Packet of the timeslot, so that it uses Explicit Source Identification, and therefore can be decrypted by the LNE unit.

Note: The LNE Slot is not required for successful SJ and not necessary for IJ until the IJ unit needs to transmit. It is advantageous to insert the LNE Slot before SJ or IJ LNE starts. This can help speed up the Media Parameter Acquisition phase by allowing the LNE unit to correctly decrypt more messages, and helps to maximize ONCS ownership detection.

The Inactive Join unit has to listen to the network traffic for the LNE SLOT Position technical message. The IJ SNC informs its DLP that it is searching for the LNE Slot

by sending a 'LNE Status' (409h) message. After the position of LNE Slot is determined, it can use the slot to communicate with its RF neighbors on the network.

When the IJ unit transmits in the LNE Slot, it sets the Explicit Source Identification to a random NILE Address, since it may not have a NILE Address yet. The Explicit Source Identification is used by the receiving units to decrypt the message, but not to identify the source LNE unit.

Multiple IJ units in the same area may compete for use of the LNE Slot. If an IJ unit does not receive a response to a request it sent, a collision in the LNE Slot may have occurred. The IJ units then take random turns using the LNE Slot.

3B.8.4 Supporting Unit

Communications between the IJ unit and the SNMU and NMU are made using a Supporting Unit (SU), which is a NU active in the Super Network and an RF neighbor of the IJ unit that acts as a bridge between the IJ unit and the SNMU and the NMU.

The IJ unit’s SNC transmits a SUPPORT UNIT SEARCH technical message in the LNE Slot. A RF neighbor that can be a supporting unit responds with a SUPPORT UNIT RESPONSE message, indicating its distance from the NMU and SNMU as defined in Figure 3B.8-13.

Indicated Distance	Meaning
0	NU is the NMU/SNMU
1	NU is one leg away from NMU/SNMU
2	NU is two legs away from NMU/SNMU
3	NU is three legs away from NMU/SNMU
4	NU is more than three legs away from NMU/SNMU

Figure 3B.8-13 SU Distance from NMU/SNMU

If the unit is the SNMU or NMU it responds immediately, whereas other units have to wait to see if they respond. The SNMU or NMU will not respond if it is already a SU for another IJ unit on the same network. The NMU will not respond if the SNMU responds.

Any other RF neighbor cannot be a supporting unit if any of the following apply.

- Either the SNMU or NMU has transmitted a SUPPORT UNIT RESPONSE technical message
- The unit is already a SU for another IJ unit on the same network
- It has received a SUPPORT UNIT RESPONSE technical message which has a total distance to the NMU and SNMU less than or equal to its own

The IJ unit listens to responses for 2 NCT, and then selects the SU from those that responded, using the following precedence.

- SNMU
- NMU
- Closest SU (NMU distance + SNMU distance)

Figure 3B.8-14 shows this protocol. The IJ unit sends the SUPPORT UNIT SEARCH technical message, which is received by RF neighbor NUs 2, 3, 4, and 5. The table

shows the order of NU transmissions, and the contents of the response made by each, if any. The IJ unit selects NU 4 as the SU over NUs 2 and 3, because NU 4 is the NMU.

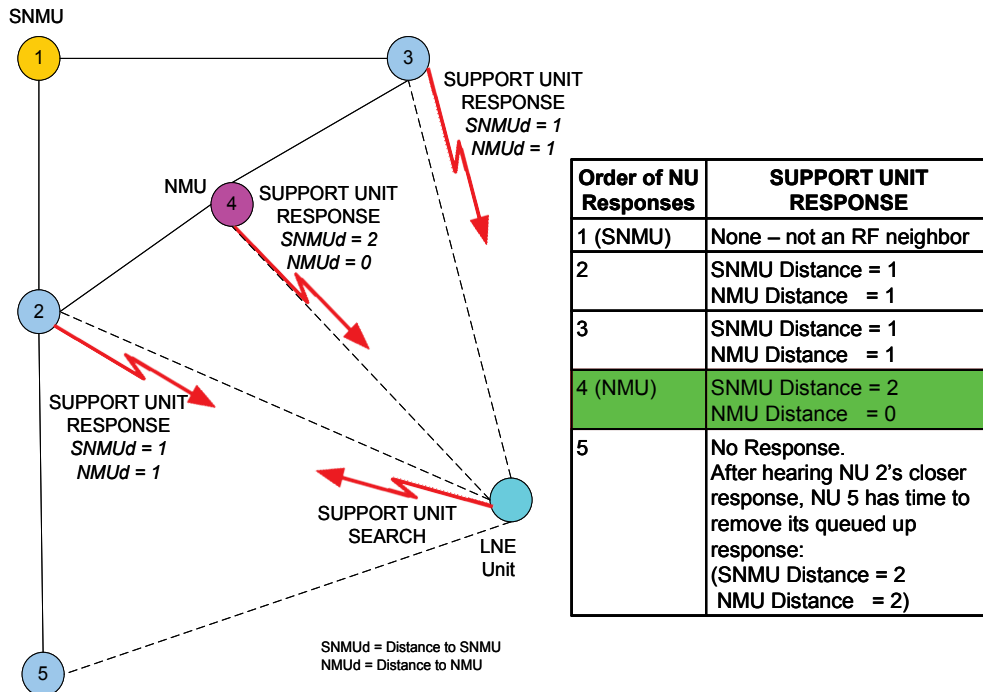


Figure 3B.8-14 Supporting Unit Search

If no responses were received, the IJ unit tries again by sending another SUPPORT UNIT SEARCH technical message. This process continues until a SU is found, or the protocol times out.

After the IJ unit SNC selects a SU, the SNC sends the LNE REQUEST technical message to the SU in the LNE Slot, requesting to join the network. The request indicates which information the IJ unit needs (ONCS, SN Directory, NILE Address, and Transmission Capacity), as listed in [Figure 3B.8-15](#).

LNE REQUEST Field	Description
SU NILE Address	The SU the IJ unit selected
IJ unit NILE Address	0 if the IJ unit needs a NILE Address
Action	Start LNE Protocol
Address, MASN, Status Version Numbers	The current Version Numbers of the IJ unit's SN Directory
Role Request	True if IJ unit needs the most recent roles
ONCS Request	True if IJ unit needs the most recent ONCS
Tx Capacity Need, Access Delay	Included if IJ unit wants transmission capacity in the ONCS

Figure 3B.8-15 LNE Request

An IJ unit that is a receive-only unit wanting transmission capacity on the network would already have a NILE Address, and a current SN Directory and ONCS. An inactive IJ unit may or may not have a NILE Address already assigned, and is likely to need an updated SN Directory and ONCS.

The SU acknowledges reception of the LNE REQUEST with a LNE REQUEST ACK, which includes the Operational Start Time of the ONCS, if the IJ unit requested ONCS information. The SU will also send the ONCS and SN Directory information, as necessary. The message exchange between the IJ unit and the SU during this phase, assuming the IJ unit needs all updated information, is shown in [Figure 3B.8-16](#).

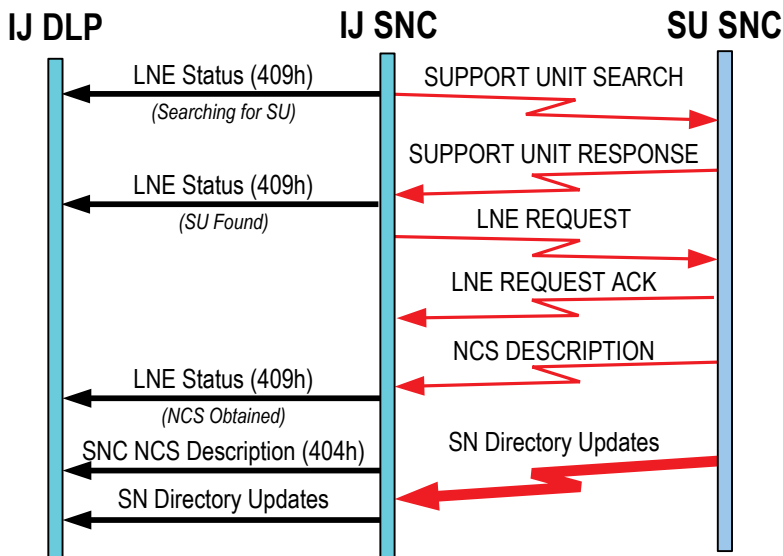


Figure 3B.8-16 IJ Unit-SU Communications

Figure 3B.8-17 shows the details of the SN Directory updates. The SU first sends the DIRECTORY RESPONSE technical message to inform the LNE SNC of the state of the SN Directory so that it knows what updates to expect. Other messages are sent as necessary.

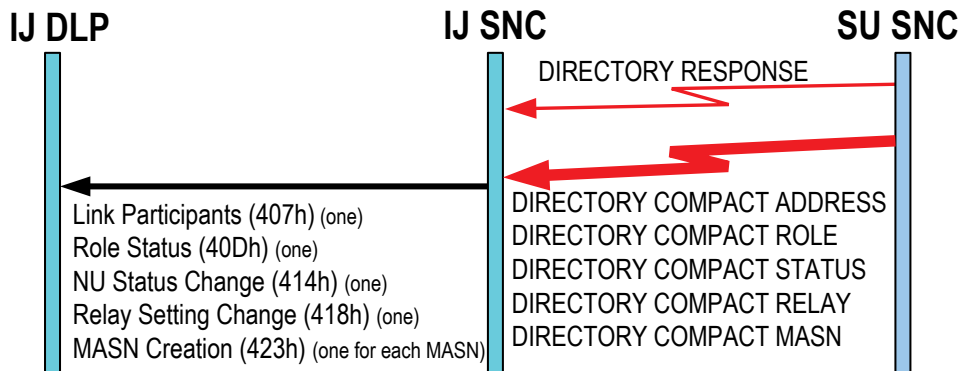


Figure 3B.8-17 LNE SN Directory Updates

3B.8.5 Permission to Join from the SNMU

A unit must get permission from the SNMU to join a network, if it was not already expected to be an active member of the network. If permission is needed, the AJ NU, or the SU (if it is not the SNMU) for the IJ unit, sends a NU ENTRY REQUEST technical message to the SNMU. The SNMU DLP/Operator is asked for permission for the unit to be added to the network MASN, if necessary. These decisions are summarized in [Figure 3B.8-18](#).

NILE Address	Member of Network MASN	Assigned timeslots in ONCS	Send NU ENTRY REQUEST to SNMU SNC	Permission from SNMU DLP required
No	N/A	N/A	Yes	Yes
Yes	No	N/A	Yes	Yes
Yes	Yes	No	Yes	No
Yes	Yes	Yes	No	No

Figure 3B.8-18 NU ENTRY REQUEST Requirements

The SNMU DLP/Operator has three choices.

- Grant access to the requested network
- Grant access to an alternate network (discussed below)
- Deny access to all networks

If access is granted, the following actions occur.

- SNMU SNC assigns a NILE Address to the IJ unit, if necessary
- SNMU SNC reports new NILE Address (if allocated) to all Super Network members (refer to section [3B.5 SN Directory Maintenance](#))
- SNMU DLP adds the unit to the MASN, if necessary (refer to section [3B.5 SN Directory Maintenance](#))

In all cases, the SNMU SNC returns the results of the request to the sender. In most cases, the results are reported to the DLP, which for IJ requires that the SU send the LNE RESPONSE technical message to the IJ unit. [Figure 3B.8-19](#) summarizes the actions at the LNE DLP for different cases.

LNE Type	TX Capacity Required	Access	LNE DLP Results
IJ/AJ	No/Yes	Denied	LNE Failure (40Ah): LNE Request Denied by SNMU LNE protocol is finished
IJ/AJ	No/Yes	Granted on alternate network	LNE Status (409h): Denied on network, granted on alternate network. Refer to section 3B.8.9 Access Granted on Alternate Network for further details
AJ	No/Yes	Granted	LNE Status (409h): LNE Granted
IJ	No	Granted	LNE Status (409h): LNE Granted LNE protocol is finished
IJ	Yes	Granted	Nothing reported to DLP yet – SU waits until results of Transmission Capacity Request are received

Figure 3B.8-19 Results of Request for Permission to Join a Network

Figure 3B.8-20 shows this protocol for an IJ unit without a NILE Address and no transmission capacity needed, which is granted permission by the operator to join the requested network. The transmission by the SNMU of the messages necessary to inform all other SN members of the new NILE Address and updated network MASN are not included in the figure.

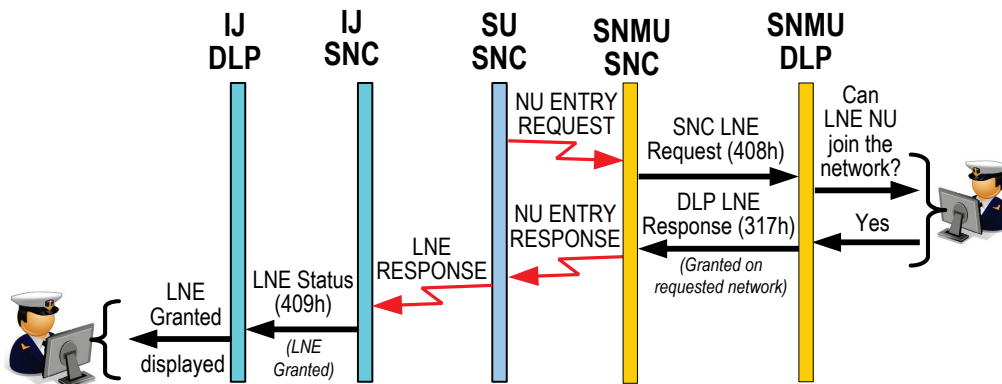


Figure 3B.8-20 NU ENTRY REQUEST Protocol

Note that even if the unit is not requesting transmission capacity, the SNMU must still be notified that the unit is joining the network, so that the SNMU can set the unit's status to Receive-Only in the network, and report this NU Status to all Super Network members.

If no transmission capacity was requested, the SU will send the LNE RESPONSE to the IJ unit after the SNMU has responded to the request to join the network.

If no NU ENTRY REQUEST is necessary, the SU will not send the LNE RESPONSE message to the IJ unit. Instead, the IJ SNC will immediately send the DLP a final 'LNE Status' (409h) message indicating LNE Granted and Capacity Allocated, and the IJ unit is then able to start transmitting on the network.

3B.8.6 Network Information from NMU

After an AJ NU is granted access to a network, the AJ SNC will transmit a NETWORK PARAMETER REQUEST technical message to the NMU of the granted network in order to obtain the media parameters and ONCS description, including the DTDMA status of the network. After receiving the media parameters, the operator configures the necessary hardware for the new network, and either informs the DLP when finished or he may decide to terminate LNE if the necessary hardware is not available. The DLP will send the 'DLP LNE Request' (316h) message to the SNC with one of the following.

- Continue with LNE protocol (transmission capacity is needed)
- Initialize the Network (no transmission capacity needed)
- Terminate LNE

Figure 3B.8-21 shows an example of this protocol.

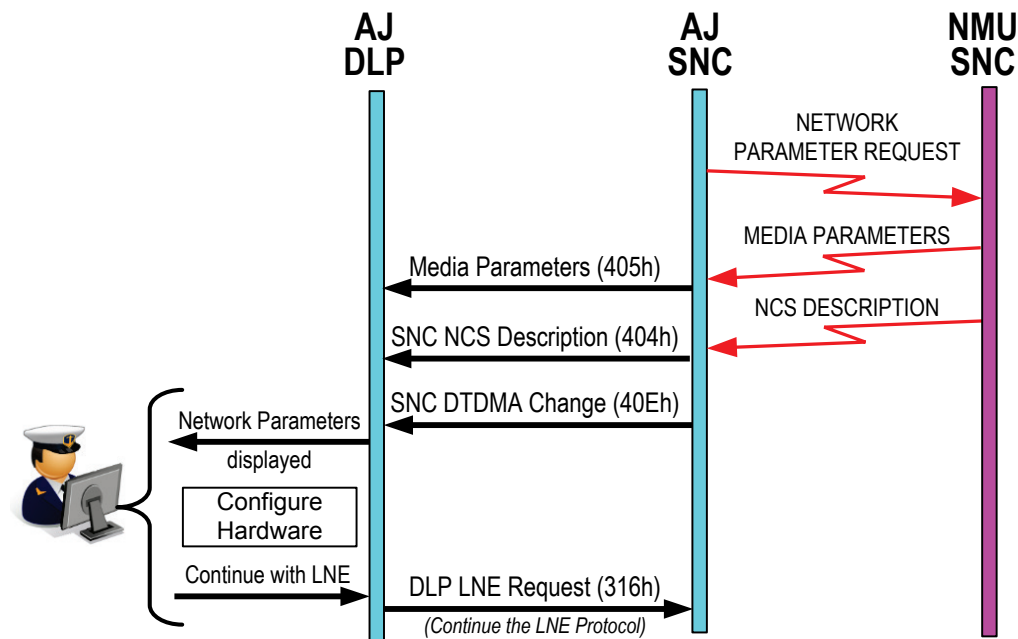


Figure 3B.8-21 AJ LNE Network Information from NMU

3B.8.7 Capacity Allocation by NMU

If transmission capacity was requested, and the unit does not have any assigned timeslots in the ONCS yet, a TRANSMISSION CAPACITY REQUEST technical message is sent by the SU (if it is not the NMU) or by the AJ NU to the NMU of the network. Figure 3B.8-22 indicates when the message is sent.

LNE Type	Access	Trigger
IJ/AJ	Granted on alternate network	DLP LNE Request (316h): Continue with LNE Protocol on alternate network
AJ	Granted	DLP LNE Request (316h): Continue with LNE Protocol
IJ	Granted	NE ENTRY RESPONSE: Confirm

Figure 3B.8-22 When is TRANSMISSION CAPACITY REQUEST sent?

The NMU DLP/Operator is responsible for deciding how to allocate capacity for the unit. The DLP/Operator has two choices.

- Allocate capacity immediately by assigning unused timeslots in the ONCS or timeslots temporarily assigned to the NMU
- Allocate capacity later (by a reconfiguration or re-initialization)

The NMU SNC sends the TRANSMISSION CAPACITY RESPONSE to the sender, indicating the allocated slots, or that no slots were currently allocated. After the SU has received the reply (from the NMU SNC or from its own DLP if it is the NMU), the SU sends the results to the IJ unit in a LNE RESPONSE.

The LNE RESPONSE includes the following.

- Permission to Join: Confirmed
- NILE Address, if assigned
- ONCS slots assigned, if any

The LNE SNC sends its DLP the ‘LNE Status’ (409h) message indicating that the transmission capacity request is finished, including the number of slots allocated, which can be zero if no slots were allocated. If slots were allocated, the SNC will send the ONCS change to the DLP in a ‘Permanent Reallocation’ (412h) message.

Figure 3B.8-23 shows the transmission capacity request protocol for an IJ unit that is granted capacity in the ONCS in the original requested network.

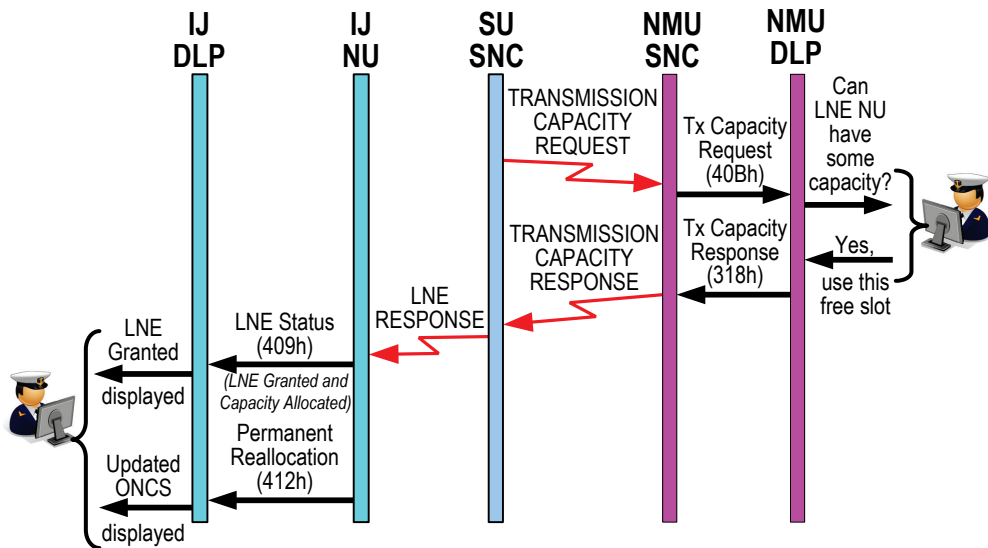


Figure 3B.8-23 IJ Transmission Capacity Request Protocol

3B.8.8 Completion of the LNE Protocol

After all LNE protocol transmissions are completed, if the transmissions were made on a network that is different than the network that is being joined, the LNE SNC will initialize the network by configuring the LLC and SPC to be used for the network, as required. After the configurations are complete, the LNE SNC will report 'Network Initialization Complete' (422h) to its DLP.

After completion of the LNE protocol, the LNE unit transmits in its assigned timeslots (if any) using Explicit Source Identification for the first 10 NCTs, so that receiving units can correctly decrypt the messages, and update the ownership of the timeslots.

Figure 3B.8-24 shows the messages that indicate the end of LNE, for different cases. Note that when SJ and IJ succeed on the requested network, the network does not need to be initialized, as it is the network that was being used to perform the LNE protocol. All other cases require a network initialization for the granted network.

LNE Type	TX Capacity Required	Access	End of LNE Messages
IJ/SJ	--	--	LNE Failure (40Ah), any reason
SJ	--	--	LNE Status (409h): Parameters Obtained Media Parameters (405h)
IJ/AJ	No/Yes	Denied	LNE Failure (40Ah): LNE Request Denied by SNMU
IJ/AJ	No	Granted on alternate network	Network Initialization Complete (422h)
IJ/AJ	Yes	Granted on alternate network	LNE Status (409h): Capacity Allocated Permanent Reallocation (412h) (if ONCS changed) Network Initialization Complete (422h)
AJ	No	Granted	Network Initialization Complete (422h)
AJ	Yes	Granted	LNE Status (409h): Capacity Allocated Permanent Reallocation (412h) (if ONCS changed) Network Initialization Complete (422h)
IJ	No	Granted	LNE Status (409h): LNE Granted
IJ	Yes	Granted	LNE Status (409h): LNE Granted and Capacity Allocated Permanent Reallocation (412h) (if ONCS changed)

Figure 3B.8-24 Messages Indicating the End of the LNE Protocol

Figure 3B.8-25 is a combined flow of IJ LNE that is granted on the requested network, and allocated transmission capacity. The displayed flow starts after the media parameters have been acquired. Operator interactions are not shown.

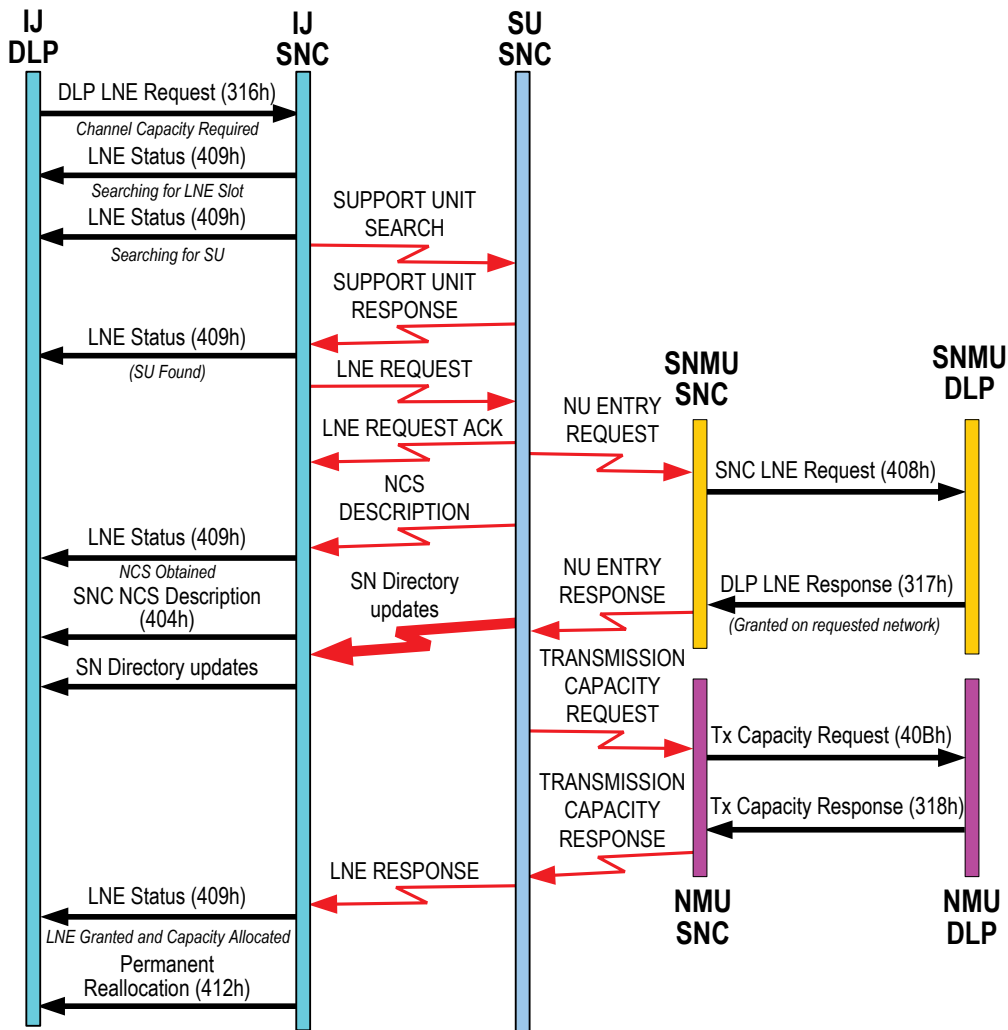


Figure 3B.8-25 IJ LNE After Media Parameter Acquisition

Figure 3B.8-26 shows the flow of AJ LNE that is granted on the requested network, and allocated transmission capacity. Operator actions are not shown.

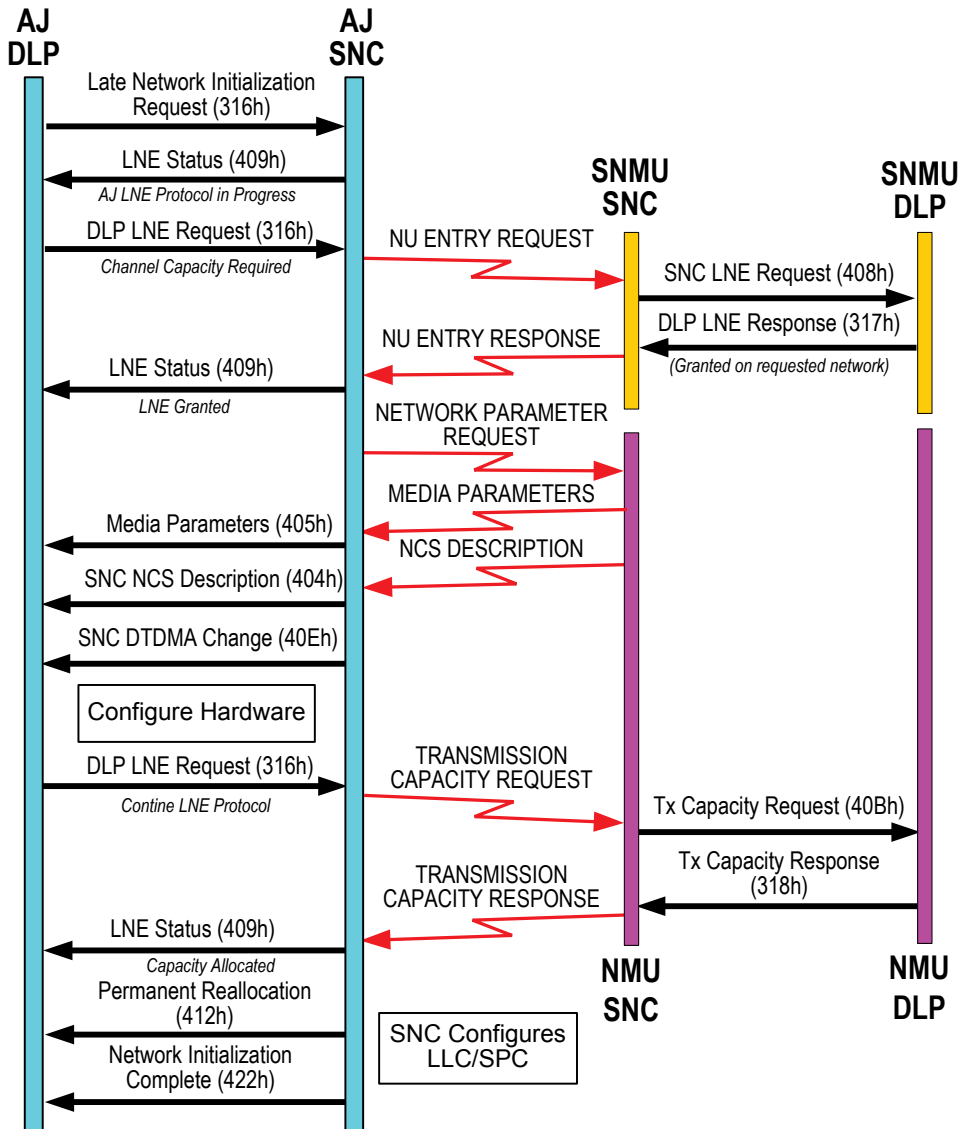


Figure 3B.8-26 AJ LNE Protocol

3B.8.9 Access Granted on Alternate Network

When the SNMU DLP/Operator is asked to grant permission for a LNE unit to join a network, he may choose to grant access to a different network than the LNE unit requested to join. In this case, the AJ NU or SU acquires the media and network parameters for the alternate network by sending a NETWORK PARAMETER REQUEST technical message to the NMU of the network on which the join is granted, if the information is not already known by the SU or AJ NU.

The parameters for the alternate network are sent to the LNE DLP/Operator, so that the DLP/Operator can decide whether or not to join the alternate network. For example, the alternate network may be using a media type that requires a different type of SPC that the unit does not have. The DLP informs the SNC of the decision by sending the 'DLP LNE Request' (316h) with one of the following choices.

- Continue the LNE Protocol on the alternate network (capacity is needed)
- Initialize the alternate network (capacity is not needed)
- Terminate LNE

□ **Transmission Capacity Needed**

If the LNE unit needs transmission capacity on the alternate network (responded with 'Continue the LNE protocol'), the transmission capacity needs to be requested from the NMU. Since this requires transmissions, this part of the protocol is performed on the original network, not the alternate network. The IJ unit sends another LNE REQUEST technical message to the SU, including the data shown in [Figure 3B.8-27](#).

LNE REQUEST Field	Description
SU NILE Address	The SU the IJ unit has been already using
IJ unit NILE Address	The IJ unit's NILE Address
Action	Join Alternate Network
Address, MASN, Status Version Numbers	Up to date
Role Request	False, up to date
ONCS Request	False, already acquired
Tx Capacity Need, Access Delay	Required capacity

Figure 3B.8-27 LNE Request on Alternate Network

The SU or AJ NU requests transmission capacity from the NMU of the alternate network, and the results are made available to the LNE DLP, as discussed in section [3B.8.7 Capacity Allocation by NMU](#).

□ Initialization of the Alternate Network

The AJ LNE protocol used when access is granted on an alternate network is essentially the same as that used when access is granted on the requested network. The only difference is that the ‘LNE Status’ (409h) message indicates ‘Denied on network, granted on alternate network’, and the AJ unit then asks for transmission capacity from the NMU of the alternate network instead of the originally requested network. The operator only initializes the network that the SNMU granted access to.

For IJ LNE that requested transmission capacity on the alternate network, the operator needs to reconfigure the hardware for use by the alternate network after the transmission capacity request processing has been completed on the original network. When finished, the operator informs the DLP, and the DLP sends a ‘DLP LNE Request’ (316h) indicating ‘Initialize the Network’. The LNE SNC configures the LLC and SPC for the alternate network using the short initialization protocol and upon successful configuration reports ‘Network Initialization Complete’ (422h) to inform the DLP that the network is now operational.

[Figure 3B.8-28](#) is an example of the IJ LNE protocol when access is granted on an alternate network, and transmission capacity is requested. The protocol is shown starting with the results of the original LNE request being reported by the SU to the IJ LNE unit. Operator interactions are not included in the figure.

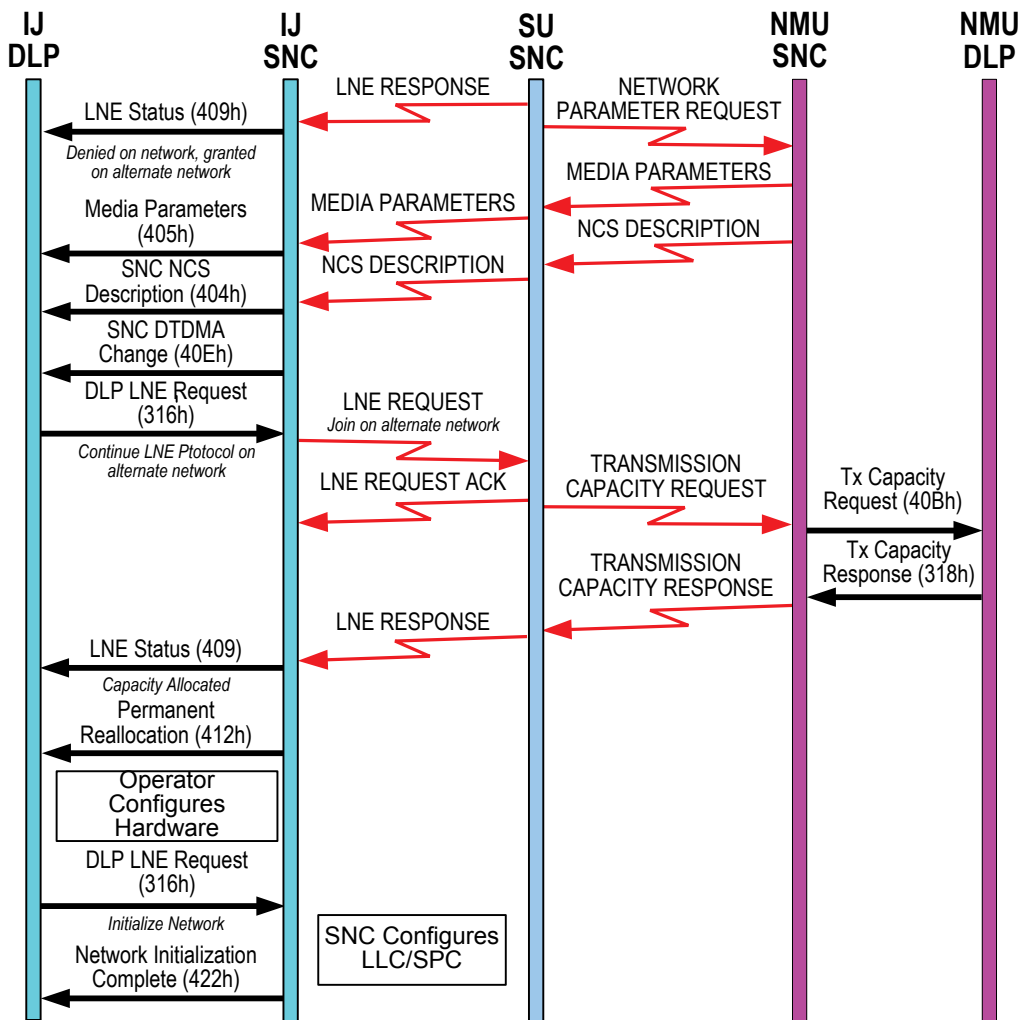


Figure 3B.8-28 IJ LNE Granted on Alternate Network

3B.8.10 LNE Failures

LNE can fail for a variety of reasons. All LNE failures are reported to the DLP in the ‘LNE Failure’ (40Ah) message, and then the LNE protocol terminates. The DLP can start another LNE attempt, if desired. [Figure 3B.8-29](#) shows the LNE failures that can be reported by the SNC.

LNE Phase	Possible Failures
Media Parameter Acquisition	Media Configuration Failure Unable to Detect Preamble Incorrect MSN Unable to Detect Fragmentation Rate
ONCS Deduction	NCS not Possible
LNE Slot Detection	Unable to Detect LNE Slot
Supporting Unit Search	Support Unit Not Found
Permission to join from SNMU	LNE Request Denied by SNMU

Figure 3B.8-29 LNE Failures

3B.9 Closedown

A closedown causes all communications to stop on a network or in the Super Network. This may be temporary or final. The following topics are described.

- Super Network Closedown
- Network Closedown
- NU Closedown
- Loss of a NU

The SNMU Operator may use an external channel to give the order, which can then be executed locally by the DLP Operator of any unit.

3B.9.1 Super Network Closedown

Super Network (SN) Closedown terminates the operation of an entire Super Network and has to be ordered by the Officer in Tactical Command (OTC), and then sent as an order from the SNMU to all NUs. The time to shutdown has to be at least 10 minutes in the future, to allow distribution of the message to all NUs with possible retransmissions. A SN Closedown is not delayed by any other order or operation in the system and will be executed by the receiving NUs at the indicated time.

The order is processed by all receiving NUs as discussed in section [3-92 Orders](#). The SNMU SNC internally sends itself a ‘Stop Communications’ (319h) message after receiving the SN Closedown order from the DLP. The SNC of all NUs updates its SN Directory to indicate that it will become inactive at the specified time.

At the time of closedown, each SNC performs the following sequence.

- Stops transmitting all tactical and technical messages
- Discards any received tactical or technical messages
- CANTCOs any TSRs from the DLP or internal TSRs from the SNC
- Discards all outstanding TSRs
- Shuts down each SPC. Send the 'SPC Configuration Request' (00C1H) message with BIT/Loopback field set to 'SPC Shutdown'
- Shuts down each LLC. Send the 'LLC Configuration Request' (8100H) message with the 'Number of SPCs' field set to 0, to indicate shutdown of all SPCs
- Informs the DLP that communications have been terminated

An example of the SN Closedown protocol is shown in [Figure 3B.9-1](#), with automatic order processing turned off.

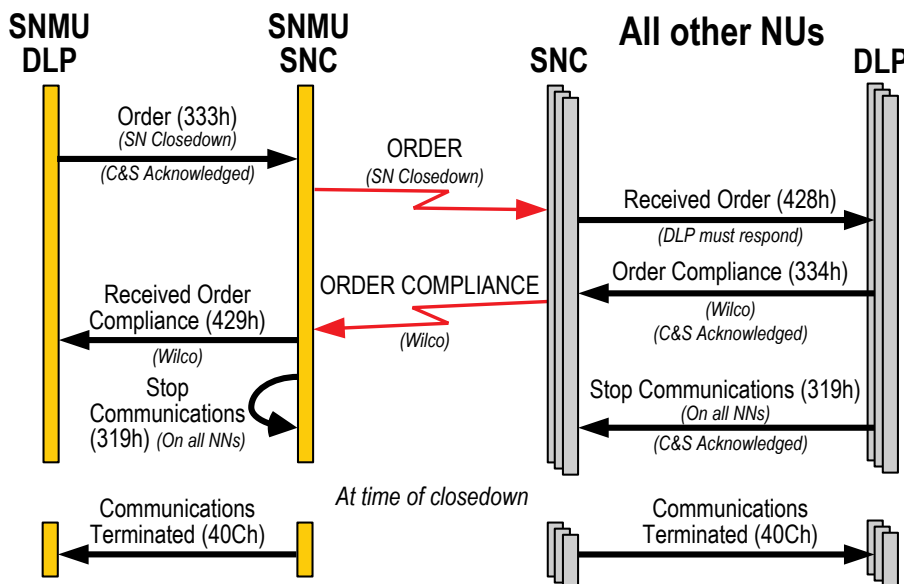


Figure 3B.9-1 SN Closedown

3B.9.2 Network Closedown

Network Closedown terminates the operation of an entire NILE network. The NMU can order a Network Closedown, and the SNMU can order the NMU to order a Network Closedown.

Processing is similar to that used for SN Closedown. The NN Closedown order from the NMU is processed by all receiving NUs as discussed in section [3-92 Orders](#). The NMU SNC internally sends itself a ‘Stop Communications’ (319h) message for the network. At the time of NN Closedown, each SNC in the network being closed performs the following sequence.

- Stops transmitting all messages on the network being closed
- Shuts down the SPC for the closed network. Send the ‘SPC Configuration Request’ (00C1H) message with BIT/Loopback field set to ‘SPC Shutdown’
- Reconfigures the LLC that was used for the closed network. Exclude the SPC of the closed network, include all other SPCs that are currently in use by the LLC, keeping the same configuration
- Informs the DLP that communications have been terminated on the network

An example of the NN Closedown protocol is shown in [Figure 3B.9-2](#), starting with an order from the SNMU, with automatic order processing activated by all involved NUs.

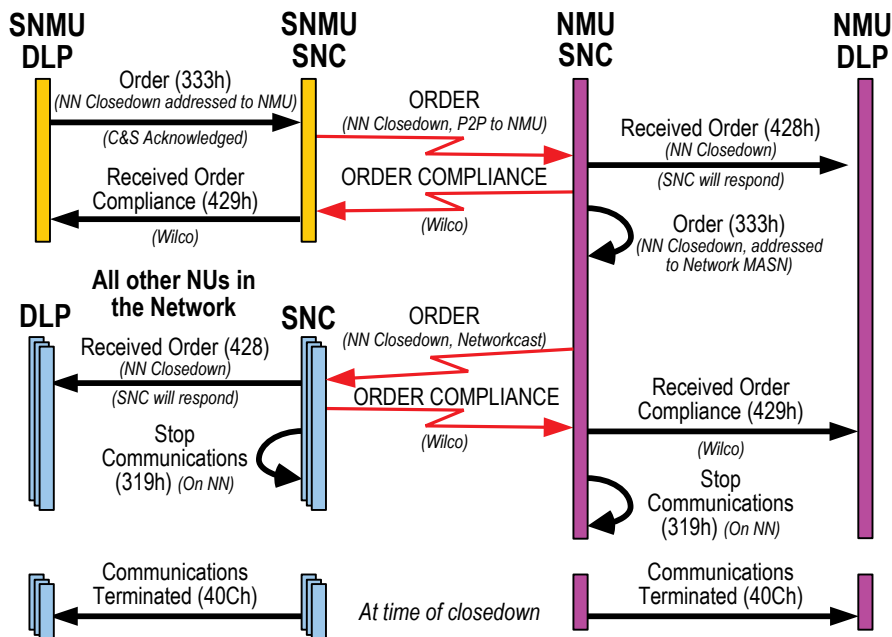


Figure 3B.9-2 NN Closedown

After a network is shut down, the DLP/Operator of the SNMU may need to update the SN Directory.

- **Network Membership MASN:** If the network closedown is permanent, the network MASN can be deleted. However, the MASN may be kept so that messages can be addressed to the units that were in the network that closed down
- **NU Status:** If a NU closed down on its only network, the SNMU automatically changes the NU Status to Inactive. If it is Receive Only or Radio Silent on other networks, a different NU Status value may be applicable. For details see section [3B.5 SN Directory Maintenance](#)

3B.9.3 NU Closedown

An NU can close down on the Super Network (SN) or on a NILE Network (NN), either temporarily or permanently, at a specified future time or immediately, as listed below.

- NU closedown in SN or NN locally ordered by the DLP Operator
 - Temporary
 - Permanent
- NU closedown in SN ordered by the SNMU
- NU closedown in NN ordered by the SNMU or NMU

When the NU permanently leaves the SN or a NN, it informs all other NUs of its intention to leave by sending a NOTIFICATION technical message (if there is time to send it). Upon reception of the NOTIFICATION, all other SNCs inform their DLPs, with a 'Received Notification (42Bh) message, that the NU is intending to leave at the specified time, and update their internal connectivity tables when the NU leaves. When the NU temporarily closes down on the SN or a NN, it does not notify any other NUs because it is planning to restart.

Figure 3B.9-3 summarizes the types of NU closedowns, and the messages used to initiate the closedown.

Closedown Type	Initiated By	Message	Other Units Notified
Temporary SN Closedown	Own Unit	Stop Communications (319h) (All Networks Flag = True)	No
Permanent SN Closedown	SNMU Own Unit	Order (333h) (Leave SN) NU Leave (31Ah) (All Networks Flag = True)	Yes
Temporary NN Closedown	Own Unit	Stop Communications (319h) (All Networks Flag = false, NN specified)	No
Permanent NN Closedown	SNMU or NMU Own Unit	Order (333h) (Leave NN) NU Leave (31Ah) (All Networks Flag = False, NN specified)	Yes

Figure 3B.9-3 NU Closedown Summary

In the case of an order, the NU Leave (31Ah) is always generated either by the DLP when automatically perform order is off or by the SNC internally, when the automatically perform order is on.

At the time the NU leaves the SN or a NN, its SNC performs the same actions that were described in section [3B.9.1 Super Network Closedown](#) or section [3B.9.2 Network Closedown](#).

After a NU has left a NN or the SN, the DLP/Operator of the SNMU can modify the associated network MASN(s) to remove the NU, as described in section [3B.5 SN Directory Maintenance](#).

After a NU has left the SN, the SNC of the SNMU sets the NU Status of the leaving NU to Inactive, and informs all other NUs, as described in section [3B.5 SN Directory Maintenance](#).

Note that when a NU is leaving the last network (All Network Flag is false), it is assumed that the NU is going to initialize on a new network, or join another existing network relatively soon. Therefore the SNMU will not change the NU Status to Inactive. If the NU intends to leave the SN, the All Networks Flag should be set to true.

[Figure 3B.9-4](#) shows a NU temporarily closing down on a network. For simplicity, the LLC Status Request (0100H)/Response (F100H) and SPC Status Request (0001H)/Response (00F1H) messages are not included in the figure. Notice that no NOTIFICATION is sent to any other NUs.

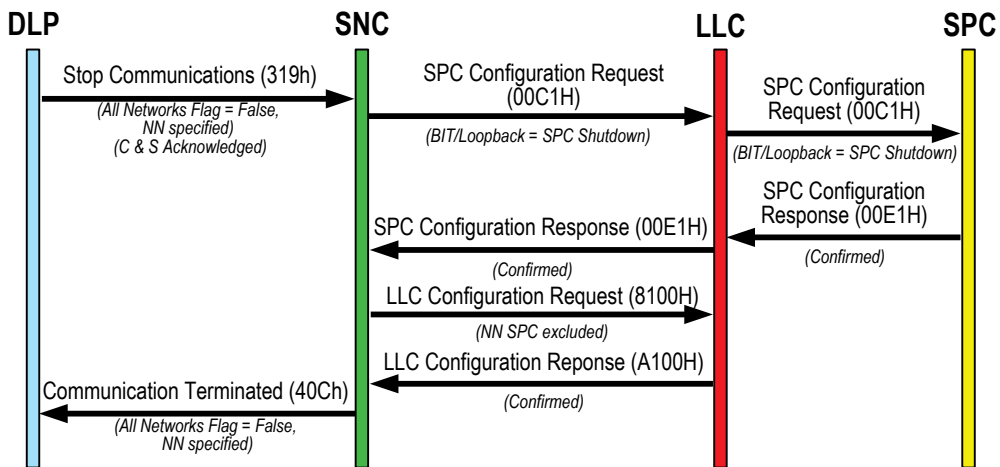


Figure 3B.9-4 Temporary NU Closedown on a Network

Figure 3B.9-5 shows an NU being ordered to leave the SN, with automatic order processing off. Note that when the SNC receives a 'NU Leave (31Ah)' message, it internally generates a 'Stop Communication' (319h) message to trigger the closedown processing that is the same for both types of closedown (temporary or permanent). Communications with the LLC/SPC are excluded from the figure.

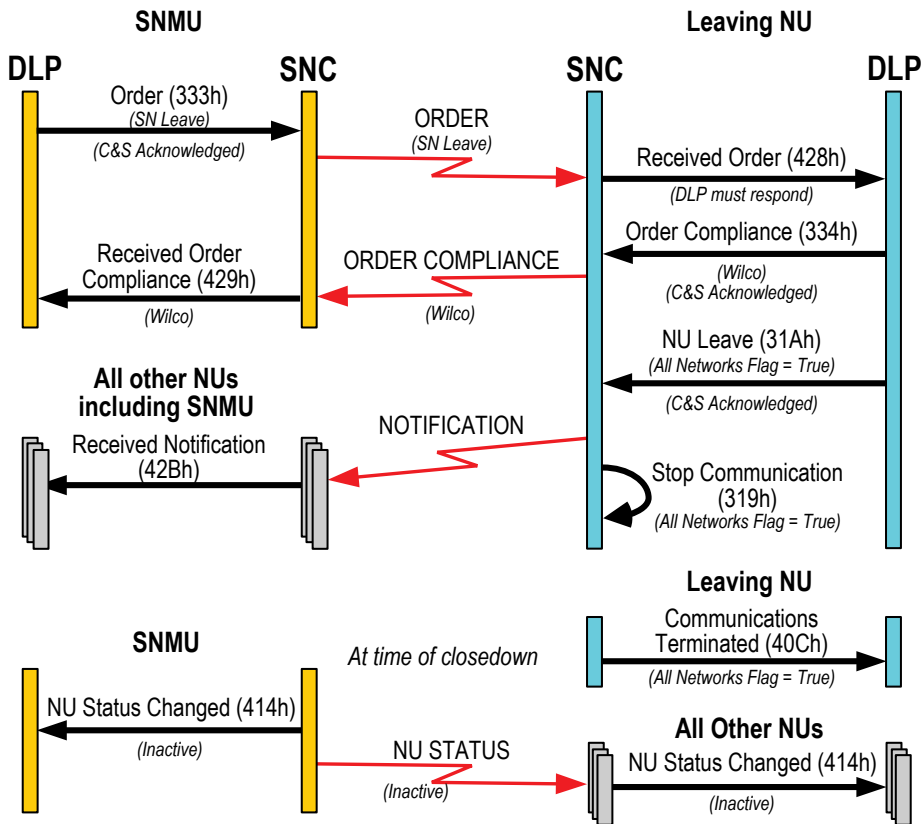


Figure 3B.9-5 SN Leave Order

After the NU leaves the Super Network, the DLP/Operator of the SNMU can remove the NU from the Network Membership MASN.

The other cases of NU closedown have similar protocols, except that the NU Status is not changed unless the NU leaves the SN.

3B.9.4 Loss of a NU

The DLP of the SNMU can detect the loss of communications from a NU by monitoring traffic from each NU. If the operator of the SNMU confirms by other communications channels that the NU will no longer be part of the Super Network, the following changes can be made.

- Set NU Status to Inactive (Mandatory)
- Remove NU from all applicable MASN_s, including the network membership MASN_s (Optional)

Also, the DLP of the SNMU can order or the NMU can activate a network reconfiguration to reassign the NU's capacity to other NUs.

The protocol to change the NU Status and the MASN_s after a NU is lost is shown in [Figure 3B.9-6](#).

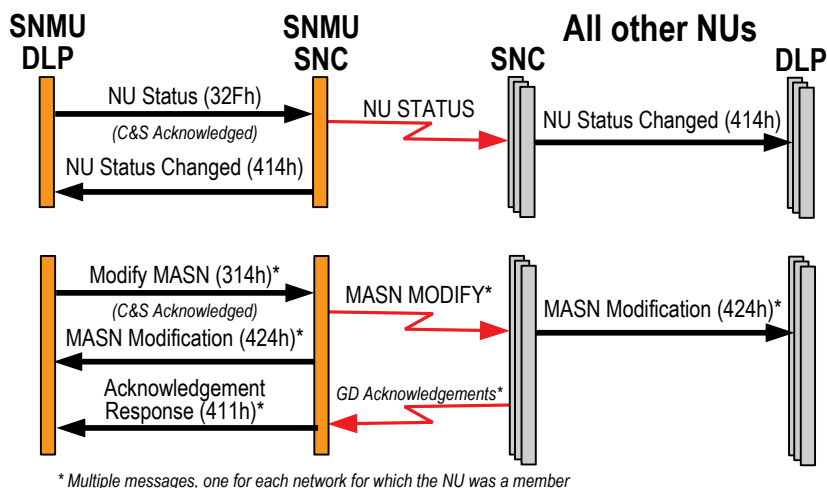


Figure 3B.9-6 NU Dropped from the Super Network

3B.10 Monitoring and Statistics

Monitoring of the system is done at the NU, Network, and Super Network level, and was discussed in Chapter 2 section 2C.2 Operation (since monitoring information can be displayed to the operator). Appendix B Troubleshooting also provides detailed monitoring information that helps to assess fault conditions and their resolution, including the 800-Series messages described in the [DLP-SNC IDD].

The following topics are discussed in this section.

- NU Data
- NU Performance Monitoring

Figure 3B.10-1 summarizes the DLP-SNC messages, and the related SNC-SNC Technical messages, if any, used in monitoring.

DLP-SNC Messages	SNC-SNC Messages
Channel Utilization (601h)	Internally calculated by each SNC
Connectivity Information (LRQ) (602h)	SHORT LINK RECEPTION QUALITY STANDARD LINK RECEPTION QUALITY COMPACT LINK RECEPTION QUALITY
Congestion Alert (603h)	CONGESTION INDEX
Error Rate Characteristics (604h)	Internally calculated by each SNC
DTDMA Participation (605h)	CAPACITY NEED GRANT RELIABILITY ACKNOWLEDGEMENT STATUS ACKNOWLEDGEMENT
NU Data (606h)	Reception of any traffic from each NU and Connectivity Information about distance
Connectivity Information (LCD) (607h)	STANDARD LINK CONNECTIVITY DATA COMPACT LINK CONNECTIVITY DATA
DLP NU Performance Data (332h)	NU PERFORMANCE
NU Performance Data (427h)	NU PERFORMANCE

Figure 3B.10-1 Monitoring Messages

3B.10.1 NU Data

The NU Data message is sent by the SNC to the DLP every 60 seconds. It provides valuable summary information about every unit in the Super Network, as listed in Figure 3B.10-2.

Message Field	Field Value
NILE Unit Link 22 Address	Link 22 Address of a unit in the SN
Received from the NU in the last day flag	This flag indicates if there was reception in the last 24 hours from the unit, and if so, indicates that the TOD of last Reception field is valid
TOD of Last Reception	The time of last reception from the unit, in seconds since midnight
Transmission Legs	This field indicates how many transmission legs are required to reach the unit. A value of zero indicates that the connectivity is not known (is more than three legs away)

Figure 3B.10-2 NU Data Fields

If TOD of last Reception is not being updated and Transmission Legs start increasing or becomes 0, this may indicate the unit has lost connectivity to the Super Network. This may be caused by one or more relay units being in Radio Silence. This could be only transient, or it could be a more lasting situation. The DLP should identify the situation for the Operator and recommend actions.

3B.10.2 NU Performance Monitoring

The SNMU, Standby SNMU, and the NMU and Standby NMU of each network monitor the performance of the system and network, from information supplied to them by each NU. Each SNC transmits a NU PERFORMANCE technical message every 20 minutes (on the hour, 20 and 40 minutes past) to the following (using technical MASN 18).

- SNMU
- Standby SNMU
- NMU for each network the NU is participating in
- Standby NMU for each network the NU is participating in

The message is also transmitted 30 seconds after a NU becomes active on a network, and upon change of data.

The NU PERFORMANCE technical message contains the same information that is sent to the DLP, as described in section 2C.2.3 Network Management. Trends of status, connectivity, congestion, and transmission needs included in this message could be used to determine the conditions for changes in the Super Network or individual network. For example, a Reconfiguration or Re-Initialization may be required if transmission needs are significantly different than the allocated ONCS capacity.

DLP NU Performance Data

The NU performance information can include 32 bits of tactical performance information. The DLP will calculate this information and send it to the SNC, as shown in Figure 3B.10-3. The SNC will include this information in the next NU PERFORMANCE technical message. The exact meaning of the tactical performance data is currently undefined.

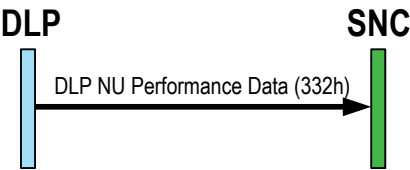


Figure 3B.10-3 DLP NU Performance Data

NU Performance Data

When the SNC receives the NU PERFORMANCE technical message, or when it transmits its own NU PERFORMANCE technical message, it sends the information to its DLP in the ‘NU Performance Data’ (427h) message, as shown in Figure 3B.10-4.

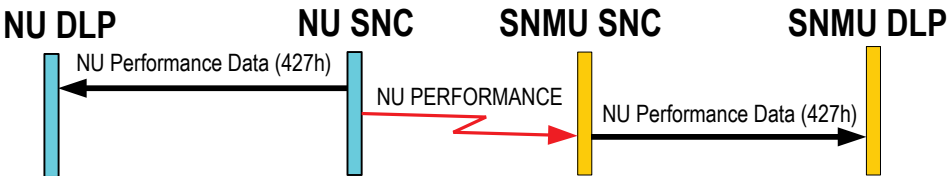


Figure 3B.10-4 NU Performance Data Protocol

Upon receipt of a NU PERFORMANCE technical message from a NU, the SNC of the SNMU will change the status of the NU to ACTIVE if it is not currently ACTIVE.

This page is intentionally left blank.

Section C Internal Protocols

Internal protocols are those that are not directly externally controlled or visible to the operator. Most of the protocols are concerned with the technical details of transmitting and receiving tactical and technical messages. Calculation of an NCS and Dynamic TDMA are also discussed. The protocols included in this section are the following.

- DLP-to-SNC Tactical Message I/F
- DLP TSR Management
- SNC TSR Queue
- SNC Transmission/Reception
- Addressing
- Duplicate Detection
- Network Cycle Structure Handling
- Relay & Routing
- Congestion
- Message Delivery & Reliability
- SNC Packing
- Dynamic TDMA (DTDMA)
- SNC-to-LLC Protocols
- LLC-to-SPC Protocols
- Technical Messages

3C.1 DLP-to-SNC Tactical Message I/F

This section details the DLP-SNC interface protocols used for the transmission and reception of tactical messages, and consists of the following sub-sections.

- Transmission
- Transmission Request Cancellation
- Transmission Priority Management
- Reception

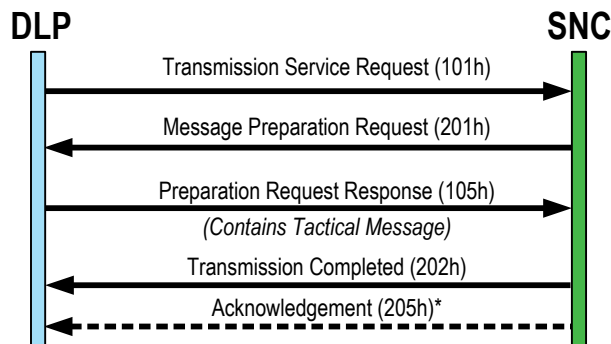
3C.1.1 Transmission

The DLP sends a ‘Transmission Service Request’ (101h) (TSR) message to the SNC to request the transmission of each tactical message. Two types of TSRs are available.

- TSR without Data
- TSR with Data

□ **TSR without Data**

If the tactical message is time dependent then the DLP sends a ‘Transmission Service Request’ (101h) (TSR) message to the SNC that does not contain the tactical message. The SNC will ask the DLP for the tactical message for the transmission time, called the Message Time of Validity (MTV). The DLP will extrapolate the tactical data to the time of transmission and supply the data to the SNC. The protocol for TSR without data is shown in [Figure 3C.1-1](#).



* Only sent if a TSR contained a Machine Receipt addressee.
Multiple messages may be sent.

Figure 3C.1-1 TSR without Data Protocol

□ **TSR with Data**

If the tactical message is not time dependent then the DLP can supply the tactical message data with the TSR (TSR with Data). As the SNC has the tactical message data it does not need to request it, so the second and third steps of the protocol are not necessary. This creates the simpler protocol for TSR with Data as shown in Figure 3C.1-2.

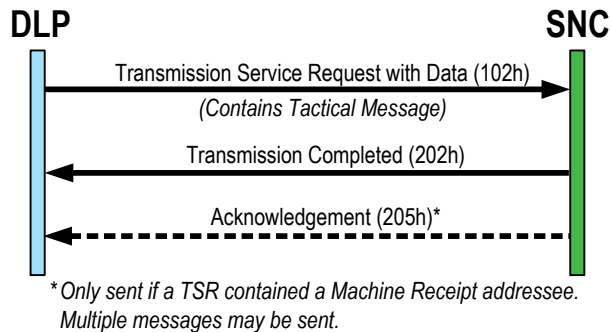


Figure 3C.1-2 TSR with Data Protocol

The three message flows are the same as those for the TSR without data.

The message flows listed are detailed in the following sub-sections.

- Transmission Service Request (TSR)
- Message Preparation Request (MPR)
- Preparation Request Response (PRR)
- Transmission Completed (TXC)
- Acknowledgement (ACK)

□ **Transmission Service Request (TSR)**

The information that the DLP supplies in the TSR is the same for both the TSR without data and TSR with Data (except for the data). The DLP supplies the following information.

- Service Request Identifier (SRID)
- Tactical Message Size
- Priority
- Source Track Number

- Reliability
- Priority Injection Indicator
- Perishable Message Indicator
- Radio Silence Override Indicator
- Addressee Information

■ ***Service Request Identifier (SRID)***

The DLP assigns a Service Request Identifier (SRID) to each TSR. The SRID is unique for the life of the TSR and is used in the protocols to identify the TSR. The DLP manages the allocation of SRIDs (covered in section [3C.2.4 SRID Management Function](#)) which are in the range 1-4095. If the DLP uses a SRID that is already in use then the SNC responds with an ‘SNC Cannot Comply’ (203h) message.

■ ***Tactical Message Size***

The DLP specifies how many Tactical Message Words (72-bits) are in the tactical message that it wants to transmit. The maximum number of TMWs that can be sent is eight.

■ ***Priority***

The DLP assigns a priority (1-4, with 1 being the highest) to each TSR. The use of Priority is described in [[STANAG 5522](#)], as the purpose/contents of a message affects the choice of Priority. The following are examples of various priority TSRs.

- 1 - Initial Hostile Surveillance Track Reports
- 2 - Initial Non Hostile Surveillance Track Reports
- 3 - Periodic Hostile Surveillance Track Reports
- 4 - Periodic Non Hostile Surveillance Track Reports

The DLP can change the priority of a TSR if the transmission has not yet been completed by sending a ‘Priority Change Request’ (106h) message to the SNC.

■ ***Source Track Number***

In the TSR, the DLP supplies the 15-bit Track Number of the unit that originated the tactical data. Usually this will be itself, but is different when forwarding data from another unit.

■ **Reliability**

For each TSR, the DLP can request Standard Reliability (80% probability of correct reception), High Reliability (90% probability of correct reception), or Guaranteed Delivery (GD). GD requires that there be at least one Machine Receipt (MR) addressee, which will take precedence over any Non Machine Receipt (Non-MR) addressees.

■ **Priority Injection Indicator**

The DLP can specify that a priority 1 message should be transmitted as soon as possible, in a Priority Injection timeslot, by setting the Priority Injection Indicator. The following rules must be met.

- The ONCS must have a Priority Injection (PI) timeslot
- The PI timeslot must occur before the unit's next allocated timeslot
- The unit must not have an allocated timeslot within 2.5 seconds after the PI timeslot

A message transmitted in a PI timeslot is also transmitted in the next assignment timeslot, because the PI timeslot may have been used by more than one unit at the same time which may cause reception problems. The DLP can change the Priority Injection Indicator and/or the Priority of a TSR if the transmission has not yet completed by sending a 'Priority Change Request' (106h) message to the SNC.

■ **Perishable Message Indicator**

The tactical data is only valid for a specific time period, and any data that has perished will not be relayed. The possible values are 15, 31, 63 and 511 seconds represented by values 0-3, respectively.

■ **Radio Silence Override Indicator**

If the unit is in Radio Silence, the DLP can request that the tactical message be transmitted anyway, by setting the Radio Silence Override flag in the TSR.

■ **Addressee Information**

Each TSR can specify two sets of destinations.

- Machine Receipt (MR), which requires an acknowledgement from the addressees
- Non-Machine Receipt (Non-MR), which does not require an acknowledgement

When both are specified, the MR destinations may take precedence. However, [STANAG 5522] does not currently address any tactical messages to both, at the same time.

Each set can be destined for one, multiple, or all units, using one of the following addressing techniques.

- Neighborcast - All NUs that are RF neighbors of the message originator, regardless of which networks they are operating on
- Point-to-Point - a single NU
- MASN - a predefined list of NUs grouped together and addressed by using a single number (MASN)
- Dynamic List - a list of up to a maximum of 5 NUs
- Totalcast - all NUs operating on the Super Network
- None

The DLP should not generate a TSR with both the MR Addressees and the Non-MR Addressees fields set to “NONE”. If it does, the SNC responds with a ‘SNC Cannot Comply’ (203h) message.

If Guaranteed Delivery (GD) is selected, the MR Addressee field cannot be “NONE”. If it is, the SNC responds with a ‘SNC Cannot Comply’ (203h) message.

□ ***Message Preparation Request (MPR)***

The ‘Message Preparation Request’ (201h) message that the SNC sends to the DLP is a request for the tactical message data for a number of TSRs, which are identified by the list of SRIDs in the message. The message also specifies the MTV. The SNC may request the tactical message data for the same SRID more than once. For example, the SNC may not have been able to transmit the message when it first requested the data, is now preparing to transmit again, and is requesting more up-to-date data. Also, if transmissions in different timeslots or Networks are required at a later time, the SNC may request updated data prior to the transmissions.

If the DLP receives a ‘Message Preparation Request’ (201h) with a SRID it cannot service, the DLP responds with a ‘DLP Cannot Comply’ (104h) message, for each SRID, and frees the SRID. The SNC cancels all transactions related to this SRID and frees the SRID. The SNC does not reply and the DLP does not expect a reply.

□ ***Preparation Request Response (PRR)***

The ‘Preparation Request Response’ (105h) message that the DLP sends to the SNC can contain the contents of one or more tactical messages, identified by their SRIDs, for the MTV specified in the message. The DLP should complete transmission of all PRRs as quickly as possible. When the SNC schedules an event to prepare a timeslot, it interpolates between the two values (Smallest Message Preparation Time and Largest Message Preparation Time) specified in the ‘MPT Specification’ (301h) message, based on the size of the timeslot (the number of tactical data words) and the knowledge of the other events happening at the same time. The DLP needs to respond in less time than the calculated amount so that the tactical message content is available to the SNC to be packed for transmission. If the DLP does not respond quickly enough the message may miss being packed and consequently would not be transmitted in the timeslot.

If the SNC receives a ‘Preparation Request Response’ (105h) message with a SRID that it is not processing, the SNC responds with a ‘SNC Cannot Comply’ (203h) message, for each SRID.

□ ***Transmission Completed (TXC)***

When all transmissions that can be performed for a given TSR have been completed by the SNC, a ‘Transmission Completed’ (202h) message is sent to the DLP, containing the SRID of the TSR that it refers to. The message also contains the Message Time of Validity of the First Transmission (in seconds since midnight) and the Transmission Success Percentage (0-100%). The Transmission Success Percentage provides the percent of the required networks on which the message was successfully transmitted. When there are no machine receipt addressees, this message indicates that the SNC has finished processing the TSR, and the DLP may reuse the completed TSR’s SRID in a new TSR.

□ ***Acknowledgement (ACK)***

For a TSR containing MR Addressees, the DLP will receive one or more ‘Acknowledgement’ (205h) messages indicating whether or not each MR Addressee that received the message was able to pass it to its DLP, or that no response was received by the time the protocol timed out. The acknowledgement message also indicates if it is the last message or not. The transmission is not complete until the DLP receives both the ‘Transmission Completed’ (202h) message and the last

‘Acknowledgement’ (205h) message. These two messages can be received in any order. After the protocol is complete the DLP may reuse the SRID.

Following a timeout of transmission, or a transmission that was not acknowledged by all required addressees, the DLP may choose to retransmit the data.

3C.1.2 Transmission Request Cancellation

The ‘Cancel Service Request’ (103h) message is sent to the SNC whenever an existing Transmission Service Request is to be cancelled. The SNC cancels all transactions related to this SRID and returns a ‘Confirm Cancellation’ (204h) message, as shown in [Figure 3C.1-3](#). Prior to the receipt of a ‘Confirm Cancellation’ (204h) message, the DLP must **NOT** re-use the SRID. Following the receipt of a ‘Confirm Cancellation’ (204h) message, the DLP can re-use the SRID.

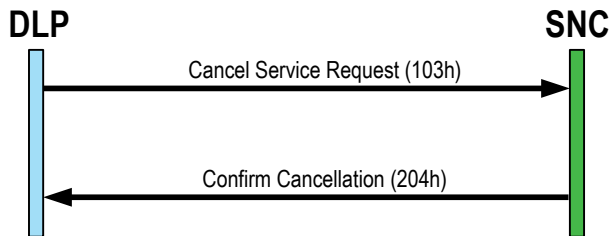


Figure 3C.1-3 Cancellation of a Transmission Service Request

Even though the TSR is cancelled, the actual Tactical Message may still be transmitted, as some transmissions may have already been made when the cancel message is received by the SNC. Also, if the Tactical Message was already packed into a message packet with other tactical messages, the transmission of the message packet cannot be cancelled unless all messages in the packet are cancelled.

If the SNC has completed the transmission of the tactical message but the DLP has not yet received the final message in the TSR protocol at the time it sends the cancellation, the SNC will reply with a ‘SNC Cannot Comply’ (203h) message.

3C.1.3 Transmission Priority Management

The DLP has the option to request a change of priority and eligibility for a priority injection for an existing Transmission Service Request, by sending the ‘Priority Change Request’ (106h) message to the SNC. There is no response to this request as shown in [Figure 3C.1-4](#). The SNC modifies the priority of the specified Transmission Service Request.

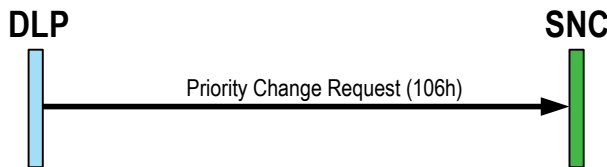


Figure 3C.1-4 Priority Change of a Transmission Service Request

If the SNC has completed the transmission of the tactical message but the DLP has not yet received the final message in the TSR protocol at the time it sends the priority change, the SNC will reply with a ‘SNC Cannot Comply’ (203h) message.

3C.1.4 Reception

There are two versions of Tactical Message Reception Protocol.

- **Explicit Flow Control Protocol** (the default)
- **Optimized Receive Protocol**, which is enabled by setting the ‘Optimized Receive Protocol’ flag in the ‘MPT Specification’ (301h) message during initialization

□ **Explicit Flow Control Protocol**

This protocol was introduced to support legacy old Host/DLP systems where flow of messages needed to be controlled. When the SNC has received Tactical Messages from another NU, it notifies the DLP that data is available by sending a ‘Tactical Messages Available’ (206h) message. The DLP indicates to the SNC that it is prepared to receive the messages by sending a ‘Ready to Receive’ (107h) message. The SNC transmits the Tactical Messages to the DLP in a ‘Received Tactical Messages’ (207h) message. This protocol is shown in the [Figure 3C.1-5](#).

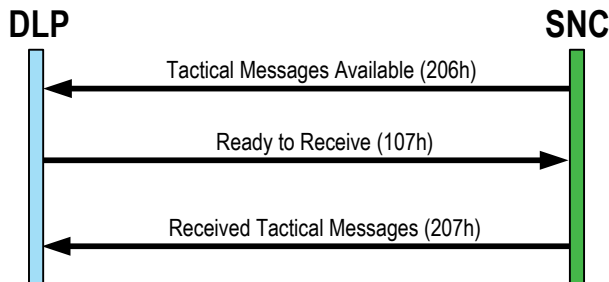


Figure 3C.1-5 Explicit Flow Control for Incoming Tactical Messages

□ **Optimized Receive Protocol**

Optimized receive protocol is the default method for a modern Host/DLP system. The flow control messages are optional, and also flow control is implicit in the TCP protocol. A more optimized interface therefore is possible with the SNC sending the received Tactical Messages to the DLP without the flow control (i.e. just using the ‘Received Tactical Messages’ (207h) message).

3C.2 DLP TSR Management

The DLP needs to provide a mechanism to retain information relating to the “current” TSRs, which are those that have been sent to the SNC, but have not yet completed the transmission protocol. The list of information about the current TSRs is referred to as the “TSR Queue”. As a minimum, the TSR attributes must be retained. The SRID attribute is particularly important as it is what is used to identify the service request, and all of the tactical interface messages exchanged between the DLP and SNC during the transmission protocol use the SRID as the unique identifier. The Priority attribute can be used to sort the TSRs based on urgency of transmission.

The DLP should know the current state of all outstanding TSRs. A TSR can be in one of several states between issue and completion, and the DLP uses the state to determine whether a particular event is valid, and what action must be performed for each event.

TSRs have two types of addressees, Non-Machine Receipt (Non-MR) and Machine Receipt (MR), which affect which states a TSR can have. If a TSR contains both Non-MR and MR addressees, it is processed through the MR states. The following protocols are explained.

- Non-MR Addressee Only TSRs
- MR Addressee TSRs
- Transmission Timeout
- SRID Management Function

Figure 3C.2-1 lists the DLP-SNC Interface message abbreviations used in the State Transition Diagram figures.

Abr.	DLP-to-SNC Messages	Abr.	SNC-to-DLP Messages
CSR	Cancel Service Request	CC	Confirm Cancellation
PCR	Priority Change Request	MPR	Message Preparation Request
PRR	Preparation Request Response	SCC	SNC Cannot Comply
TSR	Transmission Service Request	TXC	Transmission Completed

Figure 3C.2-1 DLP-SNC Interface Message Abbreviations

3C.2.1 Non-MR Addressee Only TSRs

Figure 3C.2-2 lists the Non-MR Addressee only TSR states. Figure 3C.2-3 shows the State Transition Diagram for Non-MR TSRs, both with and without data. States are shown as boxes, and transitions between states are indicated by arrows, labeled with two lines of text. The top line of text is the event within the DLP, or the message received from the SNC, that causes the transition. The bottom line of text is the action taken by the DLP in response to the event, which may include sending a message to the SNC.

State	Definition
Idle	This is not a TSR State. However, it allows the State Transition Diagram to show the TSR Creation and Deletion events
Waiting for Initial MPR	Awaiting the first Message Preparation Request message for this TSR from the SNC
Tx In Progress	Transmission of tactical message on Link 22 is deemed to be in progress. Awaiting a Transmission Completed message from the SNC
Waiting for CC	Awaiting a Confirm Cancellation message from the SNC to signify cancellation of the TSR

Figure 3C.2-2 Non-MR Addressee Only TSR States

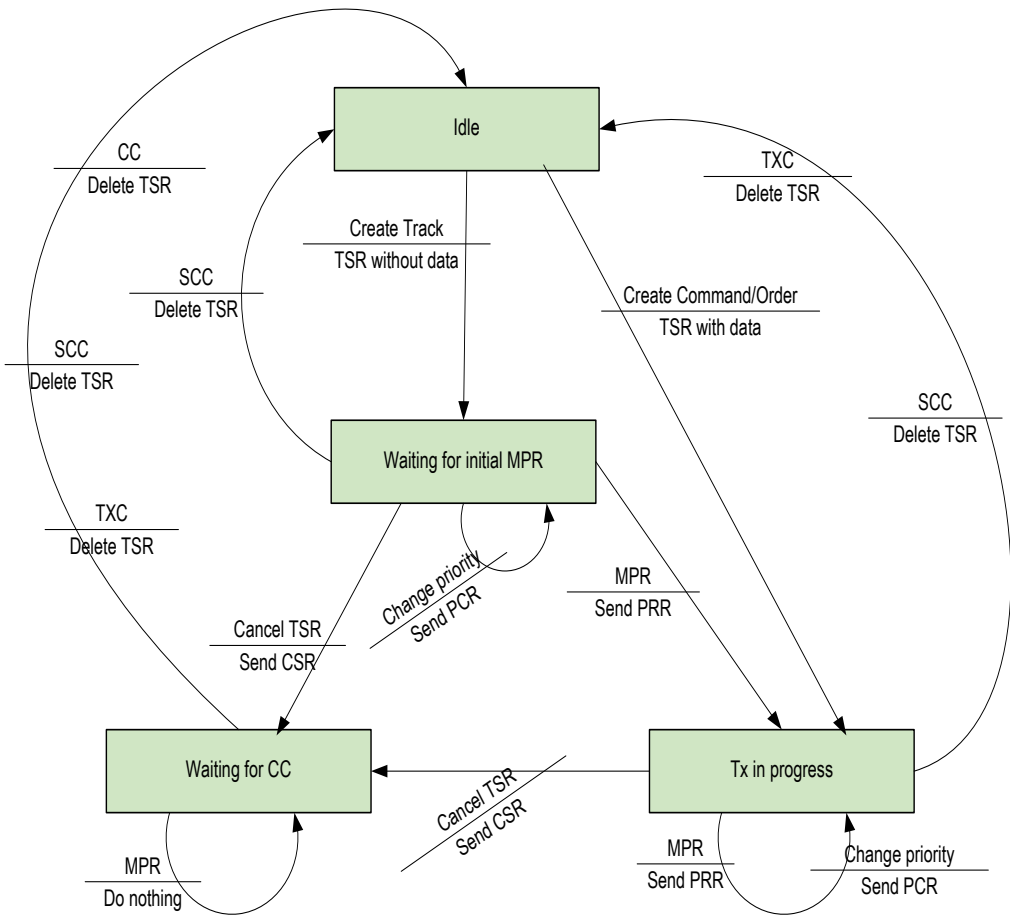


Figure 3C.2-3 Non-MR Addressee Only TSR State Transition Diagram

The main points to note in the Non-MR Addressee Only TSR State Transition Diagram are as follows.

- The State Transition Diagram starts in the Idle state when the transmission starts
- A TSR “without data” is added to the TSR Queue at creation with a state of “Waiting for Initial MPR”
- A TSR “with data” is added to the TSR Queue at creation with a state of “Tx In Progress”
- The state transition from “Waiting for Initial MPR” to “Tx In Progress” is triggered by the reception of an MPR message and generation of a Preparation Request Response message
- Once the DLP has issued a Cancel Service Request to cancel a TSR, no changes can be made to the Priority/Priority Injection Indicator attributes, and a further MPR for this TSR is ignored. The MPR is not expected but may be received due to the asynchronous nature of the DLP-SNC interface
- Receipt of the Transmission Completed message completes the transmission protocol for this TSR and so it is deleted from the TSR Queue
- Receipt of an SNC Cannot Comply message in any state signifies SNC termination of the transmission protocol for this TSR, so it is deleted from the TSR Queue
- When in “Waiting for CC” state, receipt of a Transmission Completed message from the SNC is valid if it was being waited for when the DLP cancelled the TSR. This circumstance can occur due to the asynchronous nature of the DLP-SNC interface, which allows for the possibility of the SNC issuing the Transmission Completed message at the same time as the DLP issuing the Cancel Service Request message. Therefore, receipt of this message or the expected Confirm Cancellation message signifies that the transmission protocol is complete for this TSR, so it is deleted from the TSR Queue

3C.2.2 MR Addressee TSRs

Figure 3C.2-4 lists the MR Addressee TSR states.

State	Definition
Idle	This is not a TSR State. However, it allows the State Transition Diagram to show the TSR Creation and Deletion events
Waiting for Initial MPR	Awaiting the first Message Preparation Request message for this TSR from the SNC
MR/GD Tx In Progress	Transmission of tactical message on Link 22 is deemed to be in progress. Awaiting a Transmission Completed message and one or more Acknowledgement messages from the SNC
Waiting for Final ACK	Transmission Completed message has been received, but still waiting for an Acknowledgement message that indicates No Further Acknowledgements
Waiting for TXC	Acknowledgement message that indicates No Further Acknowledgements has been received, but still waiting for a Transmission Completed message
Waiting for Protocol Completion after Cancel	A Cancel Service Request has been issued. Awaiting SNC response
Waiting for CC/Final ACK after Cancel	Awaiting a Confirm Cancellation message or an Acknowledgement message that indicates No Further Acknowledgements, to complete the Cancellation protocol
Waiting for CC/TXC after Cancel	Awaiting a Confirm Cancellation message or a Transmission Completed message to complete the Cancellation protocol

Figure 3C.2-4 MR Addressee TSR States

Figure 3C.2-5 shows the State Transition Diagram for MR Addressee TSRs.

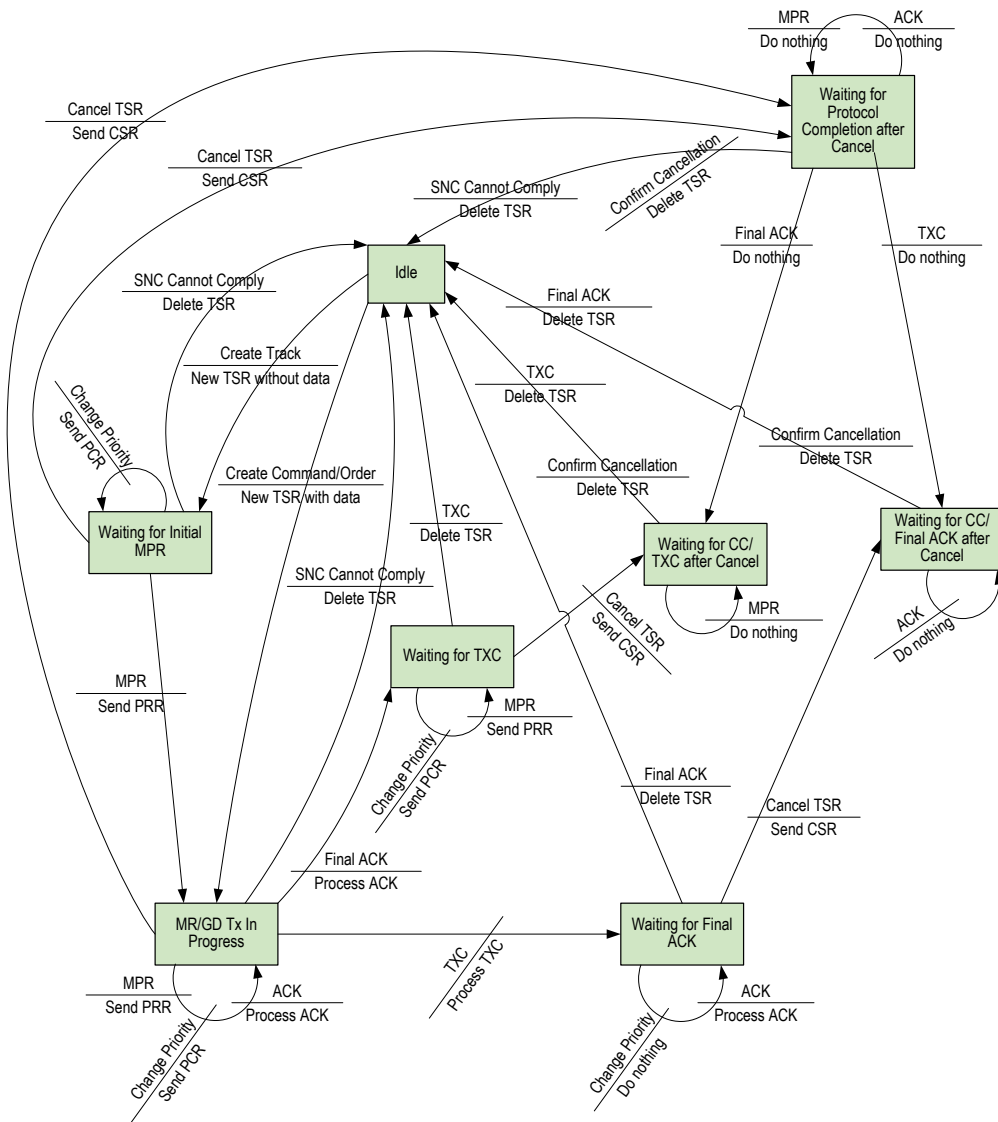


Figure 3C.2-5 MR Addressee TSR State Transition Diagram

The main points to note in [Figure 3C.2-5](#) are as follows.

- The State Transition Diagram starts in the Idle state when the transmission starts
- A TSR “without data” is added to the TSR Queue at creation with a state of “Waiting for Initial MPR”
- A TSR “with data” is added to the TSR Queue at creation with a state of “MR/GD Tx In Progress”
- The state transition from “Waiting for Initial MPR” to “MR/GD Tx In Progress” is triggered by the reception of an MPR message and generation of a ‘Preparation Request Response’ (105h) message
- The TSR transmission protocol is completed once the DLP has received both a ‘Transmission Completed’ (202h) message and an ‘Acknowledgement’ (205h) message with the No Further Acknowledgements flag set. The messages can be received in either order, hence the two states that can be entered from “MR/GD Tx In Progress” which are “Waiting for TXC” and “Waiting for Final ACK”. These states are entered when one of the messages is received and the DLP is still waiting for the other one. Once the second message arrives, the TSR is deleted from the TSR Queue, as the protocol is now complete
- Once the DLP has issued a Cancel Service Request to cancel a TSR, no changes can be made to the Priority/Priority Injection Indicator attributes, and a further MPR for this TSR is ignored. The MPR is not expected but may be received due to the asynchronous nature of the DLP-SNC interface
- Receipt of an ‘SNC Cannot Comply’ (203h) message in response to a DLP message signifies SNC termination of the transmission protocol for this TSR, so it is deleted from the TSR Queue
- When the DLP cancels the TSR, the state that is entered depends on where the DLP is in the transmission protocol. If the DLP is currently waiting for the ‘Transmission Completed’ (202h) message, the ‘Acknowledgement’ (205h) message with the No Further Acknowledgements flag set, or both, the state that is entered is one where either the ‘Confirm Cancellation’ (204h) message or one of these original messages is expected. This is due to the asynchronous nature of the DLP-SNC interface, which allows for the possibility of the SNC issuing the ‘Transmission Completed’ (202h) or ‘Acknowledgement’ (205h) messages at the same time as the DLP issuing the ‘Cancel Service Request’ (103h) message. Therefore, this TSR transmission protocol can be completed by the normal protocol messages, or by the Confirm Cancellation mechanism, and so the TSR is deleted from the TSR Queue

3C.2.3 *Transmission Timeout*

Under normal circumstances, TSRs are deleted from the TSR Queue when their transmissions have been completed, or when the DLP or SNC determine that the TSR requires early termination. However, there is always the possibility that TSRs could remain permanently in the TSR Queue, if for instance the SNC cannot transmit them due to connectivity or congestion problems, or there are physical problems with the DLP-SNC or SNC-to-LLC interfaces. Therefore, the DLP may want to provide a transmission timeout housekeeping function to process the expired TSRs. As it is not essential to remove the expired TSRs, the decision to do so is an implementation issue.

If expired TSRs are not removed in the DLP, they will remain in DLP memory indefinitely, which could cause the DLP to eventually run out of memory. If TSRs remain in the SNC TSR Queue, the queue could fill up so that no more TSRs could be accepted by the SNC.

If the DLP does implement a transmission timeout function, the following issues need to be addressed.

- [TSR Lifetime](#)
- [TSR Expiration](#)
- [Expired TSR Resolution](#)

□ ***TSR Lifetime***

A transmission timeout function requires that every TSR has a defined lifetime. TSRs have varying lifetimes dependent on such things as the type of tactical message to be transmitted, and the transmission requirements such as MR/Non-MR protocols, reliability, priority, and perishability. [STANAG 5522] does not explicitly state TSR lifetimes, but provides all of the necessary data to allow the DLP to apply an algorithm to calculate unique TSR lifetimes for each tactical message type. The impact of channel utilization and congestion on TSR transmission times must also be considered by the DLP.

However, the DLP could apply a simpler algorithm giving all TSRs the same lifetime based on the known transmission constraints plus an additional buffer margin. As an example, a value of 10 or 15 minutes could be used. This value is derived from the following known constraints.

- There is a variable length of time between the DLP sending a TSR to the SNC, and the SNC requesting the tactical message via an MPR. Allowing for the maximum length NCT of approximately 2 minutes (for HF) and assuming one timeslot per NCT, then if a TSR was created just after the timeslot, it would be nearly 2 minutes before the SNC requests the data
- An MR or GD transmission protocol will terminate 4 minutes after the initial transmission if it is not completed normally within this time period

□ ***TSR Expiration***

TSRs could be allocated a lifetime value on entry to the TSR Queue (at TSR creation time). The DLP would monitor this time to determine when a TSR had expired. This could be done on an individual TSR-by-TSR basis, or by performing a regular sweep of the entire queue. The monitoring of individual TSRs requires the use of TSR timers that are activated when a TSR has spent its lifetime in the TSR Queue. The regular sweep would use a single timer to trigger a sweep every few minutes to detect the TSRs that have expired since the last sweep.

□ ***Expired TSR Resolution***

The DLP could attempt to resolve the issue of an expired TSR in the following ways.

- By increasing the TSR priority to the next level to attempt to force a transmission (as per the “lateness” rules in [STANAG 5522]). The DLP issues a ‘Priority Change Request’ (106h) message to the SNC
- By issuing a ‘Cancel Service Request’ (103h) (CSR) message to the SNC to cancel the TSR and waiting for a response before removing the TSR from the queue. Under these circumstances it would be prudent to apply an arbitrary lifetime to the CSR in case there is a DLP-SNC interface problem that has caused the TSR to expire. After the CSR has expired without response from the SNC, the DLP can remove the TSR from the queue
- By removing the TSR from the queue without notifying the SNC

These last two actions are mutually exclusive in that only one of the actions is available to the DLP in any particular TSR state. If the TSR state is one where the DLP has already sent a CSR, then it does not need to send a second CSR to the SNC and so action 3 would be the available option.

Figure 3C.2-6 shows which actions are available to the DLP in each TSR State.

Non-MR State	Increase to TSR Priority	Cancel TSR & Delete	Delete TSR (No Cancel)
Waiting for Initial MPR	Yes	Yes	No
Tx In Progress	Yes	Yes	No
Waiting for CC	No	No	Yes

MR State	Increase to TSR Priority	Cancel TSR & Delete	Delete TSR (No Cancel)
Waiting for Initial MPR	Yes	Yes	No
MR/GD Tx In Progress	Yes	Yes	No
Waiting for Final ACK	No	Yes	No
Waiting for TXC	Yes	Yes	No
Waiting for Protocol Completion after Cancel	No	No	Yes
Waiting for CC/Final ACK after Cancel	No	No	Yes
Waiting for CC/TXC after Cancel	No	No	Yes

Figure 3C.2-6 Actions available to DLP on TSR Transmission Timeout

3C.2.4 SRID Management Function

The DLP is responsible for managing the SRID usage. There are 4095 SRIDs (1-4095) that can be allocated to TSRs by the DLP. A new TSR requires that a free SRID is allocated to it, and the SRID remains allocated to the TSR until the TSR is deleted, at which time the SRID becomes available for re-allocation. The DLP should know whether an SRID is in use or not (allocated to a TSR or not) and needs to be able to quickly identify the next free SRID for allocation to a new TSR.

3C.3 SNC TSR Queue

The SNC receives TSRs from both the DLP (tactical) and internally from other parts of the SNC (technical). The SNC stores and manipulates all the TSRs in a data structure referred to as the TSR Queue.

This section contains the following sub-sections.

- External TSR Queue View
- Internal TSR Queue Structure
- TSR Queue Operations

3C.3.1 External TSR Queue View

From an external view point (DLP), the TSR Queue is a queue of TSRs in priority and time order where time is the time when the DLP issues the TSR.

Each TSR for a tactical message has a priority and a Priority Injection Indicator (PII). The priority is a value from 1 to 4 with 1 being the highest and 4 the lowest. The PII is only set for priority 1 messages, and when set indicates that it is an important message which is eligible for early transmission in a Priority Injection slot, if there is one available. When the PII is set, the TSR is put at the bottom of any other PII TSRs which is at the top of the TSR Queue for Priority 1, whereas if it is not set then the TSR is placed at the bottom of the queue for its specified priority. The red arrows in [Figure 3C.3-1](#) show where the TSR is inserted into the TSR Queue, depending on the priority, and whether the Priority Injection Indicator is set.

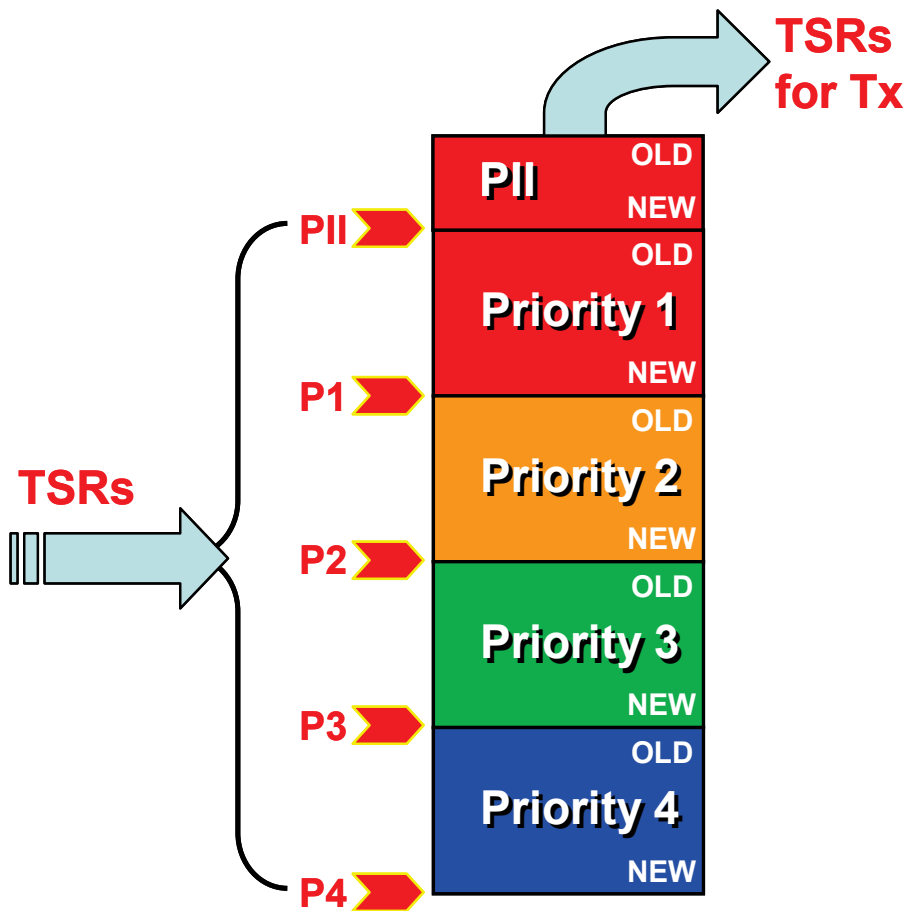


Figure 3C.3-1 SNC TSR Queue

The SNC selects TSRs for transmission in the next timeslot according to their priority, age and the space available in the timeslot. The oldest Highest Priority TSR is selected first, followed by the next oldest Highest Priority TSR that can fit in the remaining space within the timeslot. Low Priority messages might not be transmitted during times of high traffic load. The DLP has the capability to change the priority of messages, for example, when a TSR is not meeting the required update rate for the track, its priority can be increased.

3C.3.2 Internal TSR Queue Structure

The TSR Queue consists of the three following major components, as shown in Figure 3C.3-2.

- SRID Index
- TSR Information
- Message Data

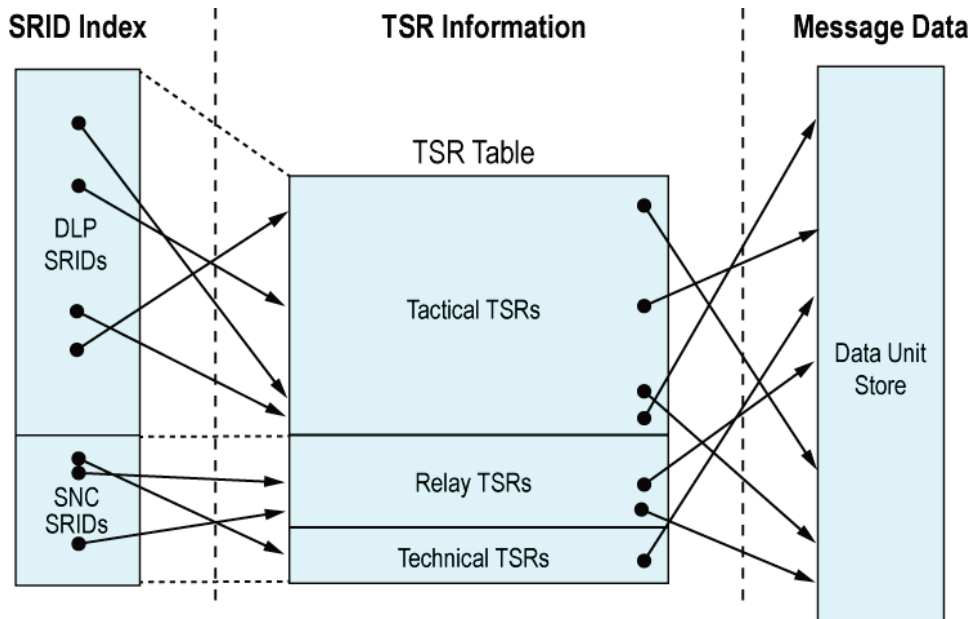


Figure 3C.3-2 SNC TSR Queue Major Components

□ ***SRID Index***

The SRID Index points to the record in the TSR Table that contains the TSR with the SRID number. The SRID Index consists of two regions as described below.

- DLP SRIDs
 - Available for use by the DLP (1-4095)
 - Only point to the Tactical TSR Table part
- SNC SRIDs
 - Used internally by the SNC (4096-5776) for both Relay and technical TSRs
 - Only point to the Relay or Technical TSR Table parts

There are more SRIDs available to the DLP than there are entries in the TSR Table for the DLP requests. There is the same number of SNC SRIDs as the sum of the Relay and Technical TSR Table records, but there is no 1-to-1 relationship. The SNC dynamically maps an SRID to the appropriate TSR Table record number depending on the type of TSR. This is important because if the TSR is cancelled, the SRID may be reused after it has received the ‘Confirm Cancellation’ (204h) message; however, the TSR Table record may still be in use until the transmission protocol completes. If the SRID is reused the SNC will map it to a different free TSR Table record. This means that there can be TSR Table records in use that are no longer mapped to any SRID.

□ ***TSR Information***

The TSR Information is stored within the TSR Table, which consists of an array of records where each record represents a single TSR. This table is divided into the three parts below.

- Tactical TSRs from the DLP
- Relay TSRs generated by the SNC (used to retransmit received Message Packets (MPs))
- Technical TSRs for the requests to transmit technical messages from the SNC

There is a separate chain of unused records for each of the three parts, which allows the allocation of a record from the correct part depending on the type of TSR. Each record contains the information listed below.

- Original TSR requested attributes
- Indexes
 - Pointer to SRID Index
 - Pointers to other TSR Table records
 - Pointer to Data Unit Store records
- Current status of the TSR
- Routing information
- MP protocol data

The MP protocol data links together up to three TSRs when they are combined into an MP. Pointers within each record form the priority queue (a double linked list) by pointing to the previous and next records in the queue. There are also external pointers to the top and bottom of each priority queue and to the top of each free chain.

□ **Message Data**

The Message Data is stored within a separate table called the Data Unit (DU) Store. Each record can contain the maximum size message. There may be multiple records for the same TSR, as the data can change with time. The TSR Table record points to the newest entry in the DU Store. The DU Store record points to the previous entry if there was one. These pointers form a chain in descending Message Time of Validity (MTV) order of the Data Units associated with the TSR. One reason for this is that a single MP may have repeat transmissions in different timeslots, and therefore require data for different MTVs. All the unused records are linked together in a free chain and there is an external pointer to the top of the free chain.

Additional details of all the components of the TSR Queue can be found in the SNC System Design Document [[SNC SDD](#)].

3C.3.3 TSR Queue Operations

The TSR Queue is a major data structure that is constantly accessed and updated. The major operations of the TSR Queue are the following.

- TSR Creation
- MP Creation
- Change Priority
- Update Data
- Cancel
- Deletion

□ **TSR Creation**

To create an entry in the TSR Queue, a TSR Table record is removed from the free queue of records corresponding to the TSR type. The record number is inserted into the SRID Index for the TSR's SRID. The fields from the TSR are then copied into the TSR Table record with Link 22 addresses being converted to NILE Unit addresses, when required. The Time of Request of the TSR is also recorded in the TSR Table record using the current time. If the TSR includes data a DU Store record is removed from the free queue, the data is stored in the record, and the DU Store record number is stored in the TSR Table record.

□ **MP Creation**

Prior to a transmission, a TSR is formed into an MP which updates the MP protocol data in the TSR Table record. The MP may contain one or two additional TSRs. When an MP is created, the TSRs in the MP are linked together using the pointers in the MP protocol data. One of the TSRs is designated as the master by setting the Master TSR Table record number to be itself. A pointer to the 2nd TSR is set to the record number of the 2nd TSR, if there is one. Similarly if there is a 3rd TSR, the pointer in the master to the 3rd TSR is set to the 3rd TSR Table record number. The additional TSRs are unlinked from the priority queue chain, leaving only the master TSR in the chain. All information related to the transmission of the MP is only stored in the master TSR. The Master TSR Table record number in the 2nd and 3rd TSRs (when existing) is set to the TSR Table record number of the master TSR.

Figure 3C.3-3 shows a simple example of a TSR queue with MPs. There is one priority 1 TSR, two priority 2 TSRs, three priority 3 TSRs, and one priority 4 TSR (linked in order by the red arrows). All the TSRs have been packed into MPs (green

arrows) except for the priority 4 TSR. The three priority 3 TSRs have been packed into a single MP, so the second and third TSRs in the MP are no longer linked in the TSR queue. Each TSR points to its Data Unit (grey arrow). The second priority 2 TSR has had one update to its DU. The priority 4 TSR has had two updates to its DU.

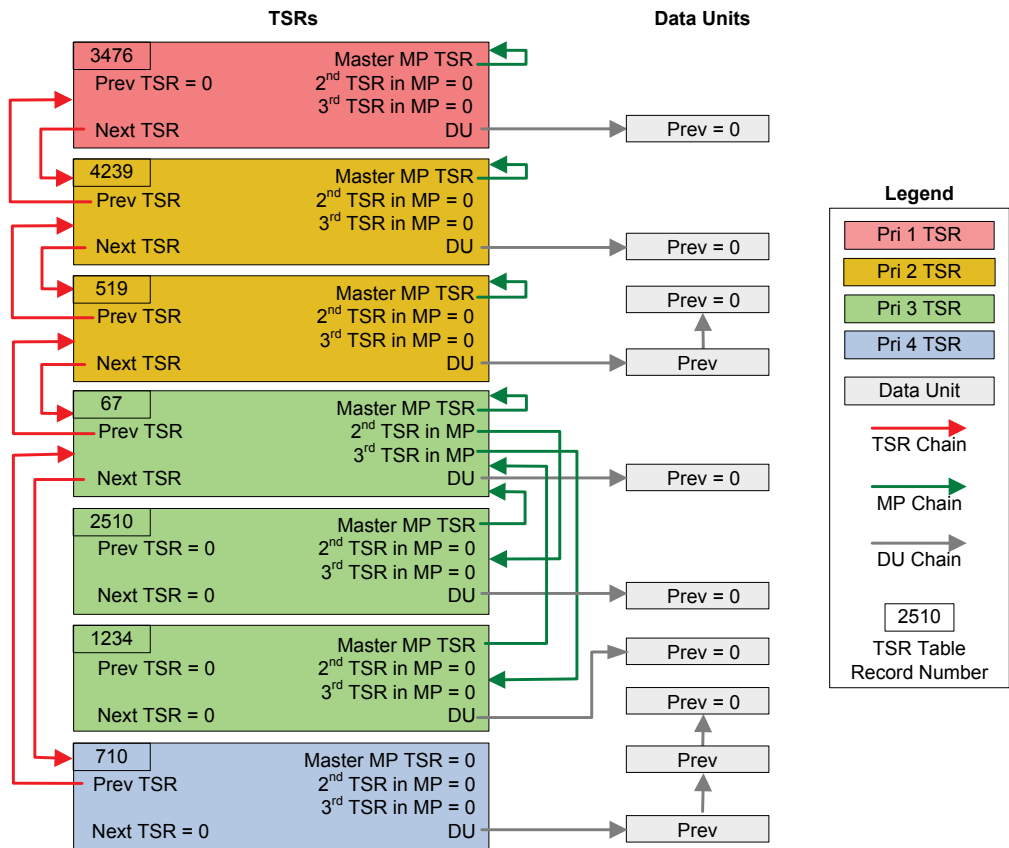


Figure 3C.3-3 TSR Queue with MPs

□ Change Priority

When the DLP changes the priority of a TSR or changes the setting of the PII, the SNC updates the TSR Table record to reflect the new priority and Priority Injection indicator. If the initial transmission of the TSR has not been performed (the MP has not been created), a new route prediction is performed. If the MP has been created,

then the MP protocol priority is also updated to be the highest priority of all the contained TSRs, taking into account the new TSR priority. This means that if an MP contains more than one TSR and only one is changed then this may affect the whole MP priority and may effectively change the priority of the other TSRs. The other TSRs in the MP do not have their priorities adjusted in the TSR Queue. The TSR or Master TSR of an MP is removed from the priority queue and inserted back into the priority queue at the appropriate position.

□ *Update Data*

When the DLP or SNC provides data for a TSR, a DU Store record is removed from the free queue and the data is stored in the record. If the data is the first data received, the TSR Table record is updated to point to the DU Store record. If it is not the first data then the DU Store record has to be inserted in the chain so that the TSR Table record points to DU Store record with the latest Message Time of Validity (MTV), and the DU Store records are linked in MTV order.

□ *Cancel*

When the DLP or the SNC cancels a TSR, the action that follows will depend on whether or not the TSR has been packed into an MP. If the TSR is not in an MP, then it can safely be deleted (the Deletion operation is then performed). However, when the TSR has been packed into an MP, this operation only marks the TSR as cancelled. The TSRs will not be deleted until all the TSRs within the MP have been cancelled or transmission processing is complete.

□ *Deletion*

When a TSR completes processing it is deleted. First all DU Store records are reset and returned to the DU Store free queue, and then the SRID Index entry is reset. The TSR Table record is removed from the priority queue if it is still in it, and then the record is cleared of all information. Deletion of an MP is achieved by performing the deletion of each TSR in the MP.

3C.4 SNC Transmission/Reception

Link 22 uses Time Division Multiple Access (TDMA) on all of its networks. TDMA means that the time is divided among the network members, and that they can only transmit in the time that is allocated to them. An Operational Network Cycle Structure (ONCS) defines when each unit is allowed to transmit (see section [3C.7 Network Cycle Structure Handling](#)). Each SNC transmits and attempts to receive based on its internal knowledge of the ONCS.

The individual unit of data that the SNC sends to the LLC for transmission, and receives from the LLC on reception, is a Network Packet (NP). The SNC controls the timing of the transmissions and receptions based on the ONCS. The messages exchanged between the SNC and the SPC, through the LLC for transmission and reception, are detailed in Sections [3C.13 SNC-to-LLC Protocols](#) and [3C.14 LLC-to-SPC Protocols](#).

This section covers the SNC-SNC communication chain, which consists of the transmission preparation, encryption, transmission, reception scheduling, reception and decryption of NPs. As the encryption and decryption are just the opposite of one another, they are described in the same sub-section.

This section consists of the following sub-sections.

- [Transmission](#)
- [Reception](#)
- [Encryption / Decryption](#)

3C.4.1 *Transmission*

When the DLP requests transmission of a message with time dependent data, such as the location of a track, the DLP does not know exactly when the SNC will transmit it, so it does not provide the actual data to be transmitted in the request. When the SNC is preparing the NPs for the timeslot that will contain the DLP's message, it asks the DLP to provide the data for the time of the timeslot. The DLP extrapolates the track position to the specified time and then provides the data to the SNC for transmission.

The time for which a message in the NP is prepared is called the Message Time of Validity (MTV). MTV is defined to be the transmission time of the beginning of the timeslot, an integer number of seconds since midnight. If the message is older than the timeslot time, then an age field is used to indicate how much older the message is. This age field is required to satisfy Link 22's requirement that the time used for preparation of the tactical data is always known.

Transmissions have to occur at specified times as defined by the ONCS. The SNC controls all the events leading up to the transmission, and the SPC controls exactly when the transmission is made. The SNC has to get the tactical data to be transmitted from the DLP, allowing the DLP time to respond. This occurs before the SNC packs the NPs and sends them to the LLC for encryption and delivery to the SPC for transmission via the radio. The SNC controls the event timings to minimize the time it takes from requesting the data to the start of the timeslot. [Figure 3C.4-1](#) shows the events in time sequence and the time intervals (not to scale) between consecutive events.

The SNC has to ensure the events are scheduled so that there is enough time to perform the operations that are specified for each interval as follows.

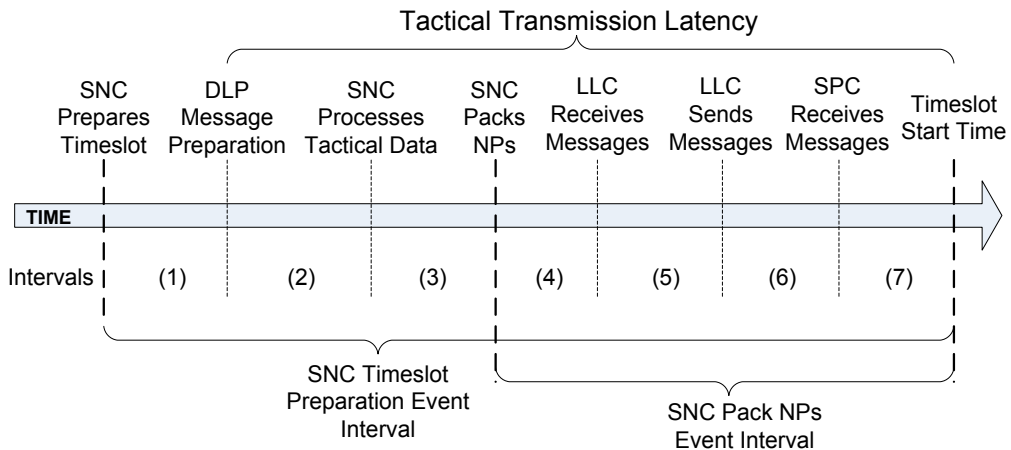


Figure 3C.4-1 Transmission Timing

□ **Interval (1)**

This interval represents the time taken by the SNC to determine which TSRs should be packed into the timeslot. The TSR queue is scanned and a packing scheme is generated, and the SNC calculates routing information, where needed. As a result, the SNC generates and sends 'Message Preparation Request' (201h) messages to the DLP, for the tactical TSRs without data. The interval also includes the time taken by TCP to deliver the messages to the DLP. This interval is relatively small (in the order of 5 ms).

□ **Interval (2)**

During initialization, the DLP tells the SNC its Message Preparation Times (MPTs) in the 'MPT Specification' (301h) message. MPT defines the amount of time the DLP requires to provide the tactical data when requested by the SNC.

The SNC computes this time interval based on the MPT values provided by the DLP and the number of TMWs that can fit in the timeslot. The interval also takes into account the time taken by TCP to deliver the messages to the SNC. This is the major interval affecting the Tactical Latency (see [Figure 3C.4-1](#)), which is the length of time in the future for which the DLP has to extrapolate the tactical data.

In order to minimize the Tactical Latency, the DLP should specify the smallest possible Message Preparation Times.

The DLP should try to ensure that the MPT times are large enough so that it can supply the tactical data within the time it specifies. The maximum value that the DLP can supply for the largest possible timeslot is one second. If the DLP does not supply the data in time, the message will not be transmitted. This may waste some bandwidth if the SNC has no other data available to transmit.

If there are multiple networks in use and the unit has transmission slots that overlap, more time is allowed for the DLP to provide the data, and the SNC adjusts the timing of the additional networks to compensate. It does this by ensuring the times do not overlap others.

□ **Interval (3)**

The SNC takes the tactical data supplied by the DLP and stores it in the TSR queue in a chain of data for a specific MTV (see section [3C.3 SNC TSR Queue](#)). This is not significant processing and only takes microseconds. This interval also takes into account delays in scheduling the tasks, completing previous tasks and other timing inaccuracies. The SNC uses a value in the order of 50 milliseconds for the sum of Interval (1) and Interval (3).

□ **Interval (4)**

The SNC recalculates how to pack the timeslot, using only those TSRs that have data available. Then the SNC performs the actual packing to produce the NPs (see section [3C.11 SNC Packing](#)). The NPs are then queued for transmission to the LLC. The interval also includes the time taken by TCP to deliver the messages to the LLC. This interval is in the order of 10 milliseconds.

□ **Interval (5)**

For those media where there is a preamble, this interval is the time taken by the LLC to process the 'SPC Transmit Header Request' (0002H) message and send the message to the SPC. For those media where there is no preamble, this interval is the time taken by the LLC to process the 'SPC Transmit Header Request' (0002H) message, to convert the first 'LLC Transmit Network Packet Request' (0303H) message into a 'SPC Transmit Network Packet Request' (0003h) message, including encryption of the data, and to send the messages to the SPC.

The SNC packs all the NPs in a timeslot at the same time. Then first it sends to the LLC the ‘SPC Transmit Header Request’ (0002H) message followed by the first ‘LLC Transmit Network Packet Request’ (0303H) message. Following the first NP, the remaining NPs are sent to the LLC, one at a time, spread through the length of the timeslot. This prevents the LLC from becoming busy encrypting NPs (its highest priority task) for a time proportional to the number of NPs in the timeslot. The LLC only has to encrypt a single NP at a time, for a transmission timeslot. When multiple networks are on the same LLC, and the transmission timeslots overlap, this ensures that the NP encryptions for one network are interleaved with those from the other networks. This ensures that this interval does not have to be increased to handle the time that the LLC is busy encrypting all the NPs for the other transmission timeslots. The time taken by the LLC to process the transmission request and the first NP is in the order of 30-50 milliseconds and 8-10 milliseconds for each subsequent NP.

□ **Interval (6)**

This interval represents the time taken for the ‘SPC Transmit Header Request’ (0002H) message and the first ‘SPC Transmit Network Packet Request’ (0003H) message to be delivered to the SPC. It incorporates delays in the LLC for the driver level software, and the serial hardware. It includes the time taken to actually transmit the message on the serial link, which is proportional to the baud rate at which the link is set. On the SPC it includes the serial port hardware delay, the driver level software, and the reception of the message processing by the SPC.

On HF FF media for a small NP, using a baud rate of 9600 baud, the transmission delay is at least 20 milliseconds. At 38,400 baud, the largest HF FF NP takes approximately 40 milliseconds. On UHF FF, the largest NP (approximately 2000 bits), using 115,200 baud takes 20 milliseconds. This interval is calculated based on the baud rate being used.

The fastest baud rate possible between the LLC and SPC should be used to minimize the serial communications delay.

In a future development of an LLC, an alternative interface that is considerably faster (such as a 100 MB Ethernet) may be an option, which if available, would need to be supported by the SPC.

□ **Interval (7)**

The major component of this interval is the SPC Processing Time, which is the time the SPC needs to complete its processing of the transmission requests from the LLC

so that it can correctly operate the radio at the timeslot time. This SPC processing time is supplied by the SPC to the SNC when the SPC status is requested, and ranges from 0 to 255 milliseconds. The SNC uses the value supplied by the SPC in its calculation of this interval.

This interval also includes additional time to handle unpredictable delays in scheduling the tasks, completing previous tasks and other timing inaccuracies.

To minimize the Tactical Latency, this interval is kept as small as possible. If the SPC reports that it has received NPs late, the SNC increases this interval.

3C.4.2 Reception

For reception, the timing is a lot simpler. The SNC just has to ensure that the ‘SPC Receive Header Request’ (0004H) message gets to the SPC before the SPC needs to process it. The SPC can queue requests in time order, so the SNC ensures that the requests are sent well in advance so that they are never late. The only constraint on sending the requests is that the SPC has a limited number of requests that it allows to be queued. [Figure 3C.4-2](#) shows the events in time sequence and the time intervals (not to scale) between events.

The SNC by default queues the Receive Timeslot Event one second before the start of the timeslot. This allows sufficient time for ‘LLC Receive Header Request’ (0404H) message to be processed by the LLC, cross the serial interface and be received by the SPC in advance of the timeslot.

The SNC parses received Network Packets from the LLC, and if the structure is incorrect or fields are out of range, they are discarded.

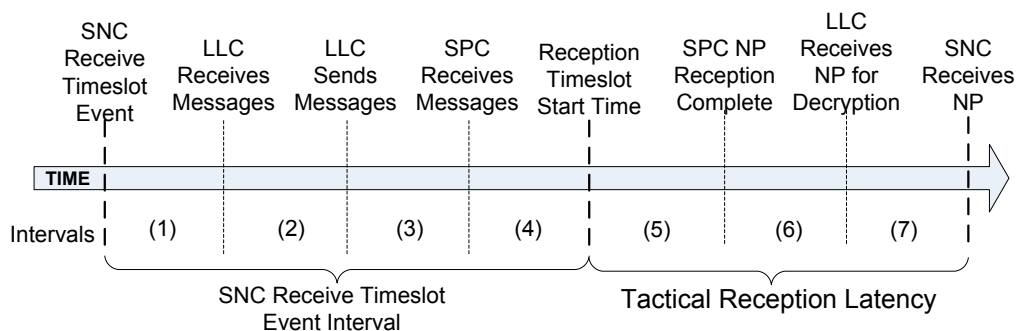


Figure 3C.4-2 Reception Timing

□ **Interval (1)**

This interval is the time taken by the SNC to send the ‘LLC Receive Header Request’ (0404H) message to the LLC, and includes the time taken by TCP to deliver the messages to the LLC. This is a very short interval in the order of 1-3 milliseconds, mainly in TCP.

□ **Interval (2)**

This interval is the time taken by the LLC to process the ‘LLC Receive Header Request’ (0404H) message, convert it to a ‘SPC Receive Header Request’ (0004H) message, and send it to the SPC through its bypass partition. Transmission requests have priority within the LLC, so it is possible for this message to be delayed within the LLC due to transmission request processing. When multiple networks are on the same LLC, and the transmission timeslots are at the same time, this delay is cumulative. However, the one second value is sufficient to handle this delay.

□ **Interval (3)**

This interval is the time taken for the ‘SPC Receive Header Request’ (0004H) message to be delivered to the SPC. It incorporates the same delays as the transmission [Interval \(6\)](#) delays in section 3C.4.1. The request that is sent to the SPC is approximately 20 bytes, so the delay on the wire can be calculated knowing the baud rate used. Adding interface overheads, this interval should be in the order of 10 milliseconds.

□ **Interval (4)**

The major component of this interval is the SPC Processing Time, which is the time the SPC needs to complete its processing of the reception requests from the LLC so that it can correctly set the radio to receive at the timeslot time. As for transmission [Interval \(7\)](#) in section 3C.4.1, the SNC uses the SPC processing time (0-255 milliseconds) reported by the SPC, in its calculation of this interval, and includes additional time to handle unpredictable delays in scheduling the tasks, completing previous tasks and other timing inaccuracies. This ensures the SPC receives the message in time.

□ **Interval (5)**

This interval is initially affected by the propagation delay, which varies depending on the distance from the transmitting unit (a distance of 300 nautical miles line-of-sight

takes approximately 1.8 milliseconds). For media that have a preamble, this interval then includes the time required for the preamble to be received by the radio and detected by the SPC. The major time affecting this interval is the time during which the NP is received by the SPC from the radio (one or more Media Coding Frames depending on the media parameters), the processing time that the SPC takes to decode and error correct the NP, and the time required for the SPC to send a 'SPC Receive Network Packet Response' (00F3H) message to the LLC for decryption. The time taken by the SPC to process a NP is in the order of 50-120 milliseconds, but varies across different SPCs and depends on the media parameters that are being used.

□ **Interval (6)**

This interval represents the time taken for the 'SPC Receive Network Packet Response' (00F3H) message to be delivered from the SPC to the LLC. This is the same as the transmission [Interval \(6\)](#) in section 3C.4.1 above, and is proportional to the baud rate and the NP size. The baud rate must be fast enough to ensure that the NP has been transferred across the interface before the next NP is ready; otherwise the interface could not handle the network traffic.

□ **Interval (7)**

Decryption has a lower priority than encryption, so the time taken to decrypt may be delayed by the encryption of a number of timeslots. This delay is greater when there are transmissions on more than one network at the same time on the same LLC.

This interval represents the time taken by the LLC to process the 'SPC Receive Network Packet Response' (00F3H), decrypt the NP data, and produce and send to the SNC a 'LLC Receive Network Packet Response' (F5F3H) message. The interval also takes into account the time taken by TCP to deliver the messages to the SNC. The time taken when not delayed by transmissions is in the order of 8-10 milliseconds.

On reception of a 'LLC Receive Network Packet Response' (F5F3H) message, the SNC unpacks the NP and sends received tactical messages to its DLP. Received technical messages are handled within the SNC.

3C.4.3 Encryption / Decryption

Transmissions are encrypted and receptions decrypted by the LLC, using the following data as input to the cryptographic algorithm.

- 9-bit project specific code
- 7-bit NILE Address

- Encryption - Transmitting SNC's NILE Address, except for an Inactive Join LNE unit transmitting in the LNE slot (see section [3B.8.3 LNE Slot](#))
- Decryption
 - ◆ Explicit Source Identification in the received message, if available
 - ◆ Value supplied by the receiving SNC (as indicated in the ONCS), if Explicit Source Identification is not available
- NILE Network number
- Timeslot Number
 - Number of Media Coding Frames since midnight
 - Day of Week
- Crypto Key
- LLC Integrity (used prior to encryption, and after decryption)

If any of the data used during decryption does not match that used during encryption, including the LLC Integrity setting, the decryption will produce seemingly random data. Explicit Source Identification, when used, allows for correct decryption even if the receiving NU expected a different transmitting NU. The LLC informs the SNC of the NILE Address it used in the decryption.

Prior to encryption, if LLC Integrity is enabled, the LLC calculates a two byte checksum and adds the checksum to the end of the data. If LLC Integrity is disabled, no extra bytes are included.

After decryption, if LLC Integrity is enabled, the receiving LLC calculates the checksum of the received data (excluding the final two checksum bytes). If the calculated checksum does not match the received checksum, the LLC discards the data and informs the SNC that data was received but discarded due to a failed integrity.

3C.5 Addressing

This section describes the different types of addressing available in Link 22. The addressing applies to both Machine Receipt (MR) and Non-MR, which can be used separately or in combination. The SNC attempts to minimize both the number of transmissions in each network and the service associated with each transmission. As detailed in [3C.10 Message Delivery & Reliability](#), the following addressing types are defined.

- **Neighborcast:** All RF neighbors in all networks
- **Point-to-Point (P2P):** A single destination address
- **Dynamic List:** A list of 2 to 5 individual addressees
- **MASN:** A Group of addressees, using a short address (0 to 31)
- **Totalcast:** All NUs in the SN

Each of these addressing types is described in the following sub sections.

Addressing is the ability to specify which destinations the message should be delivered to, and is part of the Quality of Service specified in a transmission request. Depending on the required Service Header, as detailed in [3C.11 SNC Packing](#), the address may or may not be included explicitly. All received tactical messages are sent to the DLP whether it was addressed to a unit or not. Service Headers only include the address information when necessary (when the message has to be relayed or when the receiving units may have to acknowledge the message). When a NU receives a message, the SNC can extract the address list only if the Service Header includes the address. This reduces the bandwidth used in waveforms and media with limited resources.

The same addressing types are used for both tactical and technical messages. If addressing types are used for both MR and non-MR in a single service request, the SNC combines the list of units in the two address types into a single list in order to assess the routing and relay requirements. The major constraint that exists is when a combination of MR with Guaranteed Delivery and non-MR is required. In this case, if the GD protocol completes, not all non-MR destinations may receive the message as the GD protocol takes precedence.

The referenced [[STANAG 5522](#)] only defines the addressing of a few tactical messages. For both tactical and technical message transmission requests, there are no cases where a combination of both MR and non-MR addressing is used.

A unit is defined as an RF neighbor (or just neighbor) of another unit, when it can receive from, or be received by, the other unit.

For the examples in the remainder of this section, unit number 1 is the originator of the message. Any unit relaying the message is the source of the message. The examples use the color coding as shown in [Figure 3C.5-1](#).

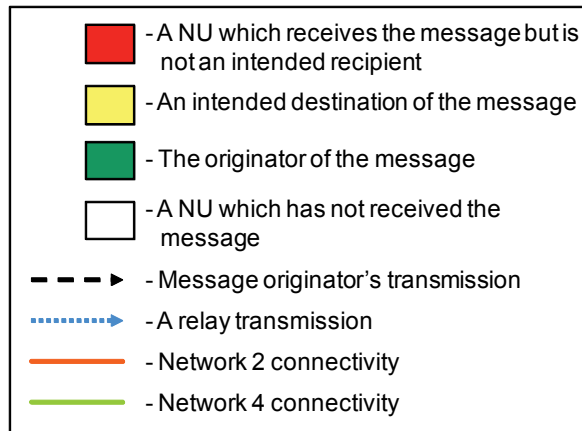


Figure 3C.5-1 Legend

In the examples, it is assumed that the connectivity between units is perfect. What actually happens cannot be stated absolutely as the radio communication conditions do vary, and units expected to receive may not and units that are not expected to receive may.

The addresses that are included in Service Headers may be different than those in the transmission request as the addressees on a network may be only a small subset of the requested destinations. When a relay transmission is made, the destination list may be reduced again to save bandwidth (for example, reducing the units on a dynamic list, or using a dynamic list if this saves space when using a MASN and a long exclusion list).

3C.5.1 Neighborcast

With neighborcast addressing, all RF neighbors of the message originator, regardless of which networks they are operating on, are the intended destinations. The transmission of a neighborcast message will be on as many networks as necessary to reach all the RF neighbors. The Service Header used indicates to all receiving units that no relay is required. In [Figure 3C.5-2](#), all the RF neighbors of unit 1 are the intended destinations of the message. For non-MR, the Service Header does not

contain any address information; all the neighbors on both networks will just receive the transmissions. For MR, the Service Header contains the address information, so all the receiving units know that they are addressees and have to acknowledge the message.

- Unit 1 transmits the message in both networks. Units 2, 4, 7, 8, 9, 10 and 11 receive the message
 - All message recipients, units 2, 4, 7, 8, 9, 10 and 11, know that no relay is required due to the Service Header used

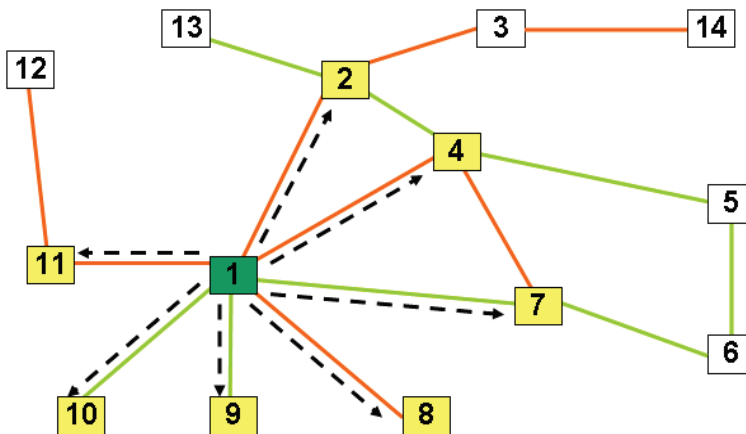


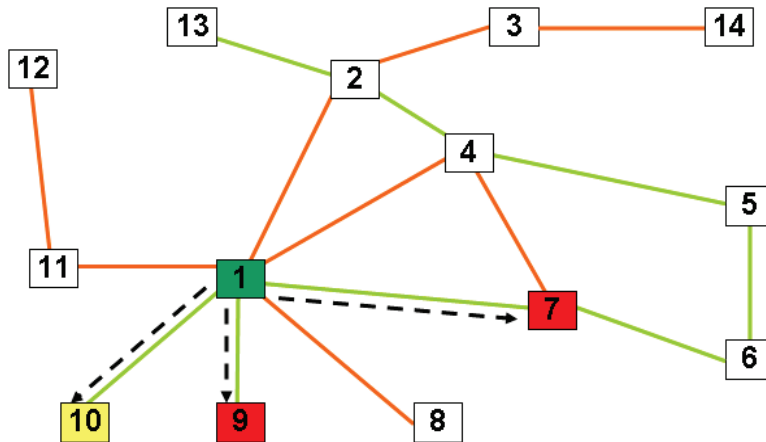
Figure 3C.5-2 Neighborcast

3C.5.2 Point-to-Point

With Point-to-Point addressing, a single unit is the only intended destination. In [Figure 3C.5-3](#), unit 1 transmits a message addressed to unit **10**, which is a neighbor. Unit 1 transmits on just network 4. For non-MR, the Service Header does not contain the addressee. All neighbors on the network receive the transmission including the intended destination. For MR, the Service Header contains the addressee, so that unit **10** knows that it is an addressee and that it has to acknowledge the message. The following events are highlighted.

- Unit 1 transmits the message only in network 4. The network 4 neighbors, units 7, 9 and **10** receive the message

- Units 7 and 9 are not intended destinations, and determines that they do not need to relay
- Unit **10**, the intended destination, receives the message and determines that it does not need to relay



include any address information in the Service Header. For MR, address information is included as unit **14** needs to know that it is an addressee and has to acknowledge receipt of the message. Units **2** and **14** receive the message

- Unit **14** is the intended destination and determines that it does not need to relay the message
- Unit **2** discards the message because it is a duplicate

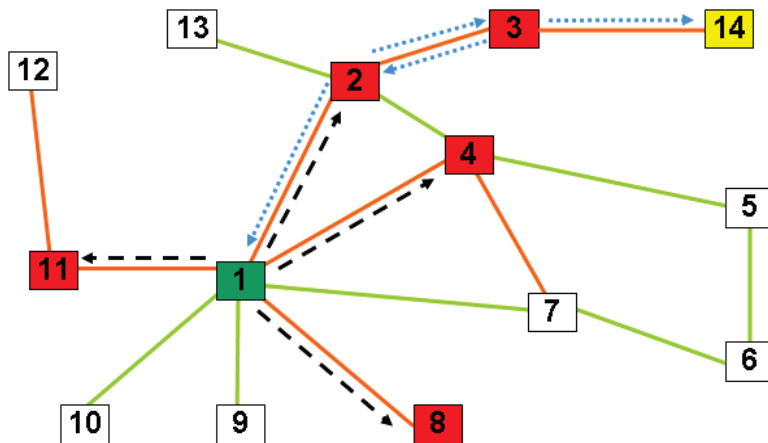


Figure 3C.5-4 Point-to-Point to a Non Neighbor

3C.5.3 Dynamic List

With Dynamic List addressing, a list of two to five units are the intended destinations. [Figure 3C.5-5](#) shows an example where units **8**, **10** and **14** are the requested destinations, as colored in yellow. The following events are highlighted.

- Unit 1 transmits in both networks 2 and 4. The transmission in network 2 is necessary to reach unit **8**, both a neighbor and an intended destination, and also to reach unit **2**, which is capable of relaying to intended destination unit **14**. The transmission in network 4 is necessary to reach unit **10**, which is both a neighbor and an intended destination. Units **2**, **4**, **7**, **8**, **9**, **10** and **11** receive the message
 - Units **8** and **10** are intended destinations and determine that they do not need to perform relay

- Unit 2 is not an intended destination, but determines that it has to perform relay for at least one of the intended destinations
- Units 4, 7, 9 and 11 are not intended destinations and determine that they do not need to perform relay
- Unit 2 performs a relay transmission in network 2. Units 3 and 1 receive the message
 - Unit 3 is not an intended destination but determines that it is a relay unit for an intended destination
 - Unit 1 discards the message because it is the originator
- Unit 3 performs a relay transmission in network 2 in order to reach unit 14. Units 14 and 2 receive the message
 - Unit 14 is an intended destination and determines that it does not need to perform relay
 - Unit 2 discards the message as it is a duplicate

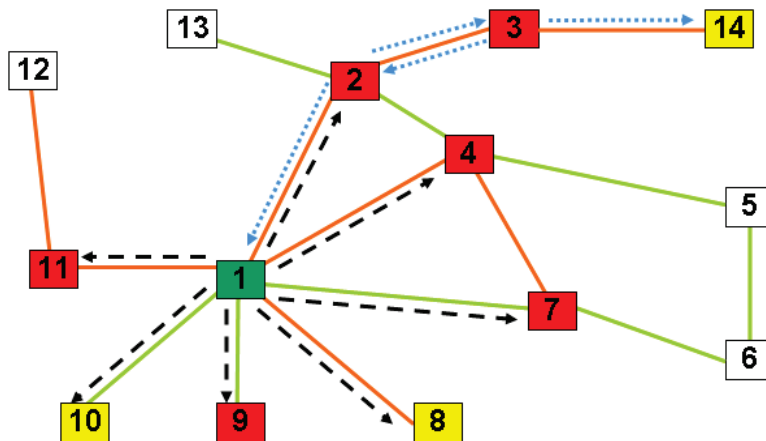


Figure 3C.5-5 Dynamic List

3C.5.4 MASN

A number of units can be grouped together and addressed by using a single number (MASN). This reduces the bandwidth used for addressing in Service Headers when the intent is to reach a group of units. MASN can be thought of as a group of destinations contained in a pre-defined list known by all units, which can be addressed by just using the list number. The units in a network are defined in a Network

Membership MASN. This allows all units in a network to be addressed by using the network membership MASN for the network. MASN are detailed in section [3B.5 SN Directory Maintenance](#). In [Figure 3C.5-6](#), MASN 27 is composed of units 2, 3, 4, 12, 13, and 14. All members of MASN 27 are intended recipients of a message addressed to MASN 27. The following events are highlighted.

- Routing determines that unit 1 only needs to transmit the message in network 2, based on the list of destination units and the knowledge of the connectivity. Units **2, 4, 8**, and 11 receive the message
 - Unit 8 is not an intended destination of the message and determines that it does not need to perform relay
 - Unit **4** is an intended destination and determines that it does not need to perform relay
 - Unit **2** is an intended destination and determines that it is a relay unit for other intended destinations
 - Unit 11 is not an intended destination of the message but determines that it is a relay unit for other intended destinations
- Unit **2** performs a relay transmission in network 4 in order to reach unit **13** and also in network 2 in order to reach units **3** and eventually **14**. Units **3, 4, 13** and 1 receive the message
 - Unit **4** discards it because it is a duplicate
 - Unit **3** is an intended destination of the message and determines that it is a relay unit for other intended destinations
 - Unit **13** is an intended destination and determines that it does not need to perform further relay
 - Unit 1 discards the message because it is the originator
- Unit 11 performs a relay transmission in order to reach unit **12**. Units **12** and 1 receive the message
 - Unit **12** is an intended destination of the message and depending on timing may perform relay
 - Unit 1 discards the message because it is the originator
- Unit **3** performs a relay transmission in order to reach unit **14**. Unit **14** and unit **2** receive the message
 - Unit **14** is an intended destination of the message and determines it does not need to perform further relay
 - Unit **2** is an intended destination of the message but discards it because it is a duplicate

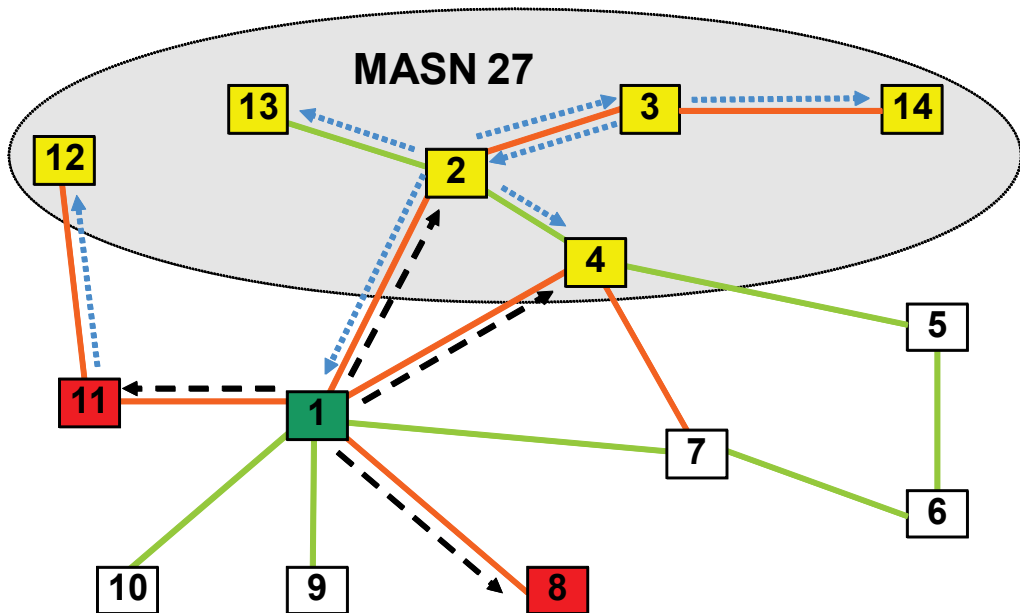


Figure 3C.5-6 MASN

3C.5.5 Totalcast

With Totalcast addressing, all other units in the Super Network are the intended destinations. In the case of Totalcast the message is relayed by the necessary relay units so as to reach all units, as defined in section 3C.8 Relay & Routing. In the example shown in Figure 3C.5-7, the following events are highlighted.

- Unit 1 injects the message in both network 2 and network 4 Totalcast, indicating that all units are intended destinations. Units 2, 4, 7, 8, 9, 10, 11 receive directly from the message originator
 - Units 8, 9 and 10 determine that they do not need to perform further relay
 - Units 2, 4, 7, and 11 determine that they are relay units for other intended destinations
- Unit 2 performs a relay transmission in network 2 in order to reach unit 13 and another relay transmission in network 4 in order to reach units 3 and 14. Units 1, 3, 4, and 13 receive the message
 - Unit 1 will discard the message as it is the message originator

- Unit 3 determines that it is a relay unit for other intended destinations
- Unit 4 discards it because it is a duplicate
- Unit 13 determines that it does not need to perform relay
- Unit 4 performs an additional relay transmission only in network 2 because its neighbors who have not received the message are all members of network 2. Units 2 and 5 receive the message
 - Unit 2 discards the message because it is a duplicate
 - Unit 5 determines that it may need to perform additional relay to its only other neighbor, unit 6
- Unit 7 performs an additional relay transmission in only network 2 because the only neighbor that has not received the message is a member of network 2. Unit 6 and unit 1 receive the message
 - Unit 6 determines that it may need to perform additional relay to its only other neighbor, unit 5
 - Unit 1 will discard the message as it is the message originator
- Unit 11 performs a relay transmission in order to reach unit 12. Unit 12 and unit 1 receive the message
 - Unit 12 determines that it does not need to perform relay
 - Unit 1 discards the message as it is the message originator
- Unit 3 performs a relay transmission in order to reach unit 14. Units 2 and 14 receive the message
 - Unit 2 discards the message as it is a duplicate
 - Unit 14 determines it does not need to perform relay
- Additional relays may occur depending on the ONCS timing
 - Either of units 5 or 6 may perform an additional transmission to relay the message. This relay depends on the ONCS timing, as one of these units may determine that its neighbor has already received the message if it receives the message relayed from the neighbor

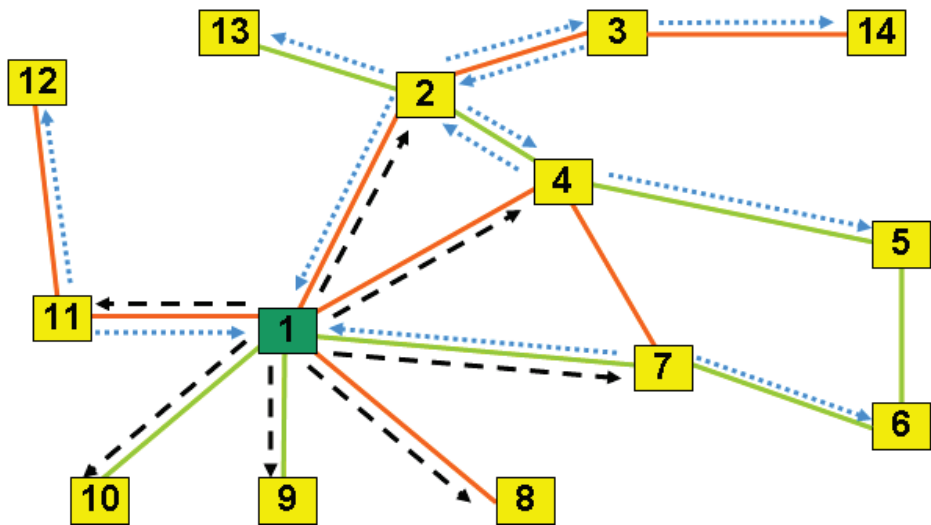


Figure 3C.5-7 Totalcast

3C.6 Duplicate Detection

Duplicate detection is the process used to determine whether a Message Packet (MP) has already been received or not. An MP consists of a service header and zero to three messages; it has associated with it a specific Message Time of Validity (MTV). For an MP to be a duplicate the following attributes all have to be the same.

- Message Time of Validity (MTV)
- Source (NILE Address)
- Type (Tactical or Technical)
- Data Unit
 - Size (Tactical Message Words or Technical number of bits)
 - Contents

Duplicate detection is very important in order to prevent data looping of an MP, as any received MP that has already been received or was transmitted is discarded. This stops the same MP from being constantly re-transmitted (relayed) by a unit. It also minimizes the number of received tactical messages sent to the DLP, and ensures that the DLP does not receive the tactical messages that it originated.

In principle, duplicate detection is a simple concept, which can be thought of as comparing the newly received MP to all previously received or transmitted MPs. However, if implemented in this way, there would be significant processing load incurred. To minimize this processing, the storage of received MPs is organized based on the comparison attributes listed above. This reduces the number of MPs that need all attributes checked. As soon as one attribute does not match, the comparison is terminated.

The majority of the processing performed by duplicate detection involves the searching of the data structures. Because the speed of execution is much more important than the amount of memory used, the data structures are memory resident, which uses significant amounts of memory. This storage is referred to as the duplicate detection Message Packet Store.

Given the importance of the duplicate detection function, the organization of the data structure and an explanation of how the processing works is detailed in the following two sections.

- Message Packet Store
- Processing Algorithm

3C.6.1 Message Packet Store

The duplicate detection Message Packet Store consists of four main parts as shown in Figure 3C.6-1. It is used by duplicate detection to store the attributes of the message packets that have been received, so that it can detect whether a received message packet has previously been received.

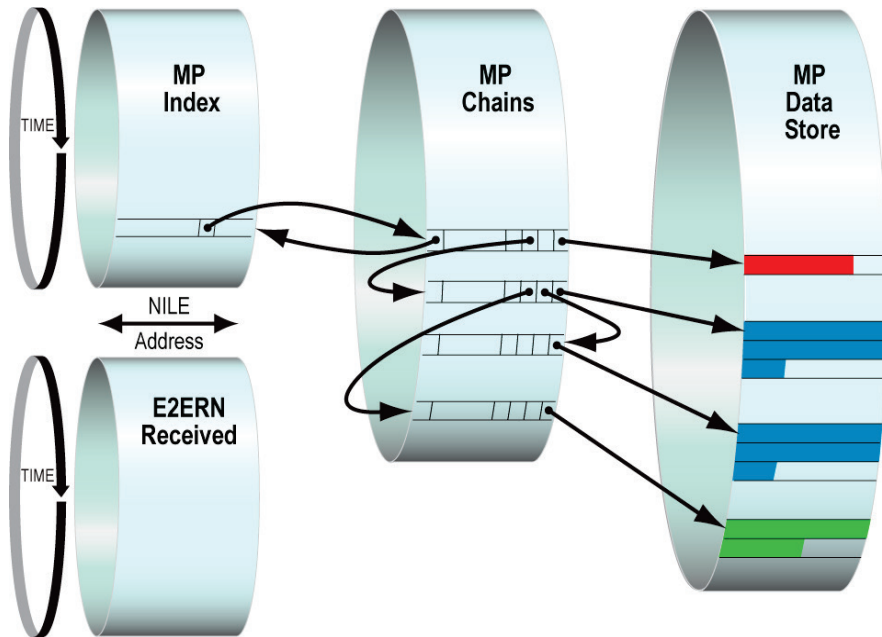


Figure 3C.6-1 Structure of Duplicate Detection Message Packet Store

The MP Index is accessed by the Time Index (see [Calculate the Time Index Value](#)) which is calculated from the MTV, and then within the record by the NILE Address. A null index value indicates no previous MP has been received from the NU with the MTV. When not null, the index points to an entry in the MP Chains, which forms the top of a chain of records that link together all MPs that have been received with the same MTV from the NU. The chain record points to the contents of the message packet which is stored in the MP Data Store. The chain record links together in one chain all of the MPs of the same type and size as the first MP. It also links to the next type and size record, and each record in this chain may have a chain of records of the same type and size, and also may point to the next type and size record.

- The End-to-End Reference Number (E2ERN) Received table is also accessed by the Time Index, and then within the record by the NILE Address. Each record is an array of Boolean values, one for each E2ERN, which indicates whether a message packet has been received for this combination of NILE Address, MTV and E2ERN.

All components of the data store are circular buffers so that as time passes, the entry of new data overwrites the old entries. This prevents the need for deletions, thus significantly reducing the processing load that would result from deleting large amounts of data.

The length of the MP Index and E2ERN Received tables is the maximum perishability (511 seconds) plus 3 extra seconds to allow for processing delay, for a total of 514 records.

The size of MP Chains is set such that it is able to hold the maximum number of Message Packets that may be received per second multiplied by the length of the MP Index (514). The size of the table means that when a record is the next to be overwritten, it is guaranteed to be out of date.

The number of elements in the MP Data Store is such that maximum bandwidth for four networks for the length of the MP Index (514) can be stored.

3C.6.2 Processing Algorithm

The algorithm for Duplicate Detection uses the components of the data store to compare progressively more detail of the Message Packet's attributes with the stored information. All of the Message Packet attributes do not necessarily need to be compared to determine that a Message Packet is unique.

The processing consists of the following functions.

- Calculate the Time Index Value
- Perform Index Maintenance
- Get and Set E2ERN Received Flag
- Check the MP Index
- Compare Type and Size to the MP Chains
- Compare the MP Data to the MP Data Store
- Store a Non Duplicate

□ ***Calculate the Time Index Value***

The MP Index and E2ERN Received data structures are circular buffers that contain a record for each second of time, with the newest record overwriting the oldest. Both circular buffer lengths are 514 records. The index into these data structures is the Time Index (0-513). The MTV of the MP is converted into the Time Index using the modulus function, taking into account any midnight boundaries that have been crossed and the length of the circular buffer. When the next midnight is crossed, the stored midnight value is updated to the value it was at this new midnight, so that there are no jumps in the value of the Time Index. The formula for calculating the Time Index is as follows.

$$\text{Time Index} = (\text{Previous Midnight Time Index} + \text{MTV}) \text{ modulus } 514$$

The maximum MTV that has been received is stored in the Last Time Index.

□ ***Perform Index Maintenance***

This operation performs the Index maintenance function on the MP Index and E2ERN Received data structures. When the MTV of a received MP is greater than the maximum MTV currently stored in the Last Time Index, the index maintenance resets (clears) all of the records after the Last Time Index up to and including the new Time Index, because any data in these records is older than one full cycle of the circular buffer. The MP Index record may contain pointers to entries in the MP Chains, which then point back (back pointer) to the MP Index record. These back pointers in the MP Chains are cleared first, and then the MP Index record is reset. The records in the E2ERN Received table for the same seconds are also reset.

The example in [Figure 3C.6-2](#) shows the received MTV being 3 seconds greater than the maximum MTV previously received and so 3 records in the MP Index (shown in

green) and the same three records in the E2ERN Received table have to be reset. In this example the records to be reset only point to 2 records in MP Chains, in which the back pointer is reset to null.

There is no additional maintenance required on the MP Chains and none on the MP Data Store, as they are sized to be big enough to contain the maximum amount of data that can be received in the duration of the Time Index. This means that writes to these data structures just use the next record to be used, and cycle around the data structures overwriting the old data. Just to be certain, a check is made on the back pointer in the MP Chains data structure to ensure that the index maintenance has reset the pointer in the record before reuse.

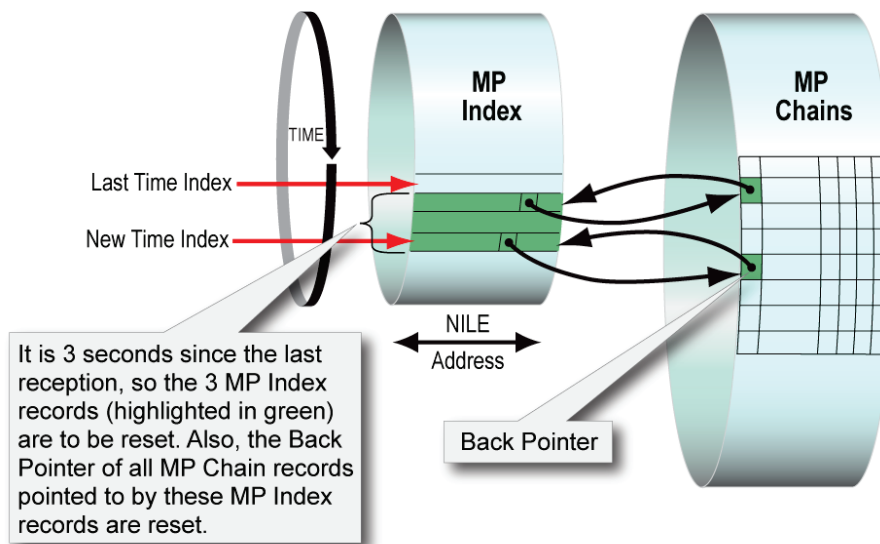


Figure 3C.6-2 MP Index Maintenance

□ Get and Set E2ERN Received Flag

If the MP contains an MR Group in the service header (contains an E2ERN), the NU's E2ERN flag in the record pointed to by the Time Index is first read to find if the MP with the E2ERN has previously been received and therefore acknowledged. If the flag was not set previously, it is now set. This is shown in [Figure 3C.6-3](#). This is used to detect when a received MP is a duplicate but the previous copies did not have an MR Group in the service header. Normally when a duplicate is detected it is discarded, but when the flag was not set, an acknowledgement has not been generated for the

previous copies of the MP, and must be generated before the duplicate can be discarded.

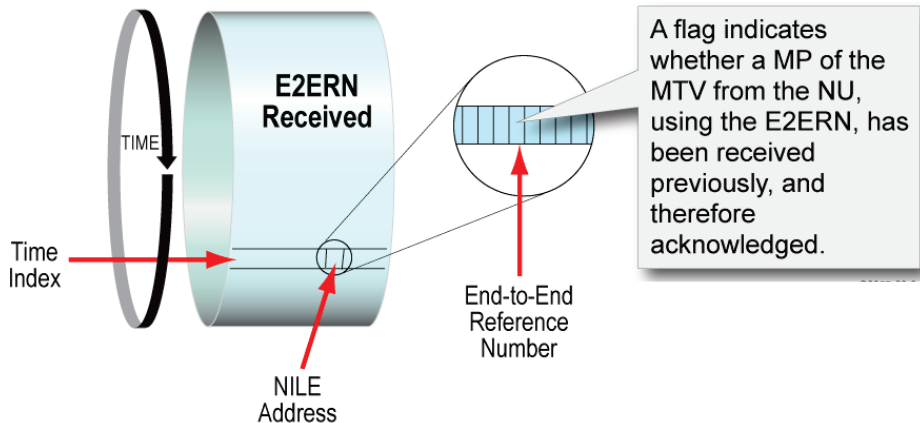


Figure 3C.6-3 Accessing the E2ERN Received Flag

□ Check the MP Index

The record pointed to by the Time Index contains a pointer for each NILE Address to the MP Chains data structure. If the pointer is null (see [Figure 3C.6-4](#)) then the current MP is the first from the NILE Address with this Time Index (or MTV). The Message Packet is therefore a non-duplicate and is stored (see function [Store a Non Duplicate](#)).

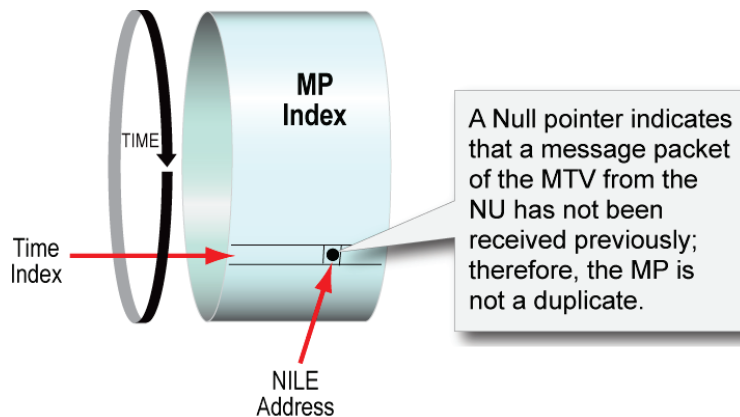


Figure 3C.6-4 Null Pointer in MP Index for NU and MTV

If the pointer is not null (see [Figure 3C.6-5](#)) then the next level of comparison must be made by checking the MP Chains (see next function [Compare Type and Size to the MP Chains](#)).

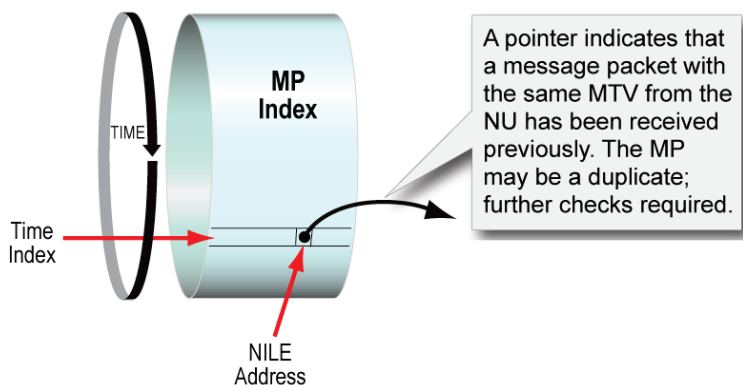


Figure 3C.6-5 Checking the MP Index

□ **Compare Type and Size to the MP Chains**

The MP Index points to a chain of at least one Message Packet in the MP Chains. The 'Type and Size' field of each entry in the 'Type and Size' chain are compared with the 'Type and Size' of the MP until a match is found or the end of the chain is reached. If no match is found, then the Message Packet has not been previously received and is therefore a non-duplicate which is stored (see function [Store a Non Duplicate](#)). If a match is made then a comparison of the MP contents will have to be made (see next function [Compare the MP Data to the MP Data Store](#)).

For example if the current MP is one tactical data word, then in [Figure 3C.6-6](#), the 'Type and Size' of the record pointed to by the MP Index does not match. However the 'Type and Size' of the record pointed to by the 'Next Type and Size' pointer (red arrow) does match.

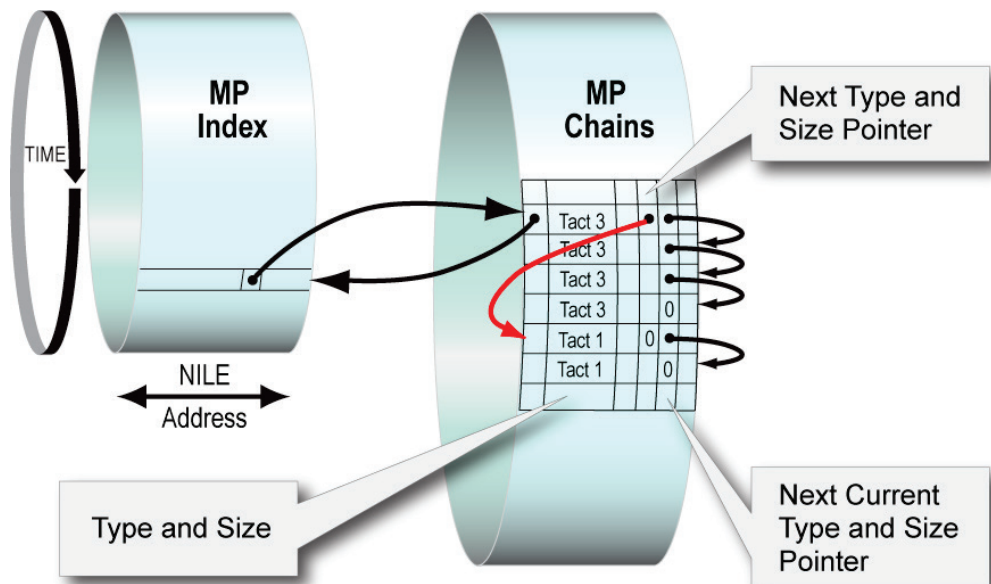


Figure 3C.6-6 Comparing Type and Size to the MP Chains

□ Compare the MP Data to the MP Data Store

From the matching 'Type and Size' entry there is a chain of records that have the same 'Type and Size'. Each record points to the MP Data Store where the MP contents are stored. The data pointed to by each chain entry is compared with the data in the current received Message Packet. For example, as shown in [Figure 3C.6-7](#), if the current MP is one tactical data word, then the contents of the current MP are compared to the two MPs stored (shaded in blue) in the MP Data Store. These are accessed using the pointers shown in blue in the figure. If the data matches either then the Message Packet is a duplicate. If there are no matches then the Message Packet is not a duplicate and is stored (see next function [Store a Non Duplicate](#)).

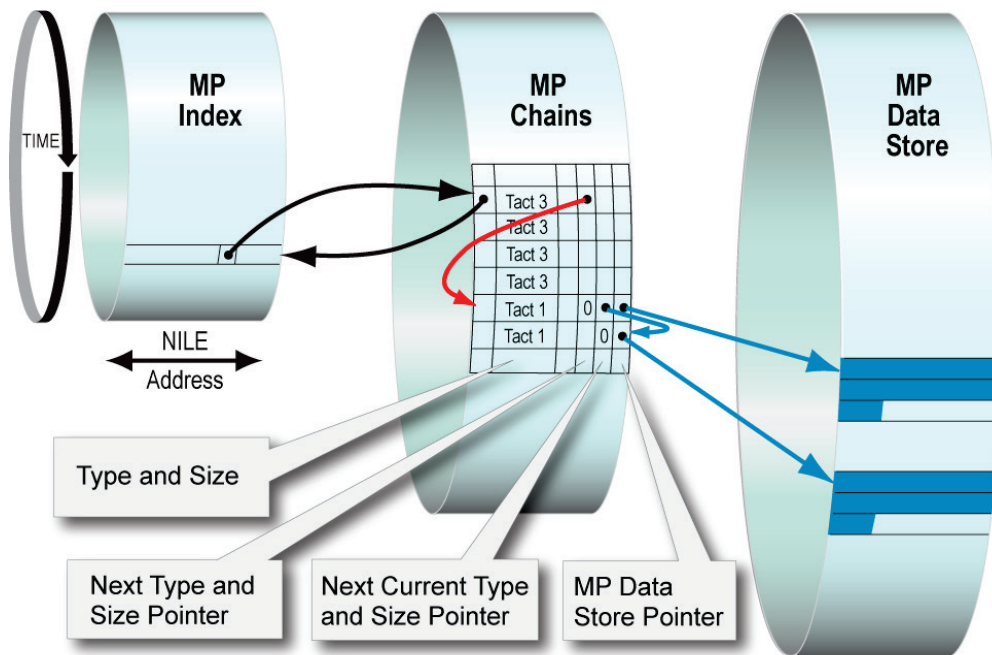


Figure 3C.6-7 Comparing the MP Data to the MP Data Store

□ Store a Non Duplicate

If a Message Packet is not a duplicate it is stored. The MP contents are stored in the MP Data Store starting at the next location as long as there is space to fit the data without going off the end of the buffer. If there is not, then it is stored starting at the beginning of the buffer. The next MP Data Store location is set to be the start location plus the length of the message in 32-bit words.

The current MP Chain record pointer is incremented, and if off the end of the array, it is set to the start. The MP 'Type and Size' is stored in the current MP Chain record. The 'back pointer', the 'next type and size' pointer and the 'next current type and size' pointer are all set to be null pointer in the new MP Chain record. The data pointer in the new MP Chain record is set to be the location in the MP Data Store where the message packet contents were stored.

Depending where in the comparison process it was found that the MP was not a duplicate affects the storage process, as follows.

- **MP Index is null pointer:** The MP Index is set to point to the new MP Chain record, and the 'back pointer' in the new MP Chain record is set to point to the Time Index
- **New Type and Size:** The end of the 'Type and Size' chain has been reached, so the 'next type and size' pointer of the current MP Chain record is set to point to the new MP Chain record
- **Type and Size found but data different:** The end of a 'This Type and Size' chain has been reached, so the 'next current type and size' pointer of the current MP Chain record is set to point to the new MP Chain record

3C.7 Network Cycle Structure Handling

An NCS can be provided directly by the DLP or computed by the SNC. In both cases, all parameters for the initialization are included in the OLM in the form of timeslots that define the NCS or input parameters to be used to calculate the NCS. Once the network becomes operational the NCS becomes the Operational NCS (ONCS). The DLP of the NMU can generate and distribute new NCSs after the network is operational. The SNMU can also order the NMU to change the ONCS.

The following parameters affect the NCS computation, as detailed in [2B.2.2 NILE Network Parameters](#) and [2B.4.3 Planner Defined NCS](#), which also provides an example of NCS computation.

- Number of Units in the Network
 - Capacity Need
 - Access Delay
- Tolerance
- Efficiency
- Media Type (HF FF, UHF FF, HF EPM and UHF EPM)
- Media Setting Numbers (MSN), from 1 to 6
- Fragmentation Rate, from 1 to 3
- TDMA Setting

Relay and Data Forwarding requirements should be taken into account when setting Capacity Need and Access Delay. Following an Initialization with probing, the SNC will automatically increase Capacity Need by 1 for the units designated as relayers.

This section describes how an NCS is calculated and what constraints there are on the NCS and is split into the following subsections.

- [NCS Computation](#)
- [NCS Constraints](#)

3C.7.1 NCS Computation

When the SNC computes the algorithm, it is mandatory that the result be deterministic. Therefore a set of rules are imposed to ensure that the same result is always achieved, regardless of the SNC computing environment.

The SNC calculation is iterative, starting from a simplified initial NCS, as show in [Figure 3C.7-1](#). The SNC attempts to create the smallest NCS that satisfies all input requirements.

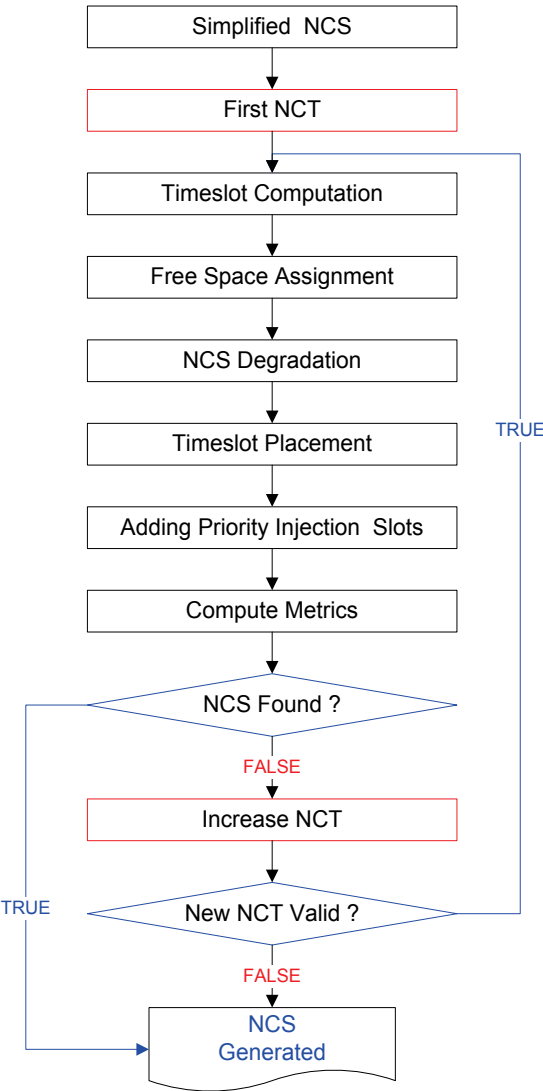


Figure 3C.7-1 NCS Computation Flow

□ ***Simplified NCS***

A simplified initial NCS is computed providing each unit with a timeslot of the minimum length that meets the media constraints and efficiency.

□ ***First Net Cycle Time (NCT)***

The First NCT is computed to verify that the constraint of 1024 minislots is satisfied, based on the formula below. Timeslot length is the maximum value allowed based on the input efficiency.

$$\text{First_NCT} = \text{Timeslot_Length} * \text{Number_of_NUs}$$

When the resulting NCT is longer than 1024 minislots, the timeslot length is reduced to some of the units, starting from the units with lowest required CN/AD. This is performed until the limit of 1024 minislots is achieved. This only occurs when using HF EPM MSN 4 with more than 78 units.

□ ***Timeslot Computation***

The SNC divides the NCS in a number of slices, based on lowest access delay.

$$\text{Number_of_Slices} = \text{roundup} \left(\frac{\text{NCT}}{\text{Shortest_AD} * (1 + \text{ADT})} \right)$$

- *Number of Slices*: Number of slices required in the current step
- *NCT*: Length of the NCT in seconds
- *Shortest_AD*: The shortest Access Delay in the input
- *ADT*: Access Delay Tolerance in decimal value (e.g. 0.15 for 15%)

For example, if the lowest access delay is 4 seconds and the First NCT is 16 seconds, four slices are created as shown in [Figure 3C.7-2](#).

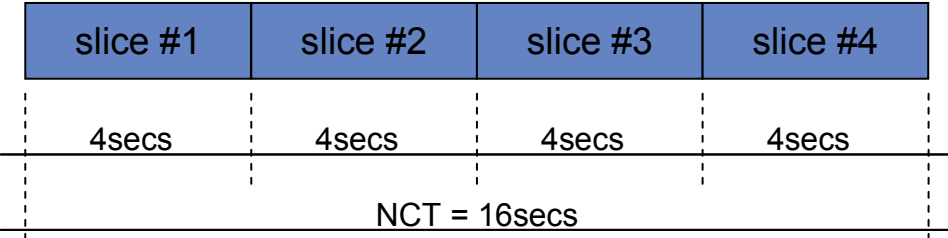


Figure 3C.7-2 NCS Slice Allocation

For each unit, the initial minimum number of timeslots is computed, along with the number of bits needed to meet the required capacity need.

The NCT is updated based on the number of timeslots and allocated capacity, assuming that timeslots assigned to each unit are distributed evenly in the NCS.

□ Free Space Assignment

When possible, the SNC attempts to add minislots to increase timeslot length and therefore increase NCS Efficiency. The process stops as soon any of the following conditions are satisfied.

- The required Efficiency is met
- There is no free space available
- Maximum timeslot length is reached

If DTDMA is enabled, any available free space is used to create additional timeslots and to increase the timeslot length assigned to each unit.

- Additional timeslots are added while there is enough free space to create timeslots with at least the Efficiency specified in the input parameters
- Timeslot length is increased and the process stops as soon as there is no free space available or the maximum timeslot length is reached

□ NCS Degradation

If the SNC cannot compute an NCS within the 1024 minislots and 256 timeslots boundary, a progressive degradation sequence is applied reducing the size and the number of timeslots assigned to the units. Units with lower CN/AD are degraded first. When multiple units have the same input parameters, the degrading starts with the unit with the highest NILE Address, progressing to the lowest address. This is performed until the NCS is within the above constraints.

□ **Timeslot Placement**

NILE Units are sorted based on the number of allocated timeslots, from the highest to the lowest, and then based on the access delay from the shortest to the longest. Timeslots are distributed among slices to optimize Access Delay. [Figure 3C.7-3](#) shows an example of placement. It can be seen that unit 1 and 2 have AD requirement (4 seconds) and are repeated 4 times (once in each slice) and in the same sequence. The units with an AD requirement of 8 seconds are placed in subgroups and only repeated 2 times within 16 seconds. Units with AD of 16 seconds or higher are placed throughout the slices, just once.

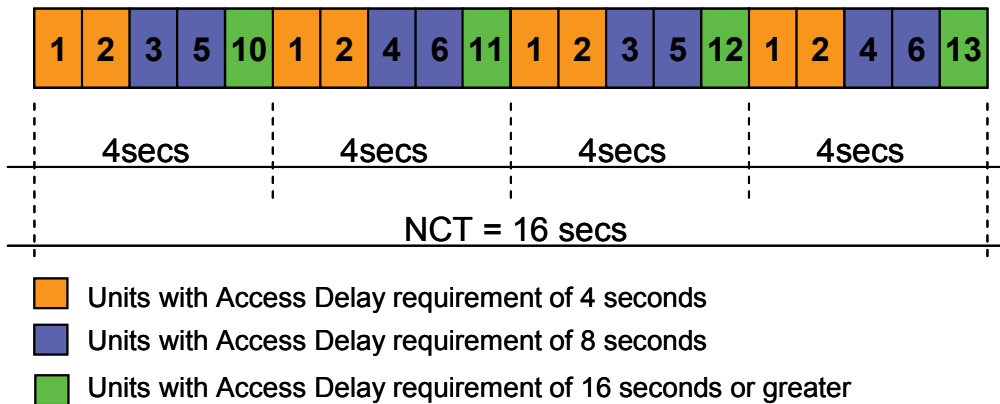


Figure 3C.7-3 Timeslot Placement

□ **Adding Priority Injection Timeslots**

Link 22 requires the inclusion of a number of Priority Injection (PI) timeslots, in addition to those needed to satisfy the Channel Access Delay, as defined by the following formula.

$$\text{Number_of_PI_Slots} = \text{roundup} \left(\frac{NCT_i - 12.5}{12} \right)$$

The formula is applied twice in order to take into account that the NCT increases when the PI timeslots are added. For example, if the current value of the NCT in HF FF is 24.3 seconds (216 minislots), adding the first PI timeslot will increase the NCT so that it is greater than 24.5 seconds. Therefore an additional PI timeslot is required.

□ ***Compute Metrics***

The NCS computation stops when a new iteration does not improve the metrics based on Delay, Capacity and Efficiency. To ease the process, a single index is computed for quick comparison.

The above sequence is applicable if the NCS fully satisfies all input parameters or the NCS is longer than 1024 and minislots and timeslots are removed.

□ ***Exit Criteria***

The NCT increases with each iteration. This is repeated until the limit of 1024 minislots is reached, or until the comparison between two iterations shows that the new computation does not improve the overall metrics.

3C.7.2 NCS Constraints

A valid NCS has a limit of 1024 minislots and 256 timeslots. The timeslot size limitations are listed in [Figure 3C.1-4](#). The SNC rejects any NCS which does not meet these constraints.

Media	MSN	Frag Rate	Assignment Slot Sizes	Permitted Priority Injection Slot Sizes
HF FF	All	1	4-16 (Valid numbers: 4, 5, ... 16)	2-16 (Valid numbers: 2, 3, 4, 5, ... 16)
		2	5-15 odd values only	3-15 odd values only
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
UHF FF	1	1	4-32	2-32
		2	5-31 odd values only	3-31 odd values only
		3	4,7,10,13,16,19,22,25,28,31(every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
HF EPM	All	1	4-32	2-32
UHF EPM	1	1	4-32	2-32
	2	1	5-31 odd values only	3-31 odd values only
	3	1	4,7,10,13,16,19,22,25,28, 31(every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
	4	1	5, 9, 13, 17, 21, 25, 29 (every 4 th)	5, 9, 13, 17, 21, 25, 29 (every 4 th)

Figure 3C.7-4 Timeslot Size Constraints

The SNC algorithm includes additional limitations which do not allow some of the smaller timeslot size values. The additional limitations on assignment timeslot size are to ensure that the timeslot can accommodate the largest possible message packet (large service header and 8 TMWs). The additional limitations on PI timeslot size are to ensure that the PI timeslot can accommodate the largest allowable PI message packet (service header and 3 TMWs). An OLM or DLP designed NCS may not have the same limitations, based on their knowledge of the likely occurrence of the larger tactical messages. However, the SNC limits that are listed in [Figure 3C.7-5](#) are the recommended values to be used by the DLP and the OLM planners.

Media	MSN	Frag Rate	Recommended Assignment Slot Sizes	Permitted Priority Injection Slot Sizes
HF FF	1	1	7–16	3–16
		2	7–15 (odd values only)	3–15 (odd values only)
		3	7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	2	1	5–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	3	1	5–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	4	1	4–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	5	1	4–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
	6	1	4–16	2–16
		2	5–15 (odd values only)	3–15 (odd values only)
		3	4, 7, 10, 13, 16 (every 3 rd)	4, 7, 10, 13, 16 (every 3 rd)
UHF FF	1	1	4–32	2–32
		2	5–31 (odd values only)	3–31 (odd values only)
		3	4,7,10,13,16,19,22,25,28,31(every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
HF EPM	1	1	5–32	2–32
	2	1	7–32	3–32
	3	1	7–32	3–32
	4	1	Min(13,Int(1024/#NUs)) – 32	5–32
UHF EPM	1	1	4–32	2–32
	2	1	5–31 (odd values only)	3–31 (odd values only)
	3	1	4,7,10,13,16,19,22,25,28, 31(every 3 rd)	4,7,10,13,16,19,22,25,28,31(every 3 rd)
	4	1	5, 9, 13, 17, 21, 25, 29 (every 4 th)	5, 9, 13, 17, 21, 25, 29 (every 4 th)

Figure 3C.7-5 Recommended Timeslot Sizes Constraints

3C.8 Relay & Routing

This section describes how connectivity information is collected and distributed, the generation of the routing table, the determination of relay units and the best route selection to inject each message based on the Quality of Service. The following topics are addressed.

- Direct Link Reception Quality
- Link Reception Quality (LRQ)
- Relay Units
- Link Connectivity Data (LCD)
- Route Path Determination
- Probability of Correct Reception
- Routing Selection
- Message Relay
- DLP Optimization

The following list summarizes requirements and constraints that summarize key elements of the protocols described.

- All protocols are distributed
- Protocols must support multiple levels of Quality of Service
- Resilient protocols are required to maximize the probability that messages are delivered. This also minimizes the effect of jamming threats
- The connectivity between two units may be different in each direction
- Connectivity information is distributed up to three legs
- Any destination that does not have an 'Inactive' status is considered reachable, therefore a solution is identified regardless of the known connectivity
- Each unit needs to determine the probability of correct reception for reliability purposes for each network transmission
- Different media have different characteristics which require harmonization for both connectivity data collection and assessment of the best paths to all the destinations
- Traffic requiring relay is estimated at 10% of the overall load
- Most of the traffic requiring relay will reach all or multiple destinations

3C.8.1 Direct Link Reception Quality

When a unit enables reception on a network it starts monitoring how well it's receiving from each of the units in the network. From the monitoring information, it generates statistics on the probability of reception from each unit in the network (called the Reception Probability (RxP)). The RxP value is a real number in the range 0.0 to 1.0 which is internally maintained by the SNC. The SNC converts the RxP value into an integer Link Reception Quality (LRQ) value (0-3), using the ranges shown in [Figure 3C.8-1](#). This LRQ value which represents how well the unit is able to receive directly from the other units in the network is referred to as the Direct LRQ.

The SNC calculates the RxP using the following weighted running average formula.

$$RxP = RxP_{cur} * Alpha + (1-Alpha) * (NP_{rx} / NP_{ex})$$

Where the terms are as follows.

- **RxP** is the calculated RxP value
- **RxP_{cur}** is the current RxP value for the unit and network
- **Alpha** is a value in the range 0.0 to 1.0 selected from those listed in [Figure 3C.8-1](#) for the current RxP value
- **NP_{rx}** is the number of received NPs in the current timeslot
- **NP_{ex}** is the number of expected NPs in the current timeslot

[Figure 3C.8-1](#) also lists what the LRQ value means, what probability level it represents, the Alpha value used for that RxP range and the colors used for LRQ values in this section.

RxP Range	LRQ Value	Link Status	Probability Level	Alpha	Connectivity Color
0.0 - 0.6	0	No Link	-	0.492	Red
>0.6 - 0.8	1	Poor	60%	0.865	Yellow
>0.8 - 0.9	2	Good	80%	0.945	Green
>0.9 - 1.0	3	Excellent	90%	0.95	Blue

Figure 3C.8-1 Reception Probability and LRQ Values

In a weighted running average, Alpha is the value that controls what affect the current value has on the average. When Alpha is low then the current value has greater effect on the average, and when it is high it has less affect. Normally, Alpha is a constant tuned to give the required rate of change. Link 22 uses different values of Alpha based on the value of RxP, as listed in [Figure 3C.8-1](#). The Alpha values used were calculated so that the loss of two timeslots lowered the probability to the next level. Upon initialization, initial RxP is 0, and initial Alpha is 0.492. In the example of the formula below, the timeslot has a length of 16 NPs and all are received. Therefore after the first timeslot reception, the SNC computes.

$$RxP = 0.0 * 0.492 + (1-0.492) * 16/16 = 0.508$$

After the first reception, the LRQ value is still 0, since RxP is below the range for being considered at least 'Poor'. After each transmission slot, the RxP values are updated. [Figure 3C.8-2](#) shows the case when all NPs expected are received correctly.

Once each NCT, the SNC first converts RxP to LRQ values and then checks to see if there has been a change. When a change occurs, the SNC queues the change for transmission at the next opportunity. If the value changes before transmission, the new value is transmitted. In this way, the Direct LRQ is distributed to the unit's Radio Frequency (RF) neighbors. One unit is defined as a RF neighbor (or just neighbor) of another unit, when it can receive from, or be received by, the other unit. The neighbors also transmit their own Direct LRQ and so neighboring units will know the connectivity between each other.

Timeslot Reception	Alpha Used	RxP after each Timeslot Reception	LRQ Value	LRQ Meaning
0	0.492	0.000	0	No Link
1	0.492	0.508	0	No Link
2	0.492	0.758	1	Poor
3	0.865	0.791	1	Poor
4	0.865	0.819	2	Good
5	0.945	0.829	2	Good
6	0.945	0.838	2	Good
7	0.945	0.847	2	Good
8	0.945	0.856	2	Good
9	0.945	0.864	2	Good
10	0.945	0.871	2	Good
11	0.945	0.878	2	Good
12	0.945	0.885	2	Good
13	0.945	0.891	2	Good
14	0.945	0.897	2	Good
15	0.945	0.903	3	Excellent
16	0.950	0.908	3	Excellent
17	0.950	0.912	3	Excellent
18	0.950	0.917	3	Excellent
19	0.950	0.921	3	Excellent
20	0.950	0.925	3	Excellent

Figure 3C.8-2 RxP/LRQ Progression

The objective of the Link Reception Quality protocol is to assess not only if two units are connected, but also how well the units are able to receive from each other. In Figure 3C.8-3 the arrow indicates that unit 1 receives from unit 2, but unit 2 does not receive from unit 1.



Figure 3C.8-3 Direct Link Reception

3C.8.2 Link Reception Quality (LRQ)

The Link Reception Quality (LRQ) represents the quality of the reception (from the receiver's point of view). A bi-directional link between two units (1 & 2) means that 1 computes the Direct LRQ from 2 and 2 computes the Direct LRQ from 1. Both transmit their Direct LRQs in technical messages. The LRQ value that 1 receives in a technical message from 2 (which is the LRQ value for the link 1 to 2); unit 1 calls this the Complimentary LRQ or CLRQ. Each unit transmits not only its Direct LRQ values but also its CLRQ values received from its neighbors (LRQ values received where it is the transmitter). Both units in a link calculate how well they receive data and they transmit this information to their neighbors in technical messages. When units receive technical messages that tell them how well their data was received, the units know the connectivity in both directions.

The LRQ technical messages transmitted by a unit are received only by its neighboring units and are not relayed. A unit knows the LRQ and CLRQ values of its neighbors and because its neighbors transmit their technical messages, it knows the LRQ and CLRQ values of the neighbors of its neighbors. Therefore, LRQ knowledge is known for two legs.

The following aspects are further detailed.

- [Link Reception Quality Computation](#)
- [Link Reception Quality Technical Messages](#)
- [Link Reception Quality Tables and Technical Messages](#)

□ Link Reception Quality Computation

In the example shown in [Figure 3C.8-4](#), after the second timeslot reception from unit 2, the SNC of unit 1 will initially transmit an LRQ technical message with the two values of 'Poor' for LRQ and 'No Link' for CLRQ (assuming unit 2 has not yet transmitted its LRQ message). If unit 2 is receiving from unit 1, it will initially transmit an LRQ technical message with the same values from its own point of view.

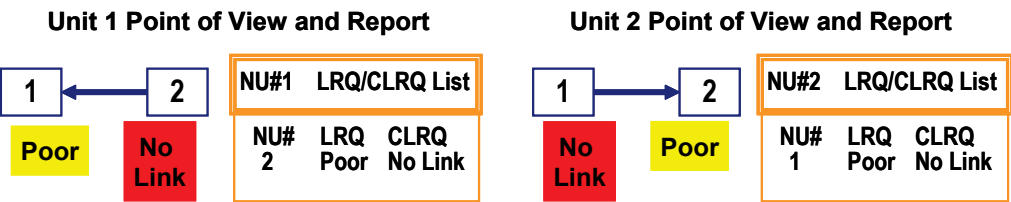


Figure 3C.8-4 LRQ first transmission

After the fourth timeslot reception, unit 1 will have updated its LRQ value for unit 2 and have knowledge of the received LRQ. The next transmission could be as shown in Figure 3C.8-5.

Unit 1 Point of View Update and Report

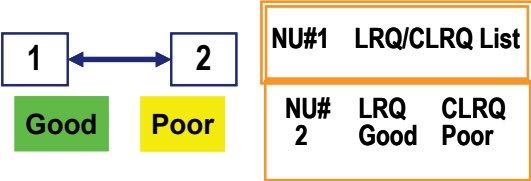


Figure 3C.8-5 LRQ additional transmission

The exact time sequence will depend on the position of timeslots in the ONCS. If we consider the following example, from the perspective of unit 1, the LRQ and CLRQ values (direct connections) will eventually (after 15 continuous receptions, derived from Figure 3C.8-2) be as indicated in Figure 3C.8-6. Note that unit 1 is directly connected to units 2, 3 and 4, but is not directly connected to unit 5.

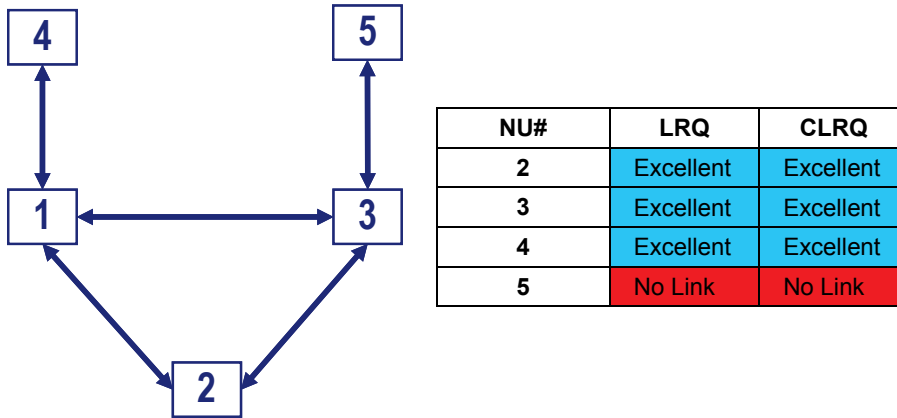


Figure 3C.8-6 LRQ – Steady State example

□ Link Reception Quality Technical Messages

There are 3 different LRQ technical messages that the SNC can transmit, as indicated in [Figure 3C.8-7](#). These are selected based on the number of entries and the reason for transmission, to minimize bandwidth use.

Message	Fixed or Variable Length	Number of Entries	Usage
Short LRQ	Fixed Length	1	Change only, used for a single change
Standard LRQ	Variable Length	1-45	Change or Periodical, if less than or equal to 45 entries
Compact LRQ	Fixed Length	125	Change or Periodical, if more than 45 entries

Figure 3C.8-7 LRQ Technical Message Summary

The standard LRQ technical message also includes a Change/Complete flag. When the SNC transmits only changes for a few neighbors, the flag is set to Change, and the technical message may include units with both LRQ and CLRQ values of zero. If the message is transmitted as a periodic message, or when all the units included have a non-zero value for both LRQ and CLRQ, the flag is set to Complete. In this case, all the entries with zero are omitted and the receiving SNC will consider all the units not listed in the message as having values set to zero. This minimizes the size of the transmitted message.

All LRQ technical messages are generated for transmission every five minutes, after the start of each network and regardless of change, to offset the loss of reception and to allow a unit joining the network to receive full connectivity information.

The SNC maintains two separate tables, one for LRQ values and one for CLRQ values, to be able to store all received values and adapt if no reception is received from a specific unit for a certain amount of time.

□ Link Reception Quality Tables and Technical Messages

Figure 3C.8-8 shows the reception of an LRQ technical message from unit 2. Unit 1 has a computed local direct value of ‘Good’ (based on the 0.82 value). Unit 1 receives a LRQ technical message from unit 2. The internal tables will be updated as indicated in Figure 3C.8-8. Note that the received LRQ entry may be stored twice, once in each LRQ and CLRQ table. This is only valid if the involved reference unit is the own ship entry, pointed to by the dashed line.

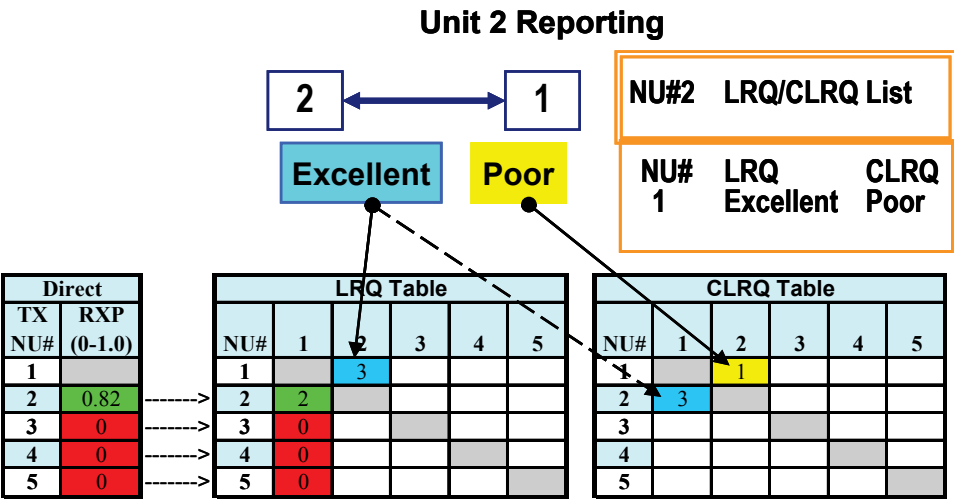


Figure 3C.8-8 LRQ and RxP tables

The blue cell in the LRQ table can be read as “NU 2 (Tx NU) is receiving from NU 1 (Rx NU) with a reported LRQ of 3”.

The yellow cell in the CLRQ table can be read as “NU 1 (Rx NU) was receiving from NU 2 (Tx NU) with a value of 1, as reported by NU 2 (Tx NU)”. This is for the benefit of the neighbors of unit 2 who are not neighbors of unit 1.

Note that in the example, this is not the same as the LRQ value that NU 1 is currently reporting for NU 2 (the green cell in the LRQ table). When steady state is reached, the two values will be the same.

With the configuration shown in Figure 3C.8-6, after the initial transition period from zero connectivity to steady state, the tables from the point of view of unit 1 will be as indicated in Figure 3C.8-9.

Direct		LRQ Table						CLRQ Table					
TX NU#	RXP (0-1.0)	NU#	1	2	3	4	5	NU#	1	2	3	4	5
1		1		3	3	3		1		3	3	3	
2	1.00	2	3		3			2	3		3		
3	1.00	3	3	3				3	3				
4	1.00	4	3					4	3				
5	0	5	0		3			5			3		

Figure 3C.8-9 LRQ and RxP Tables at Steady State

3C.8.3 Relay Units

Relay units should have extra capacity to relay traffic. Link 22 defines two levels of relay units as indicated below.

- Potential Relay NILE Unit (PRNU)
- Reporting Potential Relay NILE Unit (RPRNU)

A **Potential Relay NILE Unit (PRNU)** is defined as any NU in the SN that is able to relay messages between two units that cannot directly deliver messages to each other in any of the two directions. For a neighbor to be considered a PRNU, the connectivity in both directions needs to have a Link Status of at least ‘Good’.

In the example of Figure 3C.8-10, this is true for units 1, 3 and 4. For example, unit 1 needs to connect units 4, 5, 6 and 2. Similarly, unit 3 needs to connect units 4 to 2 and unit 4 connects 5 to 3. Initially NUs 1, 3 and 4 are defined as PRNU.

A **Reporting PRNU (RPRNU)** is a special type of the PRNU which is positioned to minimize injections to Totalcast or unknown destinations. A RPRNU is defined as a

PRNU which has a neighborhood that is not a proper subset of any other PRNU in the SN, as shown in Figure 3C.8-10. Each row of the table indicates all the neighbors it can reach. For this rule, a unit is considered a neighbor when CLRQ is equal to 1 or better. It can be seen in Figure 3C.8-10 that the neighbors of unit 3 and 4 are a subset of unit 1 neighbors. Therefore, unit 1 is promoted to RPRNU while unit 3 and 4 maintain the status of PRNU.

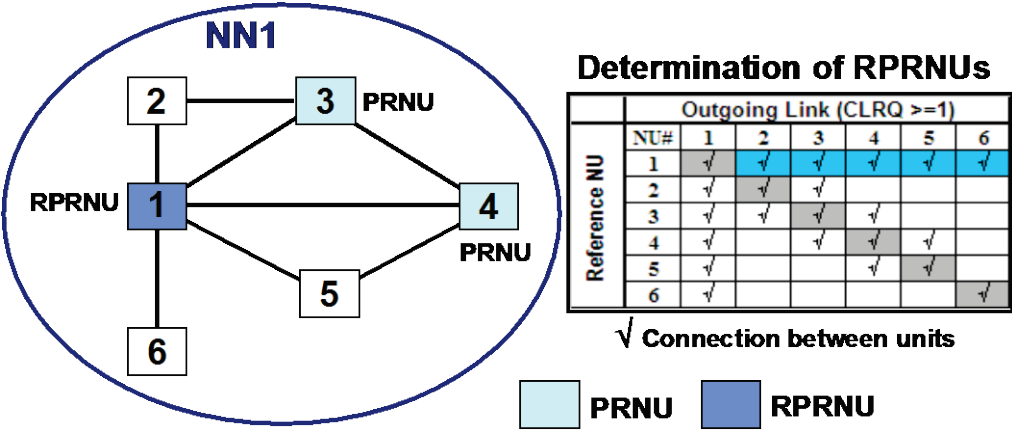


Figure 3C.8-10 Determination of PRNU and RPRNU

The check for PRNU and RPRNU is only performed on the LRQ information. The table part of Figure 3C.8-10 is internally called the “flat LRQ”, since it combines the multi-dimensional network connectivity in a single Super Network flat view. As a reminder, LRQ is limited to two legs. For PRNU computation, this rule considers only the list of reachable neighbors.

In the case of a tie in the number of neighbor units, the PRNU with the lowest NILE address is automatically selected as RPRNU among PRNUs with the same reachable destinations.

3C.8.4 Link Connectivity Data (LCD)

The Link Connectivity Data (LCD) represents the connectivity, “at least good connectivity” or “not connected,” between two NILE units bi-directionally and up to three legs away. The following aspects are further detailed.

- Link Connectivity Data Computation
- Link Connectivity Data Technical Messages

□ **Link Connectivity Data Computation**

Only the RPRNUs may need to generate a Link Connectivity Data (LCD) technical message to extend the connectivity knowledge up to three legs. In the above example (Figure 3C.8-10), all units are within 2 legs and no LCD is needed. All NUs will receive and store information in the LCD technical message, since the information is used to compute routing and relay. Figure 3C.8-11 shows two networks and illustrates how PRNU and RPRNU computations change. However, the concept is also valid if the units are all in the same network.

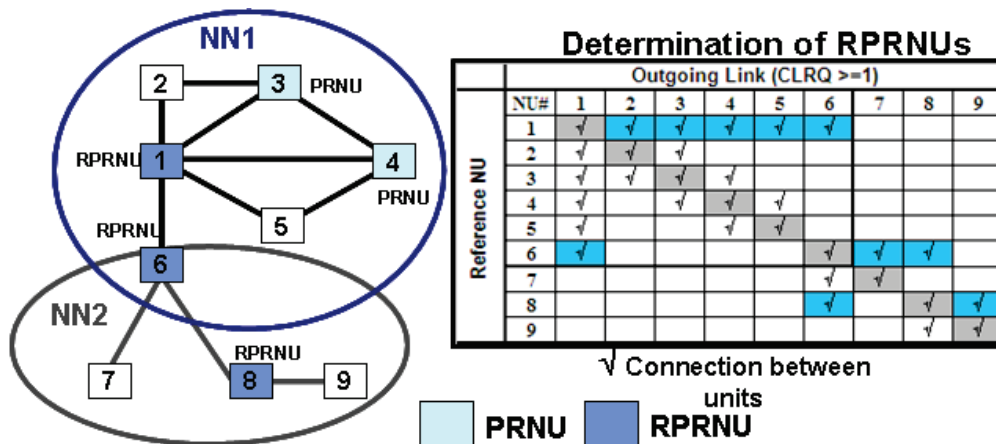


Figure 3C.8-11 Link Connectivity Data

In Figure 3C.8-11 unit 1 is still an RPRNU. Units 3 and 4 are still PRNUs. With the inclusion of NN2, unit 6 is now an RPRNU since its neighbor set is not included in the set of any neighbor. Similarly, unit 8 is also an RPRNU.

LCD messages are then generated, as detailed by the following summary rules.

- Only RPRNUs generate LCD technical messages
- LCDs are generated by the neighbor RPRNUs to allow the three leg knowledge to their own neighbors
- LCD messages include neighbors of the RPRNU which are at least GOOD in both directions based on LRQ Information
- Transmission occurs upon change and periodically to extend knowledge to silent or late entering units

Each RPRNU must check if LCD generation is required. In the example of [Figure 3C.8-11](#), unit 1 assesses that unit 2 has no knowledge of unit 7 and 8, which are neighbors of 6. Therefore, unit 1 generates an LCD technical message for Network 2, with reference RPRNU equal to 6, including 7 and 8 as bi-directional neighbors of unit 6. One LCD technical message per network needs to be generated, when required.

When LCD technical messages are received, the SNC maintains LCD tables that include all received LCD information, using RPRNUs as the row index and neighbor unit as the column index.

The SNC also computes an additional table called Flat Connectivity, which combines the multi-dimensional network connectivity in a single Super Network flat view. This includes connectivity information up to three legs. This table is also used to build routing tables.

□ Link Connectivity Data Technical Messages

There are 2 types of LCD technical messages that the SNC can transmit as indicated in [Figure 3C.8-12](#). These are selected based on the number of entries and the reason for transmission, so as to minimize bandwidth use.

Message	Fixed or Variable Length	Number of Entries	Usage
Standard LCD	Variable Length	1-15	Change or Periodical, if less than or equal to 15 entries
Compact LCD	Fixed Length	125	Change or Periodical, if more than 15 entries

Figure 3C.8-12 Link Connectivity Data Technical Messages

The standard LCD technical message also includes a Change/Complete flag, with the same meaning as described for the standard LRQ technical message. As for the LRQ technical messages, all LCD technical messages are generated for transmission every 5 minutes, after the start of each network and regardless of change, to offset loss of reception and to allow a unit joining the network to receive full connectivity information.

3C.8.5 Route Path Determination

Each unit builds routing tables to identify the best routes for all the units within three legs, by using the combination of LRQ and LCD information.

The routing protocol allows destinations to be reached with the least number of injections and with a reliable level of probability that the messages will be received. Routing answers the questions: where, how & how many times?

Routing selects the best three shortest paths to each destination, based on LRQ, LCD, PRNU, RPRNUs and their described tables. Each path is identified by a Routing Control Value (RCV). The path defines which of the neighboring unit(s) need to relay. The RCV has only 4 values (0-3). RCVs 1-3 are used to indicate which of the three paths was selected. Each NU uses the same process to compute its routing tables and therefore knows which path its neighbor is referring to with a specified RCV. RCV 0 is used to indicate limited flooding, which requires all RPRNUs to relay the message. If all destinations are within three legs, RCV 0 is not used for transmissions by the next relay unit.

In order to better optimize injection into multiple networks, the path number 1 shown in [Figure 3C.8-13](#) has to include an RPRNU for non-neighbor units. Therefore, if path number 1 is not the shortest path, the selections are modified to make sure path 1 includes the shortest path involving an RPRNU.

Paths are sorted based on the number of legs, also known as distance. First, all paths are sorted with distance two and then with distance three. Within the same distance, the lowest NILE address of the first unit on the path is used to sort the paths. If path number 1 does not include an RPRNU, sorting is performed to have path 1 include an RPRNU for the first leg. [Figure 3C.8-13](#) shows the 3 shortest paths from NU 1 to NU 6, after route determination and sorting.

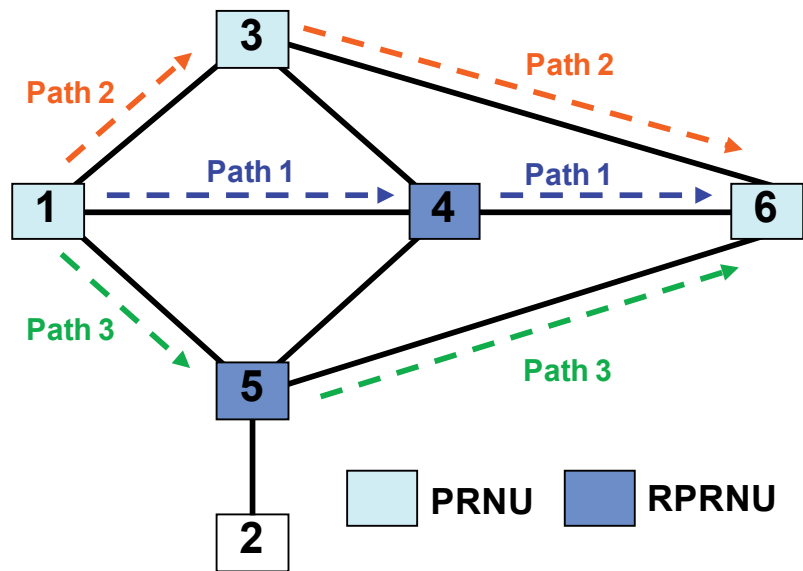


Figure 3C.8-13 Routing Path

Figure 3C.8-14 shows the sequences of paths before and after sorting, since the first path involves NU 3 which is not an RPRNU. This resulted in the swapping of paths 1 and 2, so that RPRNU unit 4 was included in path 1.

Path Number	RCV	Before Sorting	After Sorting
1	1	NU1 → NU3 → NU6	NU1 → NU4 → NU6
2	2	NU1 → NU4 → NU6	NU1 → NU3 → NU6
3	3	NU1 → NU5 → NU6	NU1 → NU5 → NU6

Figure 3C.8-14 Routing Path and Sorting

When one of the destinations that do not have an ‘Inactive’ status is beyond three legs, the SNC needs to compute a route that minimizes injections. As mentioned above, RPRNUs are defined to minimize injections. The SNC uses a “limited flooding” protocol in order to reach all RPRNUs and all the end nodes in the relevant networks. When relay is required, the RCV is set to 0, which means that only RPRNUs are eligible to relay the messages.

In Figure 3C.8-13, if unit 1 attempts to reach unit 12, which is more than three legs away, it will use RCV 0. Each injection by a relaying unit is independent of the

received RCV. Once any RPRNU has knowledge of all remaining destinations, the appropriate non-zero RCV will be used. Therefore, unit 2 and 3 may both relay using RCV 1 to reach unit 12.

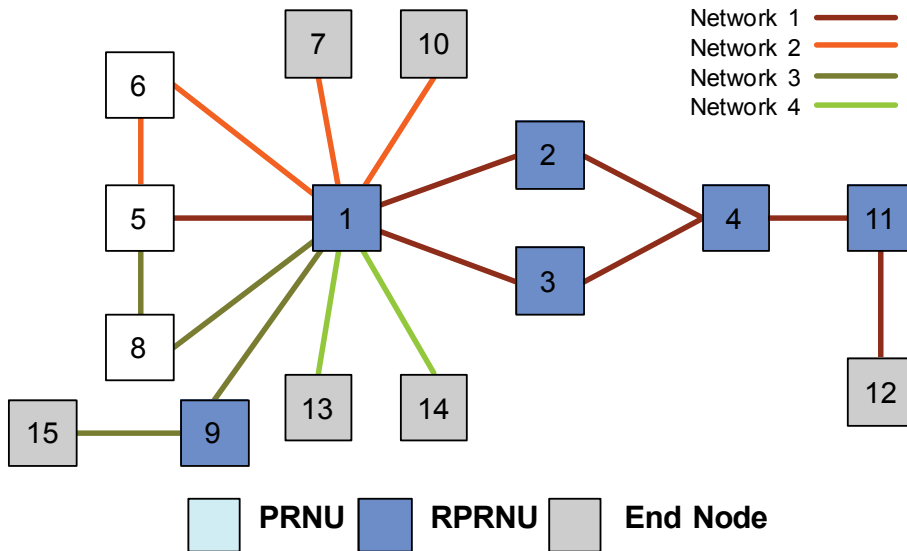


Figure 3C.8-15 Routing Example

A Relay service header includes routing information used to determine whether the message needs relaying and is not required if all the destinations in a network are neighbors. In [Figure 3C.8-15](#) when unit 1 is addressing unit 12, 13 and 14, transmission in network 4 to reach unit 13 and 14 only requires a non-relay service header, which is smaller in size.

3C.8.6 Probability of Correct Reception

For each injection in each network, the SNC computes how many times the transmission is required to achieve the required level of reliability. This does not apply to the case of Guaranteed Delivery, where repetitions are stopped when all addressees’ acknowledgements have been received or the maximum number of transmissions has been performed. [Figure 3C.8-16](#) defines the different levels of reliability.

Value	Description
Standard Reliability (STD)	Probability to be received on each leg equals 80%
High Reliability (HR)	Probability to be received on each leg equals 90%
Guaranteed Delivery	Repetitions based on the reception of acknowledgements

Figure 3C.8-16 Reliability Definition

The probability of correct reception is detailed in [\[SNC SS\] 3.1.2.3.4.5](#). The SNC utilizes the CLRQ information for this computation to assess the number of transmissions. If the message requires High Reliability (90%) and the CLRQ is 2 (Good, 80%), the SNC has to repeat the message twice to achieve the required probability. The probability of 80% is mathematically expressed as 0.8.

$$\text{Probability} = 1 - (1-0.8)^2 = 0.96 \text{ or } 96\% > 90\%$$

The above example does not consider the size of the message packet encapsulated in the Network Packet. If more than one fragment is required, a similar formula applies where the minimum number of repetitions is to be computed to reach the required level. The protocol only allows up to three transmissions (or two repetitions). [Figure 3C.8-17](#) highlights that if the probability is 80% on each leg, the combined probability to receive a message from two legs away decreases to 64%. When the unit is three legs away, the probability is 51.2%.

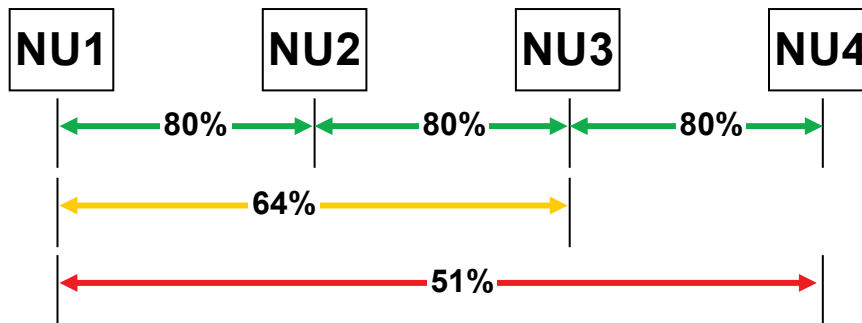


Figure 3C.8-17 Reliability Level after multiple injections

□ **Number of Transmissions and Number of Fragments**

The SNC determines the number of transmissions required and the number of fragments allowed, to meet the requested reception reliability (either Standard (80%) or High Reliability (90%)).

This protocol is called Leg Reliability, as it is performed independently for each required leg.

For each network that requires transmission, the SNC needs to consider the neighbor unit with the lowest probability of correct reception, which is represented by the CLRQ value.

A parameter that depends on message size and packing is the Message Packet to Network Packet (MP/NP) Ratio, which represents the minimum whole number of fragments required to inject a message packet. A message packet can be fragmented into more than the minimum number of fragments, but this reduces the probability of correct reception. Based on probability computation, the required level may be achieved using multiple fragments as long as it is not less than the requested minimum level. [Figure 3C.8-18](#) lists all the threshold cases for the different combinations.

In the following examples, the CLRQ is 3 and the required reliability is Standard.

If the NP is 168 bits and the message packet is 144 bits, the MP/NP Ratio is 1. The first row applies as the MP/NP ratio is less than or equal to the maximum number of fragments. Only one transmission is required. Since the Standard level requires 80% probability of reception, extending the number of fragments from 1 to 2 still exceeds the requested level of probability, but reduces the probability of reception from 99% to 81%. So if needed during packing, a maximum of two fragments can be generated.

If the NP is 168 bits and the message packet is 360 bits, the MP/NP Ratio is 3. This value is higher than the value in the 'Max Num of Fragments' column of the first row ($3 > 2$), so next row is considered, where two transmissions are required with a maximum of 5 fragments. As 3 (MP/NP Ratio) is less than 5 (maximum fragments) this row applies. The SNC can fragment the message from 3 to 5 and still satisfy the required level of probability ($83\% > 80\%$) with two transmissions.

CLRQ	Requested Reliability STD or HR	Minimum Number of Transmissions	Reliability Based on Minimum MP/NP Ratio	Max Num of Fragments	Achieved Probability
3 (0.9)	STD (0.8)	1	0.90	2	0.81
3 (0.9)	STD (0.8)	2	0.99	5	0.83
3 (0.9)	STD (0.8)	3	0.999	8	0.82
3 (0.9)	HR (0.9)	1	0.90	1	0.90
3 (0.9)	HR (0.9)	2	0.99	3	0.93
2 (0.8)	STD (0.8)	1	0.80	1	0.80
2 (0.8)	STD (0.8)	2	0.96	2	0.87
2 (0.8)	STD (0.8)	3	0.99	3	0.88
2 (0.8)	HR (0.9)	2	0.96	1	0.96
1 (0.6)	HR (0.9)	3	0.94	1	0.94
2 (0.8)	HR (0.9)	3	0.99	2	0.95
1 (0.6)	STD (0.8)	2	0.84	1	0.84

Figure 3C.8-18 Threshold Value for Probability Calculation

3C.8.7 Routing Selection

There are two different phases for route determination and both use the same route selection criteria. This section consists of the following subsections.

- [Route Prediction](#)
- [Route Production](#)
- [Selection Criteria](#)

□ **Route Prediction**

Route Prediction is the function used to identify all possible networks that could be used to reach the requested addressees. It selects a possible route based on the selection criteria. It also uses this route to update the congestion information. Route Prediction is performed when a Transmission Service Request (TSR) is received, and is periodically updated when a congestion refresh is performed, as detailed in [section 3C.9 Congestion](#).

□ **Route Production**

Route Production is performed when a transmission opportunity in a network occurs and the last route prediction identified the network as a possible solution. Route Production determines the routing solution for the network which is used in Network Packet production.

□ **Selection Criteria**

When more than one solution is available (in both route prediction and production), a set of criteria is used to determine the best route. The order in which the selection criteria apply is dependent on the priority of the message. The criteria and the order they apply for the different priorities are shown in [Figure 3C.8-19](#).

Priority 1-3	Priority 4
Maximum Coverage	Maximum Coverage
Minimum Delay	Maximize User Throughput
Maximize User Throughput	Minimum Delay
Maximize Reception	Maximize Reception
Random Selection	Random Selection

Figure 3C.8-19 Routing Selection Criteria

Each selection criteria listed in [Figure 3C.8-19](#) is discussed in the following sub-sections. Each solution includes transmissions in one or more networks. RCV values may be different, if needed at all. This depends on the units to be reached in the network. The routing also provides the information necessary to select the Service Headers to be used during each transmission in each network.

■ ***Maximum Coverage***

The first criterion of Maximum Coverage is satisfied by the way Routing tables are built and the use of RCV 0. This requirement implies that all destinations need to be included regardless of their relative position and the cost to reach each of them.

■ ***Minimum Delay***

If multiple solutions exist, the SNC considers the minimum delay based on the overall cost for each solution. Cost measures the overall delay added by the applicable network congestion at each involved unit. The SNC converts the congestion for a network into a delay by multiplying it by the Network Cycle Time. If the difference of the total cost between solutions is within 15% error margin, the solutions are considered to have the same cost and the next criterion is applied.

■ ***Maximize User Throughput***

If multiple solutions still exist, the SNC selects the solution that has the minimum number of injections, thereby maximizing the user throughput. The required reliability, the MP/NP Ratio and the CLRQ determines the number of injections required, as previously shown in [Figure 3C.8-18](#).

■ ***Maximize Reception***

If multiple solutions still exist, the SNC maximizes the reception by selecting the solution that reaches the maximum number of additional non-addressee neighbor units. This may allow more units to receive the message, even though they were not included in the original address list.

■ ***Random Selection***

If the above rules are not sufficient to select between multiple solutions, the SNC then performs a random selection among the solutions not eliminated by the above criteria. However, if this occurs during production and the network being served is one of the choices, the network is automatically selected.

3C.8.8 Message Relay

Each PRNU also computes the routing tables from the point of view of all its neighbors. A subset of this information is retained and identified as Routing Control Tables. This indicates for a given source-destination pair the PRNU that is required to relay the traffic for each value of RCV.

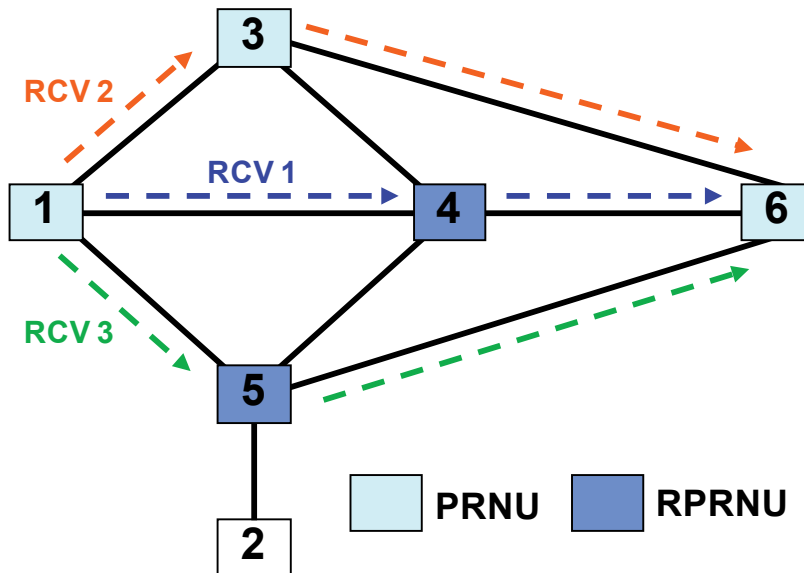


Figure 3C.8-20 Routing Path

In Figure 3C.8-20, NU 3, 4, and 5 receive the initial transmission from NU 1. If NU 1 selected RCV 1, NU 4 checks its Routing Control Table with unit 1 as reference for that value. It determines that it is the selected unit and must perform the relay. The message packet is queued for transmission if at least one destination needs to be reached (in this case NU 6). NU 3 and NU 5 will also check their Routing Control Table and will determine that RCV 1 means NU 4 will perform the relay. Therefore NU 3 and NU 5 will not relay the message.

The above rules allow for more than one unit to relay a message for the same set of destinations since each unit uses the local information to build the tables. This implies that more than one unit may assume that it has to relay, for a specified RCV.

When a message packet requires relay, a request is generated for its re-transmission. Relay stores the lists of destinations that still need to be reached, and the addressees contained in the received service header. This information is used to determine the addressees for the retransmission.

The SNC continuously monitors traffic and eliminates unnecessary transmissions if it determines that another PRNU has already injected the message packet to reach all the destinations that this unit would be attempting to reach. This is based on the duplicate detection algorithm and the connectivity information. When the same message packet is received more than once, the SNC updates the list of destinations that may have already received the message.

Another relay protocol rule is called equivalence. In the case of [Figure 3C.8-20](#), unit 3 and 4 are neighbors in all the connected networks. Therefore, they are considered equivalent and they both will queue for relay. If unit 3 relays the message, unit 4 will not relay it if a transmission has not yet occurred. This would also be the case if the transmission occurred due to missed connectivity updates.

Each intermediate relaying unit calculates independently the required path and may use different RCVs in different networks. The new RCVs may also be different from the received RCVs. If the relay transmission is only to neighbor destinations, no RCV is used as in the case of [Figure 3C.8-20](#) from unit 4 to unit 6.

Duplicate detection and relay protocols both work to avoid data looping.

3C.8.9 DLP Optimization

The DLP Operator has two ways of influencing connectivity and relay units

- [Change Relay Settings](#)
- [Link Quality Status](#)

■ Change Relay Settings

The DLP of the SNMU can elect to affect the PRNU and RPRNU computation by changing the relay setting of NUs by modifying the SN Directory. It does this by sending a 'Change Relay Settings' (31Ch) message to its SNC. This message can have one of three possible values for each unit, as listed in [Figure 3C.8-21](#). The SNC will distribute the message to all other NUs in the Super Network and inform its DLP of the acknowledgements it receives.

Value	Usage
Automatic	The SNC uses the above internal procedures to determine PRNUs and RPRNUs
Inhibited PRNU	The unit cannot become PRNU, regardless of its connectivity
Preferred RPRNU	If two units have the same number of neighbors, the preferred unit is selected as RPRNU, instead of the lowest NU index

Figure 3C.8-21 Relay Setting

■ **Link Quality Status**

The DLP can elect to affect the connectivity of units which cannot transmit by sending ‘Link Quality Status’ (328h) messages. Two units are involved, the destination unit and the passive unit. Figure 3C.8-22 shows the case of the SNMU notifying unit 3 that it has a passive receiving unit to reach. Unit 3 becomes RPRNU since it now needs to reach unit 5.

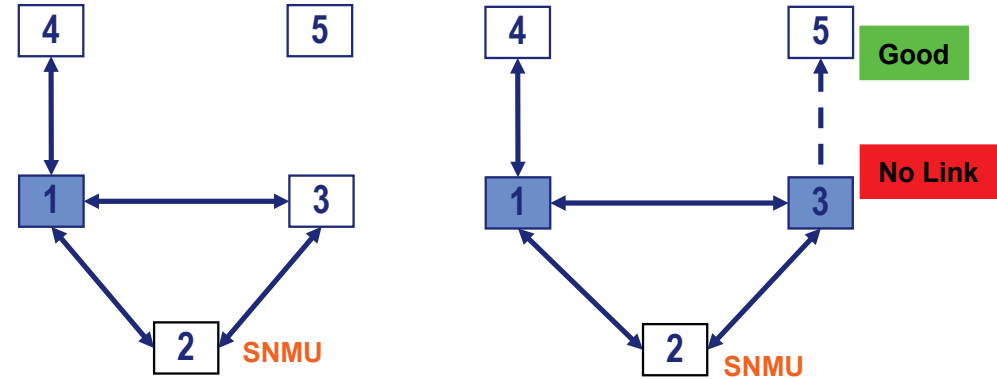


Figure 3C.8-22 Passive NUs

This protocol is shown in [Figure 3C.8-23](#). Unit 3 generates an LRQ technical message containing the new connectivity information, after receiving the instruction from the SNMU.

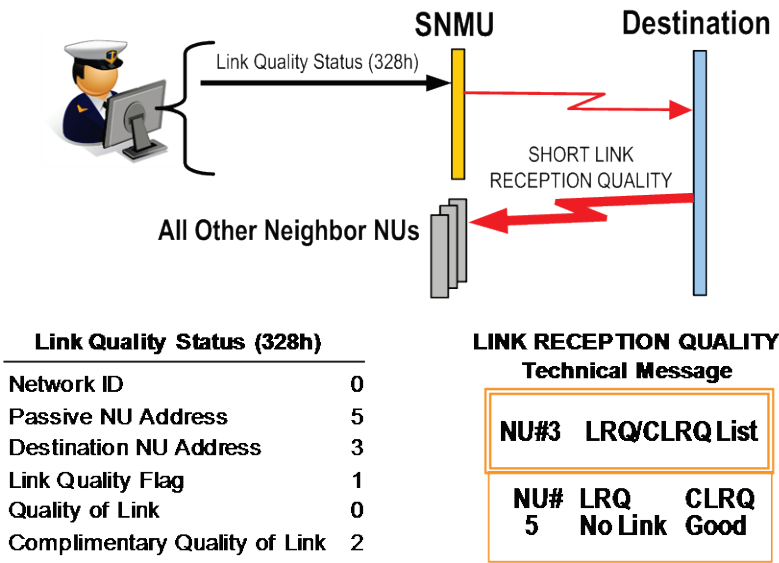


Figure 3C.8-23 Link Quality Status (328h) – Protocol

Unit 3 will then relay messages that have unit 5 as an addressee. Unit 5 will then be able to receive the messages where it was included as an addressee. This allows Radio Silence and Receive Only units to be able to receive addressed messages when relay is required.

If unit 5 starts transmitting, the passive link is automatically removed, and the actual LRQ values are used.

3C.9 Congestion

The SNC monitors the congestion and calculates the Congestion Values. The SNC uses this information when performing route calculations, and uses it to trigger both DTDMA (if enabled) and Relay Flow Control. The SNC also provides congestion information to its DLP and to its neighbors, who retransmit the information to their neighbors. These are described in the following subsections.

- Congestion Value Calculation
- Congestion Information Distribution

3C.9.1 Congestion Value Calculation

The SNC continuously monitors its congestion and computes a number called the Congestion Value, for each message priority on each network. The Congestion Values are internal to the SNC itself. A Congestion Value indicates how many NCTs (or fractions thereof) are required to transmit all the messages of a specific priority on a network. This includes transmitting all the messages of higher priority that need to be transmitted on the network. For each network the SNC maintains a total of the number of bits to be transmitted for each priority. The total is divided by the allocated capacity in the ONCS to produce the Instantaneous Congestion Value (ICV). In the following example figures the red, orange, yellow and green boxes represent the number of bits queued for each priority and the grey box represents the available capacity. The example in [Figure 3C.9-1](#) shows the lengths of the each of the priorities compared with the available capacity and their ICVs. It also shows that the ICV at each priority are cumulative, that is they include the values of the higher priorities.

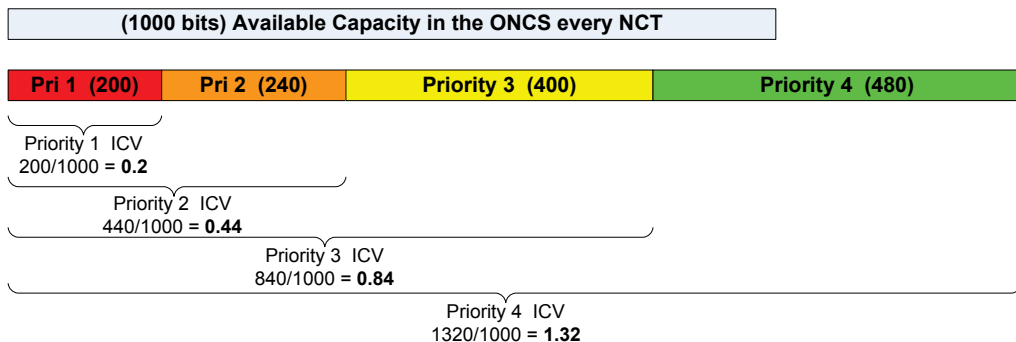


Figure 3C.9-1 Instantaneous Congestion Values per network

The Congestion Value is a filtered (smoothed) version of the ICVs. The SNC computes it using a digital low-pass Butterworth filter applied to the ICVs. This is to avoid making the system unstable or too sensitive to rapidly changing values. These filtered values are the ones used to trigger both DTDMA (if enabled) and Relay Flow Control. The Relay and Routing Management function also uses the filtered values when calculating a route.

Congestion calculations are performed periodically and are also performed when events happen that change the congestion. These events are the following.

- TSR Initial Route Prediction
- Periodical Prediction Update
- TSR Route Production
- Transmission Complete
- Priority Change and Cancellation
- ONCS Change

□ ***TSR Initial Route Prediction***

When the DLP, or internally the SNC, requests to transmit a message they produce a Transmission Service Request (TSR). When the SNC receives a TSR, it predicts all possible network combinations where a transmission is possible. It selects the lowest cost solution. Based on this assessment, the SNC adds the size of the message to the priority total for each predicted network.

The example shown in [Figure 3C.9-2](#) shows a new priority 2 TSR of 80 bits that is to be transmitted on only a single Network. The effect on the ICV for each priority is shown. It does not affect the priority 1 congestion, but does affect the others.

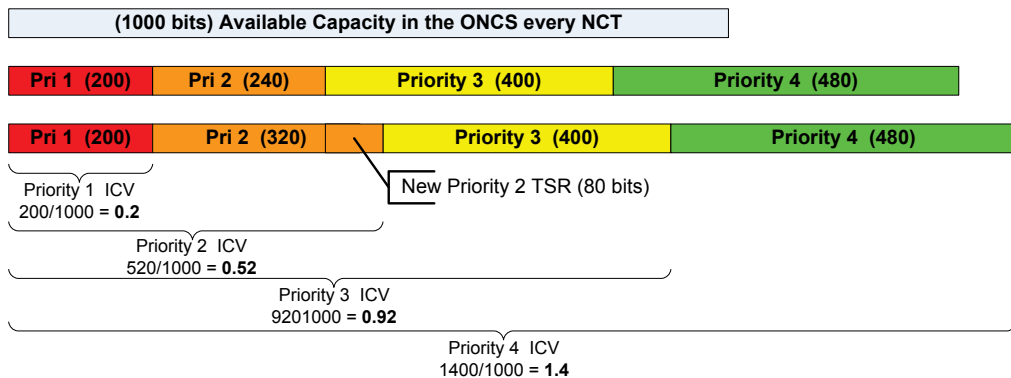


Figure 3C.9-2 Instantaneous Congestion Values affected by new TSR – Single Network

When the message needs to be transmitted in multiple networks, each network is updated independently, as shown in Figure 3C.9-3, where Network 2 and 6 are affected.

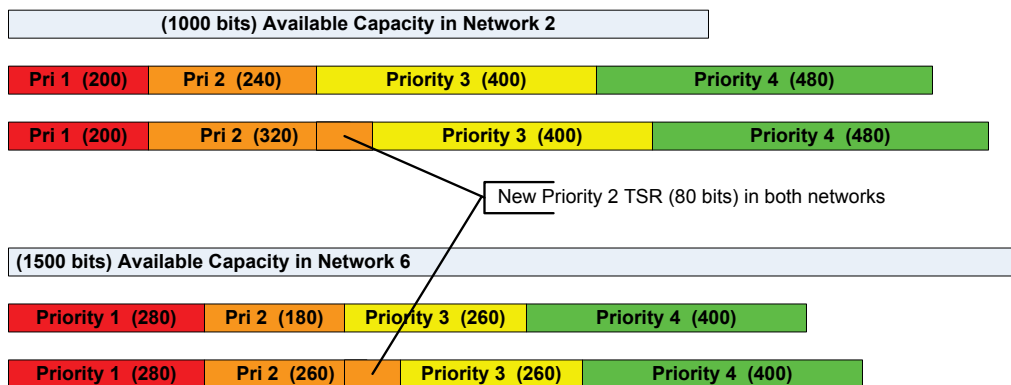


Figure 3C.9-3 New TSR needs to be transmitted on Multiple Networks

□ Periodical Prediction Update

Over time, the initial route prediction may become inaccurate. Therefore the SNC periodically (every 10 NCT) performs a new route prediction on the TSRs that are not being serviced and recalculates the Congestion Value. If multiple networks are active, the SNC selects the refresh based on the longest NCT.

□ ***TSR Route Production***

After the initial prediction, when a message can be transmitted in the network being served, an update is performed to assess if the networks indicated in the prediction are confirmed. Two cases are possible.

- Prediction and production affect the same Network
- Production differs from prediction for the eligible Network

In the first case, no changes are required. In the second case, the Congestion Values of the relevant network are updated to reflect the change in allocation.

□ ***Transmission Complete***

The SNC update the Congestion Values, after a message is transmitted and therefore removed from the TSR queue. The size of the message is removed from the networks indicated in the last prediction or production, when defined. This occurs after the end of each transmission timeslot within the ONCS.

□ ***Priority Change and Cancellation***

When the SNC receives a request to change the priority for a pending TSR, the Congestion Values for the two priority levels (old and new) are updated accordingly. When a request for transmission of a message is cancelled, the SNC also updates the Congestion Values.

□ ***ONCS Change***

Changes in the amount of capacity allocated to a unit on a network can occur when the unit is involved in a dynamic capacity reallocation or when the NMU changes the ONCS. When the amount of capacity allocated is changed, the Congestion Values for the network are updated. The values are updated by the ratio of the old allocated capacity to the new allocated capacity.

3C.9.2 Congestion Information Distribution

The Congestion Values calculated by the SNC (detailed above) are internal to the SNC only. For distribution of the congestion information, the SNC converts each filtered Congestion Value into a Congestion Index (0-3), which indicates the level of congestion from none to severe. The meaning of each congestion index is shown in [Figure 3C.9-4](#).

Index	Meaning
0	No Congestion
1	Light Congestion
2	Moderate Congestion
3	Severe Congestion

Figure 3C.9-4 Congestion Index

Each congestion index represents a range of Congestion Values. The range of values varies depending on the priority. The range of the Congestion Value (CV) represented by the congestion index for each priority is shown in [Figure 3C.9-5](#).

Index	Priority 1	Priority 2	Priority 3	Priority 4
0	CV ≤ 0.5	CV ≤ 0.8	CV ≤ 1.5	CV ≤ 2.0
1	0.5 < CV ≤ 0.7	0.8 < CV ≤ 1.5	1.5 < CV ≤ 2.5	2.0 < CV ≤ 3.5
2	0.7 < CV ≤ 1.0	1.5 < CV ≤ 2.0	2.5 < CV ≤ 3.0	3.5 < CV ≤ 4.0
3	CV > 1.0	CV > 2.0	CV > 3.0	CV > 4.0

Figure 3C.9-5 Congestion Conversion by Priority

The SNC distributes congestion information to its DLP and to other units in the following ways.

- Congestion Alert
- CONGESTION INDEX Technical Message
- NU Performance

□ **Congestion Alert**

For each active network at the end of each NCT, the SNC sends a ‘Congestion Alert’ (603h) message to its DLP, which contains the Congestion Index for each priority.

This allows the DLP to maintain a knowledge and history of its own level of congestion. The DLP may monitor the congestion level and may adjust the number of tactical message transmission requests it sends to the SNC, to control the congestion level.

□ **CONGESTION INDEX Technical Message**

The SNC uses the CONGESTION INDEX technical message to distribute the congestion index information. Whenever there is a change in any Congestion Index value for a network, the transmission rules for the CONGESTION INDEX technical

message are reassessed, according to the rules listed in [Figure 3C.9-6](#). This technical message is transmitted in a special way to reach all the neighbors and their neighbors (two legs). This is achieved by the SNC transmitting the message as Totalcast for the first leg, and all receiving relay units re-transmit the message, converting the addressing type to neighborcast.

Condition	Transmission rules
The congestion index for at least one priority is three	Every five NCTs with priority one
The congestion index for at least one priority is three and none of the congestion index is greater than two	Every ten NCTs with priority two
The congestion index for at least one priority is three and none of the congestion index is greater than one	Every fifteen NCTs with priority three
The congestion index for at least one priority changed from greater than zero to zero and now all priorities are zero	Transmit in three different timeslots with priority three

Figure 3C.9-6 Congestion Values Transmission Rules

When a unit receives a CONGESTION INDEX technical message the information in the message is stored. The SNC maintains a Congestion Table which contains the Congestion Index for each priority on the network, for all units and all networks.

When the SNC does not receive a new CONGESTION INDEX technical message for a network from a unit for more than 20 NCTs, it resets to zero the stored values for the network for that unit.

These stored values are used by Routing and Relay in the calculation of possible routes.

□ NU Performance

Every unit periodically sends a NU PERFORMANCE technical message to the SNMU, its standby, and the NMU and its standby for all networks the units is active on. The technical message contains the highest priority that has been congested since the previous transmission of the technical message. If the unit does not know the connectivity (such as in the case where a network has just initialized), the SNC transmits the message using Totalcast.

When the NU PERFORMANCE technical message is received, the SNC sends the information to its DLP by sending a ‘NU Performance Data’ (427h) message. This provides the DLPs with congestion information about other units.

3C.10 Message Delivery & Reliability

This section details the message delivery protocols and the requirements that affect them. It comprises the following subsections.

- Perishability
- Reliability
- Message Delivery Protocols

3C.10.1 Perishability

A tactical TSR (from the DLP) or technical TSR (internal to the SNC) specifies the Perishability of a message, which defines how long its data is valid. Choices are 15, 31 and 63 seconds, and non-perishable (511 seconds).

Technical messages are all non-perishable. The Perishability to be used for tactical messages is defined in [STANAG 5522]. The purpose and content of a tactical message affects the choice of Perishability; an example of each is given in the following list.

- Short (15 seconds) - Air Track Reports
- Medium (31 seconds) - Track Management messages
- Long (63 seconds) - Surface Track Reports
- Non-Perishable - Track/Point Amplification messages

Perishability is used by Relaying NUs to determine whether the data within a message is still valid and therefore still needs be relayed. All perished messages are deleted from the TSR queue. Even Non-perishable messages age, and will be discarded by a Relay if the message is over 511 seconds old.

3C.10.2 Reliability

A tactical or technical TSR also specifies the required reliability for the transmission of the message, using one of the following options.

- Standard - 80% probability of reception
- High Reliability - 90% probability of reception
- Guaranteed Delivery

Standard and High Reliability applies to both Non-MR and MR addressing, but Guaranteed Delivery only applies to MR.

The use of Reliability for tactical messages is defined in [STANAG 5522]. The use of Reliability for technical messages is detailed in [SNC SS] Appendix B and in section 3C.15. The purpose and content of a message affects the choice of Reliability. For example, High Reliability is used for the initial report of surveillance tracks, whereas Standard Reliability is used for surveillance track updates, ID change, and IFF update. An example of the use of GD is the Engage Command tactical message.

□ **Standard and High Reliability**

The Probability of Reception for Standard and High Reliability is achieved by transmitting the message multiple times (1-3). All transmissions do not have to be made in the same timeslot. Only a single transmission is allowed within an individual network packet. The number of transmissions is calculated from the required reliability and the current reception probability for the destination NUs, as detailed in section 3C.8.6 [Probability of Correct Reception](#). The Reliability removes the need for the DLP to make redundant transmissions.

□ **Guaranteed Delivery**

Guaranteed Delivery attempts to provide approximately 100% probability of reception, but cannot actually guarantee the delivery. The TSR originator is responsible for determining the required action if delivery of messages is not acknowledged. GD is similar to MR, in that both use acknowledgements.

3C.10.3 Message Delivery Protocols

A TSR contains two address groups, as detailed in section 3C.5 [Addressing](#), which are the following.

- [Non-Machine Receipt](#)
- [Machine Receipt](#)

The purpose and content of a message affects the choice of Addressee Group. Both Non-MR and MR Address Groups can be used in the same TSR. For example, when the SNC is instructed by the DLP to transmit a 'Radio Silence Order' specifying that an individual NU is to go Radio Silent on all networks, the SNC will transmit an ORDER technical message, addressed as follows.

- MR Point-to-Point to the individual NU
- Non-MR Totalcast to all other NUs

The reference [STANAG 5522] does not require any tactical messages to use both MR and Non-MR Addressing at the same time.

A TSR must always specify at least one of these Addressee Groups, and may specify both. If both are specified then the message delivery protocol for MR Address group is used. There is no difference between GD and MR as far as the TSR originator is concerned. When the TSR specifies GD, the MR Address group must be specified.

□ **Non-Machine Receipt Address Group**

Non-MR Message Delivery is used when there is no MR Address group requested. Non-MR is relatively simple as there are no acknowledgements required. The message is just transmitted the required number of times to achieve the requested level of reliability (Standard or High). The transmission does not include any MR Addressee information, so that the receiving units know not to acknowledge the message. Received technical messages are delivered internally within the SNC and received tactical messages are delivered to the DLP. The SNC informs the TSR originator (the DLP for tactical TSRs, or internal in the SNC for technical messages) when the transmissions are completed, and this indicates that the processing of the TSR is complete. The message flows are shown in Figure 3C.10-1 for a tactical TSR.

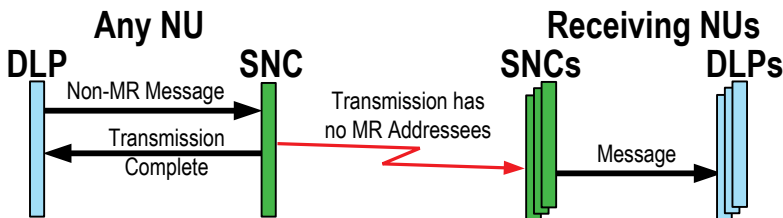


Figure 3C.10-1 Non-Machine Receipt (Non-MR) Protocol

□ **Machine Receipt Address Group**

When MR Addressees are specified, the Message Delivery is more complicated and involves the transmission of acknowledgements by the addressees, and the delivery of the acknowledgements to the TSR originator, as shown in Figure 3C.10-2 for a TSR originated by the DLP.

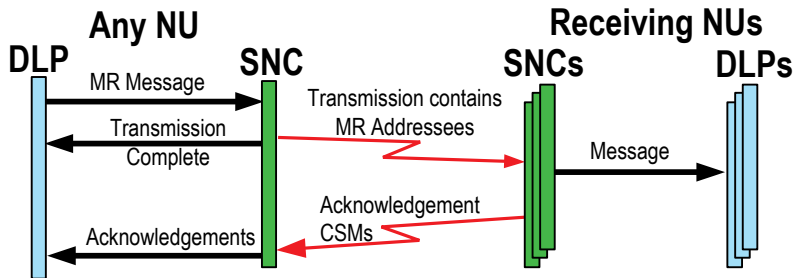


Figure 3C.10-2 Machine Receipt (MR) Protocol

The SNC of each Receiving NU responds with an acknowledgement Communications Service Message (CSM) on receipt of the message. The originating SNC informs the TSR originator when all the transmissions have been completed, and also provides any received acknowledgements. Processing of a TSR is complete after transmissions are complete and the originating SNC informs the TSR originator that there are ‘No Further Acknowledgments’.

When Machine Receipt addressees are requested, the following three Message Delivery protocols are used. The protocol used depends on the addressees and the conditions associated with each protocol; the first protocol in the list that meets the conditions is used.

- **Leg Acknowledged Delivery** – All Addressees are RF Neighbors
- **Machine Receipt** – Standard/High Reliability
- **Guaranteed Delivery** – GD Reliability

Machine Receipt (MR) and Guaranteed Delivery (GD) protocols are normally associated with Non-perishable messages, as the protocols time out (complete) after four minutes and the other perishability values are 63 seconds or less.

It is not recommended to use both GD and Non-MR Addressee Groups at the same time because GD takes precedence and the Non-MR addressees may not all receive the message.

The following subsections describe the protocols and the examples given relate to units that are connected as shown in [Figure 3C.10-3](#).



Figure 3C.10-3 Connectivity for the Examples that follow

■ *Leg Acknowledged Delivery*

The Leg Acknowledged Delivery (LAD) protocol is used when all the MR addressees are RF neighbors of the transmitting unit, and is also used by Guaranteed Delivery. The source unit transmits the message on all networks required to reach the addressees, and waits for a Leg Acknowledgement CSM from each of the addressees. The SNC automatically makes retransmissions on any Network that routing calculates is needed to reach the addressees from which a positive Leg Acknowledgement CSM has not been received. Retransmissions made on a Network are made in a timeslot at least one Net Cycle Time after the Timeslot Time of the previous transmission, to allow time for the Acknowledgements to be received. The SNC terminates transmissions when all acknowledgements have been received, or when two retransmissions per network have been made, or one minute after the time of the first transmission is reached. Retransmissions are addressed only to those units that have not acknowledged the message. Two retransmissions are allowed to occur if there is time. The source stops waiting for CSMs (the protocol times out) one minute after the time of the last transmission. This means that the maximum length of the protocol is two minutes.

The LAD protocol uses a Leg Message Packet Reference Number (Leg MPRN) to identify the message packet (containing the message), so that the Leg Acknowledgement CSM only needs to use the Leg MPRN, and the NILE Address of the unit that transmitted it, to identify which message packet is being acknowledged. This makes the CSM small, thereby minimizing the total bandwidth used by all the addressees in acknowledging the message packet. To further save bandwidth the Leg MPRN is only 5 bits long (0-30), which under normal conditions is sufficient. If more than the 31 values are needed, a value of 31 is used and then an additional 5-bit extension field (0-31) is added to the first field value (31) to produce the Leg MPRN. The Leg MPRN has 62 values, so there is a limit of 62 LAD protocols that can be in progress at the same time for a unit. A Leg MPRN cannot be reused until the protocol has timed out (completed).

In the example shown in [Figure 3C.10-4](#) NU2 transmits to NU1 and NU3 (black line). NU1 does not receive the transmission. NU3 receives the message and transmits a Leg Acknowledgement CSM back to NU2 (red line), which NU2 receives. NU2 does not receive a CSM from NU1 within one NCT, so it retransmits the message as long it is less than one minute from the time of the first transmission. NU1 receives the message this time and transmits a Leg Acknowledgement CSM back to NU2. NU2 does not receive the CSM within one NCT, and so it retransmits the message again (time

permitting). NU1 receives the message again and transmits a Leg Acknowledgement CSM back to NU2, which NU2 receives.

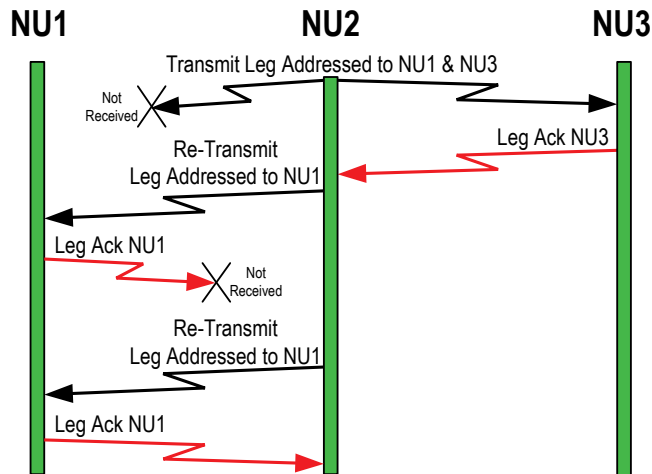


Figure 3C.10-4 Leg Acknowledged Delivery (LAD) Protocol

■ Machine Receipt

The Machine Receipt (MR) protocol is used when MR Addressees and Standard or High Reliability are requested, and at least one of the addressees is not an RF neighbor (relay is required). Only the source unit has to perform any special protocol. The addressed units only have to transmit the MR Acknowledgement CSM to the source. Units perform their normal relay retransmissions to reach the specified destinations. The relay of the message packet and the returning CSM can take different paths. The relaying depends on connectivity and congestion as detailed in section 3C.8 [Relay & Routing](#). Every transmission may be repeated to achieve the required level of reliability (Standard or High).

The MR protocol uses an End-to-End Reference Number (E2ERN) to identify the message packet to all addressees. The addressees use the E2ERN in the MR Acknowledgement CSM that they transmit to the source. The E2ERN is associated with the MTV of the message packet and has only eight values, and therefore there is a limit of eight MR protocols per second per source NU.

In the example shown in [Figure 3C.10-5](#) NU1 addresses message packet (MP1) to only NU4. NU1 transmits the message packet addressed to NU4 (black line) which is

received by NU2. NU2 relays the message packet to NU3. Similarly, NU3 relays the message packet to NU4. NU4 transmits a MR Acknowledgement CSM to NU1 (blue line), which in this example has to be relayed by NU3 and then NU2 to reach NU1. It can be seen that there are no acknowledgements from NU2 or NU3.

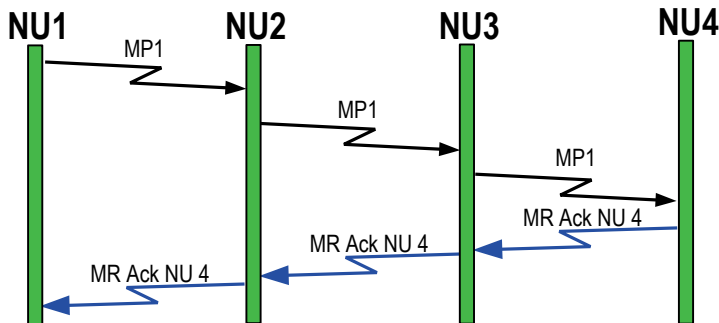


Figure 3C.10-5 MR Protocol to NU4 only

If NU1 addresses the message packet to NU2, NU3 and NU4, then the message flow is as shown in the example in Figure 3C.10-6. NU1 transmits the message packet addressed to the three units (black line) which is received by NU2. NU2 transmits a MR Acknowledgement CSM to NU1 (dark green line). NU2 relays the message packet to NU3. Similarly NU3 transmits a MR Acknowledgement CSM to NU1 (light green line), which has to be relayed by NU2 to reach NU1. NU3 relays the message packet to NU4. Similarly NU4 transmits a MR Acknowledgement CSM to NU1 (blue line), which has to be relayed by NU3 and then NU2 to reach NU1.

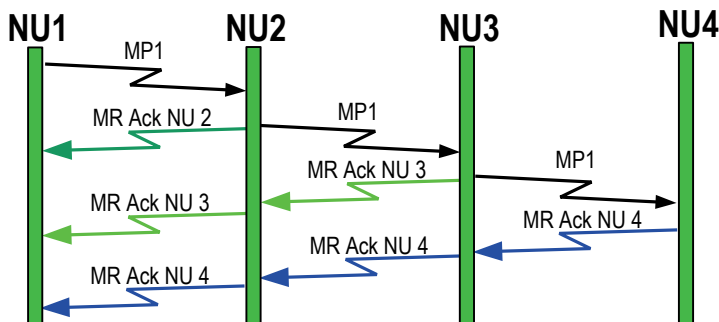


Figure 3C.10-6 MR Protocol to NU2, NU3 & NU4

The difference between the two examples is that NU2 and NU3 transmit MR Acknowledgement CSM to NU1 (green lines).

■ *Guaranteed Delivery*

The Guaranteed Delivery (GD) protocol is used when MR Addressees and GD reliability are requested, and at least one of the addressees is not an RF neighbor (relay is required). The source transmits the message packet with a service header containing the MR Addressees and the Leg Addressees. The Leg Addressees are the MR Addressees and any other units that have to relay the message, which are neighbors in the network.

Successful delivery of a message using the GD protocol will result in the source receiving Leg Acknowledgement CSMs from the Leg Addressees, and Delivery Acknowledgement CSMs from all other non-neighbor addressees.

The units that have to perform relay when performing GD protocol are referred to as Reliable Relayers, and they may also be addressees. A Reliable Relayer performs the LAD protocol with its RF neighbors that are needed to reach its subset of the addressees, and sends Delivery Acknowledgement CSMs or Delivery Failure CSMs to the source (via relay if necessary) to notify it of the success or failure to receive acknowledgements from its subset of the MR Addressees. When this has been completed, or the GD protocol has timed out, the GD protocol on the Reliable Relayer is complete. The source unit waits to receive all the Delivery Acknowledgement or Delivery Failure CSMs from the Reliable Relayers, or until the protocol times out, which is four minutes after it starts. Reliable Relayers will not perform any actions if the GD protocol has timed out on the source.

As the Guaranteed Delivery protocol uses the LAD protocol for each leg, the restriction on the number of LAD protocols above also applies to GD for each leg. The Leg MPRN used by the source is only used on the first leg. On additional legs, the Reliable Relayer uses one of its own Leg MPRNs for its retransmission. The GD protocol also uses an E2ERN for the Reliable Relayers to identify the message packet in the CSMs that they transmit to the source unit, so the limits on the E2ERNs also apply to GD.

In the example shown in [Figure 3C.10-7](#) NU1 addresses message packet (MP1) to only NU4. NU1 uses the LAD Protocol (black line) to NU2, which as part of the LAD protocol returns a Leg Acknowledgement CSM to NU1 (red line). Similarly NU2 uses LAD Protocol to NU3 which returns a Leg Acknowledgement CSM to NU2. Similarly NU3 uses LAD Protocol to NU4 which returns a Leg Acknowledgement CSM to NU3. NU3 sends the acknowledgement from NU4 to NU1 using a Delivery Acknowledgement CSM (blue line). In this example the CSM has to be relayed by NU2 to reach NU1, but it may take other paths if available.

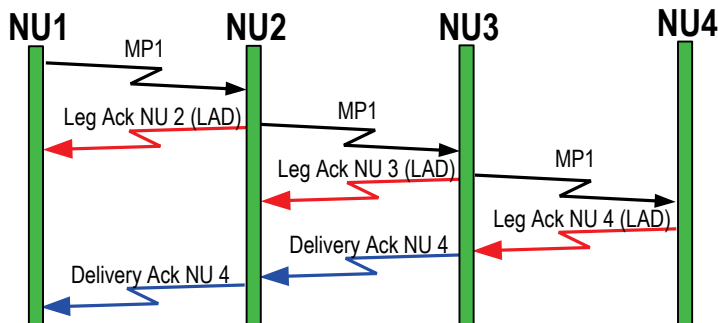


Figure 3C.10-7 GD Protocol to NU4 only

If NU1 addresses the message packet to NU2, NU3 and NU4, then the message flow is as shown in the example in [Figure 3C.10-8](#). The only difference between this and the previous example is that NU2 sends the acknowledgement from NU3 to NU1 using a Delivery Acknowledgement CSM (green line).

NU2 queues the Delivery Acknowledgement CSM containing NU3's acknowledgement for transmission when it receives the Leg Acknowledgement CSM from NU3. If it receives the Delivery Acknowledgement CSM for NU4 before it has transmitted the Delivery Acknowledgement CSM for NU3 it will combine them into one CSM. If it does not, then NU2 has to wait for a period of time (to collect more acknowledgements) before transmitting the next Delivery Acknowledgement CSM, unless the CSM is the last one and then it is queued immediately. In this case the one for NU4 is the last one and so will be queued for transmission immediately.

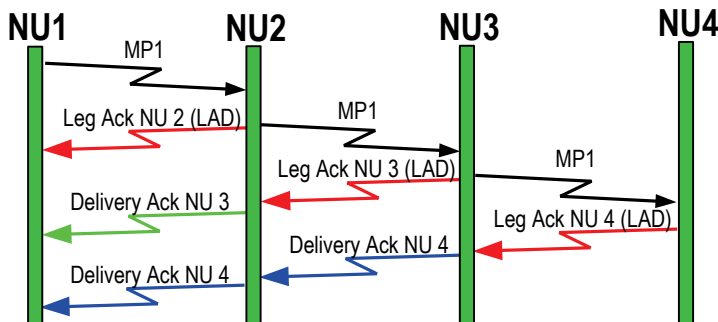


Figure 3C.10-8 GD Protocol to NU2, NU3 & NU4

3C.11 SNC Packing

Link 22 communicates tactical and technical messages. Tactical messages are discussed in [Chapter 2 Section D](#) and officially defined in [STANAG 5522]. Technical Messages are used to communicate management information between SNCs and are listed in section [3C.15 Technical Messages](#). The transmission of the tactical and technical messages is based on quality of service requirements as indicated by the DLP for tactical messages, or for technical messages defined by the SNC in accordance with [SNC SS] Appendix B. Messages with the same quality of service requirements can be grouped together. Message Packets (MPs) are used to contain the service requirements and messages, as discussed in section [3C.11.2 Message Packet Structure](#). MPs and/or fragments of MPs are placed into NPs for transmission.

The role of SNC Packing is to produce the Network Packets (NPs), which is accomplished by assembling together the information that needs to be transmitted, while obeying the rules governing the structure of NPs. All rules are deterministic and as long as the rules are applied, the NPs will have a correct structure. When these NPs are then received, it will be possible to unpack them and extract the transmitted information using the knowledge of the structure rules. The SNC packs all the NPs in a timeslot at the same time. Continuation Fragmentation allows the SNC to pack information across adjacent NPs. This section consists of the following subsections.

- [Network Packet Structure](#)
- [Message Packet Structure](#)

In this section, the figures use the darker blue for mandatory fields and the lighter blue for the optional ones.

3C.11.1 Network Packet Structure

A Network Packet consists of a Header and Data as shown in [Figure 3C.11-1](#).

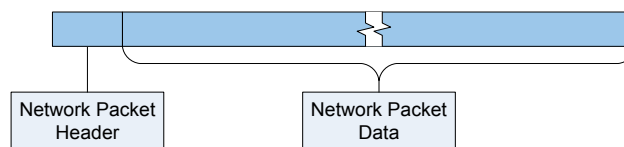


Figure 3C.11-1 Network Packet Structure

□ **Network Packet Header**

The structure of the Network Packet Header is shown in [Figure 3C.11-2](#). Link 22 currently only uses full capability packing so the first bit of the header, the Network Packet Type, should always be one. If the Explicit Source Identification Flag bit is one, then the next seven bits contains the Explicit Source Identification, which is the NILE Address of the unit that transmitted the NP. If the Explicit Source Identification Flag bit is zero, then the optional field is not included in the header. The next bit is the DTDMA Control Flag, which is always present and is used by the DTDMA protocol. The last bit is the Continuation Flag, which when set to one, indicates that the beginning of the NP Data contains a continuation from the previous NP in the same timeslot. The NP header is therefore either 4 or 11 bits long, depending on the second bit.

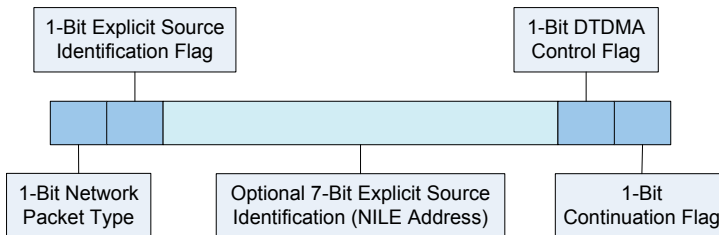


Figure 3C.11-2 Network Packet Header Structure

□ **Network Packet Data**

The NP Data consists of three optional parts as shown in [Figure 3C.11-3](#). The Continuation Data part (contains the continuation of a MP) is only included if the NP Header Continuation Flag bit is set to one. The first NP in a timeslot cannot start with Continuation Data. The optional Data part is where the MPs are inserted. This part is optional as it may be empty (for example, when there are no messages to be transmitted). The optional padding part is only included when there is space left at the end of the NP.

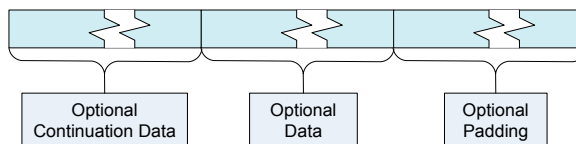


Figure 3C.11-3 Network Packet Data Structure

□ **Optional Continuation Data**

The structure of the Continuation Data as shown in [Figure 3C.11-4](#) depends on the length of the NP.

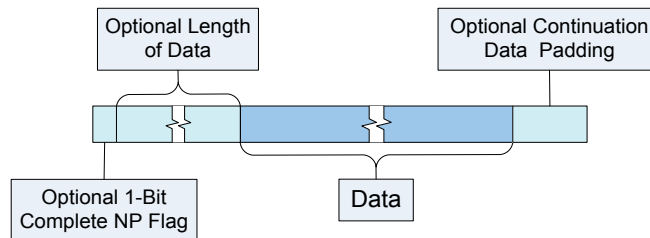


Figure 3C.11-4 Structure of Continuation Data

Optional Complete NP Flag: The optional Complete NP Flag is included only when NP size is < 200 bits, which occurs only in the first two cases listed in [Figure 3C.11-5](#). When the flag is included, it is set to one if the Length of Data field and the remaining continuation data will not fit in the NP. If just the data will fit, then there can be a few bits unused at the end of the NP (less than the size of the Length of Data field). If the data is larger than the NP space, then all the space is used and the remaining data is continued on into the next NP. This saves the space used by the Length of Data fields when a large amount of data fills many small NPs.

Optional Length of Data: The optional Length of Data field is included when the NP size is > 200 bits, or when the Complete NP Flag is zero. The number of bits used for the Length of Data field (7-10 bits) is proportional to the length of the NP, as listed in [Figure 3C.11-5](#).

Data: The Data field is the continuation of the Message Packet to be transmitted.

Optional Continuation Data Padding: The optional Continuation Data Padding is included only if the Complete NP Flag is set to one, and the data does not fill up the entire NP. When the NP size is 96 bits, the number of bits used by the Length of Data field is seven bits, and when the data fills up the NP there are 0-6 bits of padding. Similarly, when the NP size is 168 bits, the Length of Data field is eight bits, and when the data fills up the NP there are 0-7 bits of padding.

NP Size	Bits in Length of Data	NP Size	Bits in Length of Data	NP Size	Bits in Length of Data	NP Size	Bits in Length of Data
96	7	384	9	608	10	936	10
168	8	456	9	624	10	1152	10
240	8	464	9	720	10	1216	10
312	9	480	9	768	10	1368	10
336	9	504	9	912	10	1824	10

Figure 3C.11-5 Number of Bits in Length of Data Field per NP Size

□ **Optional Data**

The Optional Data part is where the message packets or fragments are inserted. There are two types of fragments: continuation fragments and leg fragments. Continuation fragments are used for MP fragments split across adjacent network packets in the same timeslot. The leading continuation fragment is placed at the end of the Data part in a NP (with no padding), and the continuation fragment is packed at the beginning of the next NP Data, as described in [Optional Continuation Data](#) above. Similarly, the first Leg Fragment (Leading Leg Fragment) of a MP has to be packed at the end of a NP. The remainder of the MP (whole or further divided), called supplementary leg fragments, can be inserted in the unused space in a NP or can be held over for later transmission in another timeslot. The structure of the Data part is shown in [Figure 3C.11-6](#).

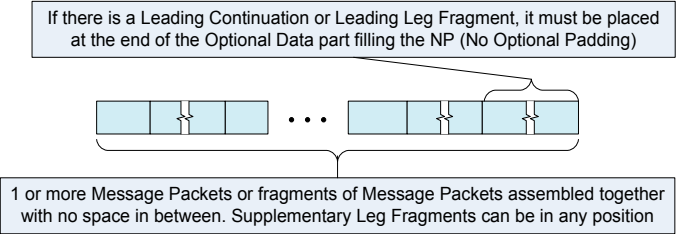


Figure 3C.11-6 Structure of Optional Data

❑ **Optional Padding**

The optional padding is used to fill any remaining space at the end of a NP. When the remaining space is at least six bits long, this is formed by inserting a Padding CSM (see [Communication Service Message \(CSM\) Structures](#) in section 3C.11.2), into the NP which uses all the remaining space. The 6 bit Padding CSM header indicates the start of the padding, which is then followed by the CSM contents a variable length (zero or more bit) NP Authentication Code, calculated from the used NP contents. If there are less than 6 bits of space the CSM header will not fit and the space is filled with a NP Authentication Code of length equal to the remaining space (1-5). The structure of the optional padding is shown in [Figure 3C.11-7](#).

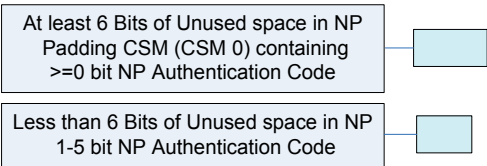


Figure 3C.11-7 Optional Padding Structure

3C.11.2 Message Packet Structure

Message Packets consist of a Service Header followed by a Data Unit, which contains zero to three messages, as shown in [Figure 3C.11-8](#) (only Service Header 7 contains no Data Unit). Within a Message Packet, all the Messages are either Tactical or Technical. They are not mixed and they all have the same Service Header requirements.

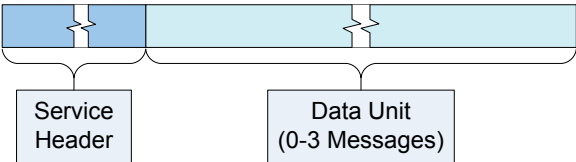


Figure 3C.11-8 Message Packet Structure

□ **Service Header**

Service Headers contain the message delivery information that is required to process the associated message data. Service Headers contain a 3-bit Service Header Identifier, followed by the variable length Service Header Contents, as shown in [Figure 3C.11-9](#).

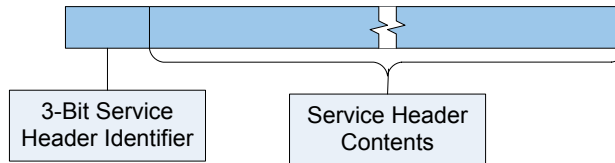


Figure 3C.11-9 Service Header Structure

There are eight Service Headers (0-7), which may only be used for specific purposes as listed in [Figure 3C.11-10](#). There is a pair of Service Headers for each of the first three usages. The first of the pair is a short Service Header that provides only the mandatory data, not all of the message delivery information, to use the minimum possible bandwidth. The second of the pair is the extended Service Header that supports all the message delivery information and is longer than the short Service Header. Service Header 6 is only used for Supplementary Leg Fragments, when Leg Fragmentation is used. Service Header 7 is a technical Message Packet without a Data Unit (just a Service Header), which is referred to as a Communication Service Message (CSM). The structure of the CSMs is defined in section [Communication Service Message \(CSM\) Structures](#).

Service Header	Usage
0 and 1	Initial transmission of a MP that is not required to be relayed by any neighboring NU on the Network on which it is injected
2 and 3	Initial transmission of a MP when relay is required
4 and 5	Retransmission of a received MP by a relaying NU
6	Transmission of the additional fragments of a MP (not the first) (Leg Fragmentation)
7	Transmission of a Communication Service Message (CSM)

Figure 3C.11-10 Service Header Usage

The message delivery information that can be included in each of the Service Headers (0-5) is listed in [Figure 3C.11-11](#).

Message Delivery Information	Service Header Number					
	0	1	2	3	4	5
Message Delineation Group	Y	Y	Y	Y	Y	Y
MR Group		X	S	S	S	S
Relay Control Group			Y	Y	S	S
Perishability			Y	Y	Y	Y
MP Age	I	S	I	S	E	E
MP Originator	I	I	I	I	E	E
Data Originator Group	I	S	I	S	I	S
Leg Delivery Group		S		S		S

Legend

- Y - Yes: always provided by the Service Header
- I - Implicit parameters of the timeslot
- E - Explicit value overrides the implicit timeslot value
- S - Selectable: Service header allows the capability to be selected as required
- X - Selectable: Provided by using Leg Delivery

Figure 3C.11-11 Service Header to Message Delivery Information Mapping

□ Service Header Structures

Within the Service Headers, 1-bit flags are used to indicate the inclusion or exclusion of an optional field or a group of fields. The structure of all the Service Headers is given in this section. A complete definition of the Service Headers is contained in [\[SNC SS\]](#) Appendix A. The structure of Service Header 0 is shown in [Figure 3C.11-12](#).

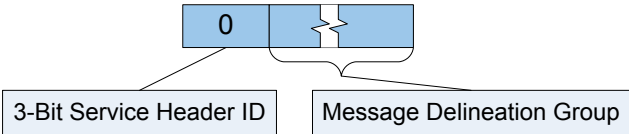


Figure 3C.11-12 Service Header 0 Structure

The structure of Service Header 1 is shown in [Figure 3C.11-13](#).

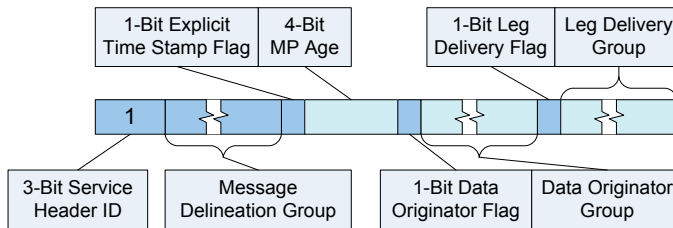


Figure 3C.11-13 Service Header 1 Structure

The structure of Service Header 2 is shown in [Figure 3C.11-14](#).

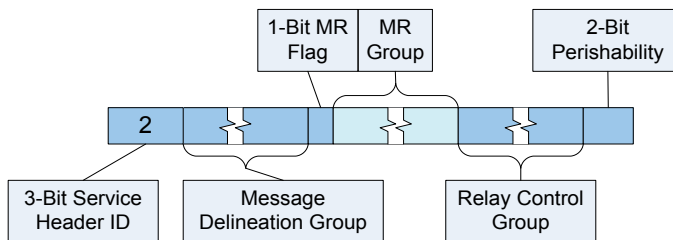


Figure 3C.11-14 Service Header 2 Structure

The structure of Service Header 3 is shown in [Figure 3C.11-15](#).

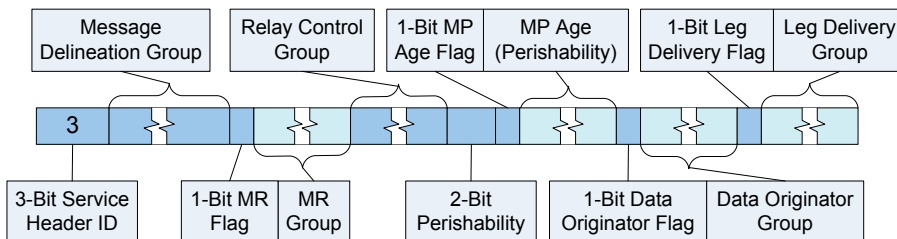


Figure 3C.11-15 Service Header 3 Structure

The structure of Service Header 4 is shown in [Figure 3C.11-16](#).

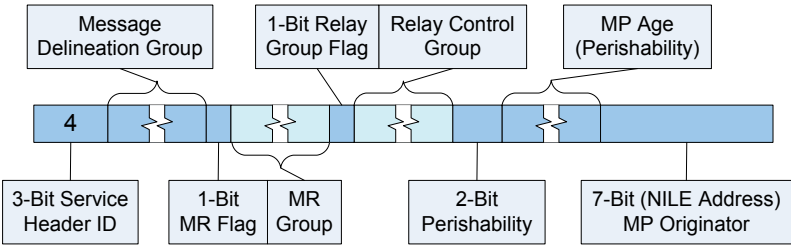


Figure 3C.11-16 Service Header 4 Structure

The structure of Service Header 5 is shown in [Figure 3C.11-17](#).

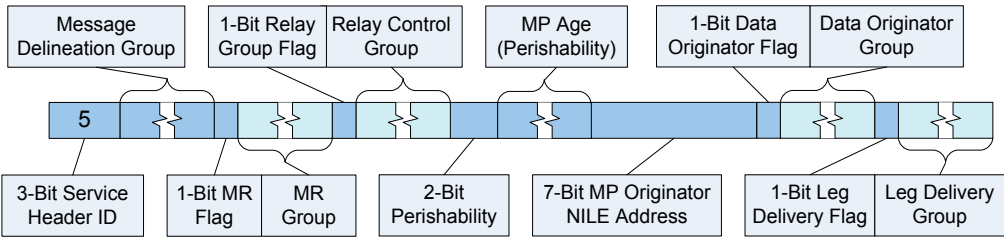


Figure 3C.11-17 Service Header 5 Structure

The structure of Service Header 6 is shown in [Figure 3C.11-18](#). Service Header 6 is used for the transmission of Supplementary Leg Fragments, when Leg Fragmentation is used. Leg Fragmentation can be selected in Service Headers 1, 3 and 5.

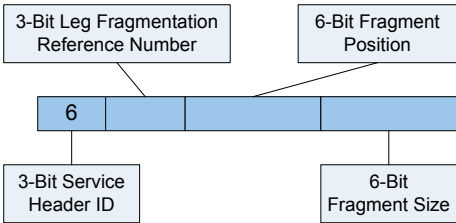


Figure 3C.11-18 Service Header 6 Structure

Service Header 7 is used to transmit CSMs, and the structure of a CSM is as shown in [Figure 3C.11-19](#). The 3-bit CSM ID field that follows the Service Header ID indicates which of the CSMs is being used and this defines the contents of the CSM that optionally follow the field.

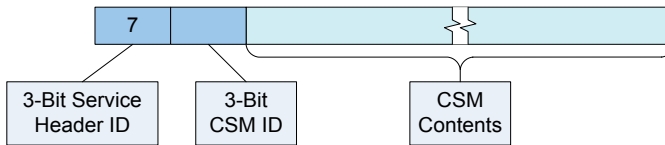


Figure 3C.11-19 Service Header 7 Structure

□ Message Delivery Information Structures

The Service Headers contain the following Message Delivery Information fields or groups of fields.

Message Delineation Group: Service Headers 0-5 include the Message Delineation Group, the structure of which is shown in [Figure 3C.11-20](#).

For Tactical messages, the Message Delineation Group provides the number of messages in the message packet and the number of Tactical Message Words in each message using a 4-bit Data Unit Configuration Code (DUCC). The meaning of the DUCC values is shown in [Figure 3C.11-21](#).

For Technical messages, it provides how many messages (1-3) are in the message packet. The length of the technical messages is known upon transmission, but has to be determined on reception by parsing the MP until the end of each message in the message packet is found.

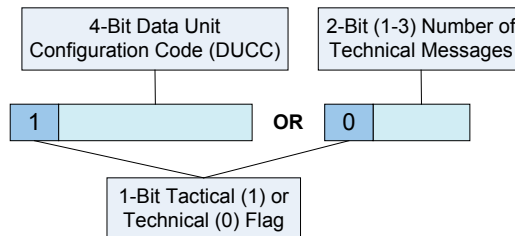


Figure 3C.11-20 Message Delineation Group Structure

DUCC	Number of Messages	Number of Tactical Message Words			
		First Message	Second Message	Third Message	Data Unit (Total)
0	2	1	1	0	2
1	3	1	1	1	3
2	2	1	2	0	3
3	2	2	2	0	4
4	2	1	3	0	4
5	3	2	1	1	4
6	not used				
7	not used				
8	1	1	0	0	1
9	1	2	0	0	2
10	1	3	0	0	3
11	1	4	0	0	4
12	1	5	0	0	5
13	1	6	0	0	6
14	1	7	0	0	7
15	1	8	0	0	8

Figure 3C.11-21 DUCC Values and Meanings

Machine Receipt Group: The Machine Receipt (MR) Group is selectable in Service Headers 2-5. MR for non-relay transmissions is supported by the Leg Delivery Group in Service Header 1. The MR Group structure is shown in Figure 3C.11-22. The End-to-End Reference Number (E2ERN) is a 3-bit number associated with this unit and the MTV. This means that there are eight E2ERs available per second. The Address Group (also used by the Relay Control Group and the Leg Delivery Group) has the structure as shown in Figure 3C.11-27.

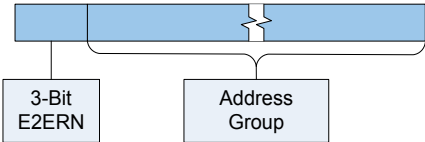


Figure 3C.11-22 MR Group Structure

Relay Control Group: The Relay Control Group is mandatory in Service Headers 2 and 3 and is selectable in 4 and 5. The group contains the Address Group, which is for Non-MR addressing. The Relay Control Group structure is shown in [Figure 3C.11-23](#). The Relay Control Value fields is only included when the Address Group Flag is set to one.

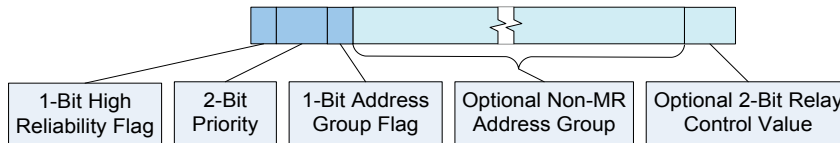


Figure 3C.11-23 Relay Control Group Structure

Perishability: Perishability is a 2-bit field that indicates the message packet perishability. All messages in the message packet have the same perishability. Message packets with an MTV that is more than the perishability duration prior to the current time are not relayed. The values of this field and their corresponding duration in seconds are listed in [Figure 3C.11-24](#).

Message Packet Age: Message Packet Age is implicitly zero unless an explicit value is provided, which can be selected in Service Headers 1 and 3. For relayed transmissions using Service Headers 4 and 5, an explicit MP Age is always included. The message packet age is a 4-bit field for Service Header 1. For Service Headers 3, 4 and 5, the length of the field is proportional to the perishability, as listed in [Figure 3C.11-24](#).

Perishability Field Value	Perishability Duration	MP Age Length (Bits)
0	15 seconds	4
1	31 seconds	5
2	63 seconds	6
3	511 seconds	9

Figure 3C.11-24 MP Age Length for each Perishability value

MP Originator: The originator of the MP is implicit when the MP is transmitted by the originator (the timeslot owner) and explicit (7-bit NILE Address of the message packet originator) when the MP is relayed and is included in Service Headers 4 and 5.

Data Originator Group: The Data Originator Group only applies to Tactical messages (known from the message delineation group). The data originator is the same as the MP Originator unless explicitly specified. This is selectable in the extended Service Headers 1, 3 and 5. When explicitly specified in the Data Originator Group, a flag indicates whether the Data Originator Address is a 15-bit Link 22 Address or a 7-bit NILE Address, as shown in [Figure 3C.11-25](#).

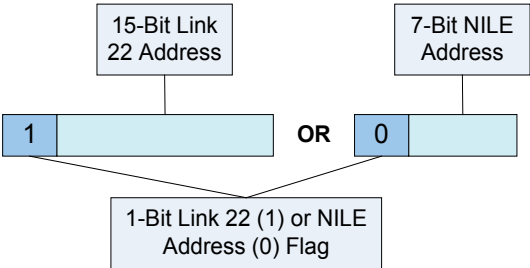


Figure 3C.11-25 Data Originator Group Structure

Leg Delivery Group: The Leg Delivery Group is selectable in the extended Service Headers 1, 3 and 5. The structure of the group is shown in [Figure 3C.11-26](#). If the Leg Fragmentation Flag (the first field) is set to one, then the second and third fields are included, otherwise they are not. If the first field is zero or the third fields is set to one, the remaining fields may be present, otherwise none are. The optional Leg Message Packet Reference Number (MPRN) Extension field is only included when the previous Leg MPRN field contains 31 (all bits set to one). There are no NILE Addresses in the Exclusion List when the List length is zero.

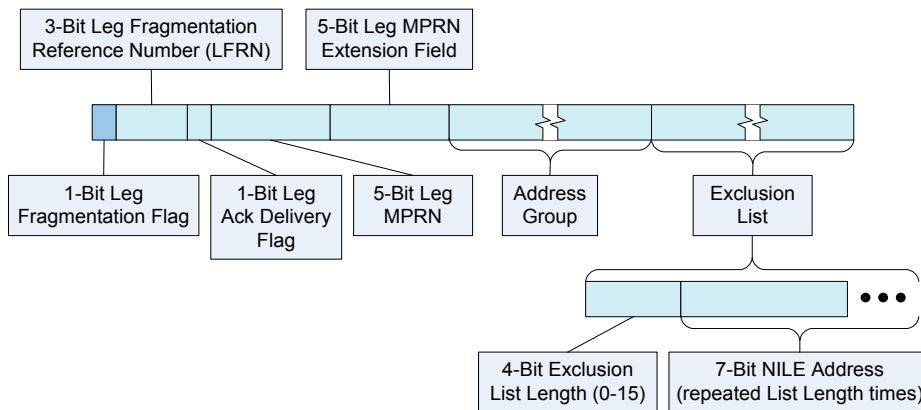


Figure 3C.11-26 Leg Delivery Group Structure

Address Group: The address group is used in the MR Group, the Relay Control Group and in the Leg Delivery Group. The group provides four different addressing types, as shown in Figure 3C.11-27. When used in the MR or Relay Control groups, the ‘All NUs’ option means all NUs in the Super Network (Totalcast), whereas when used in the Leg Delivery Group it means all NUs in the Transmission Leg (Neighborcast).

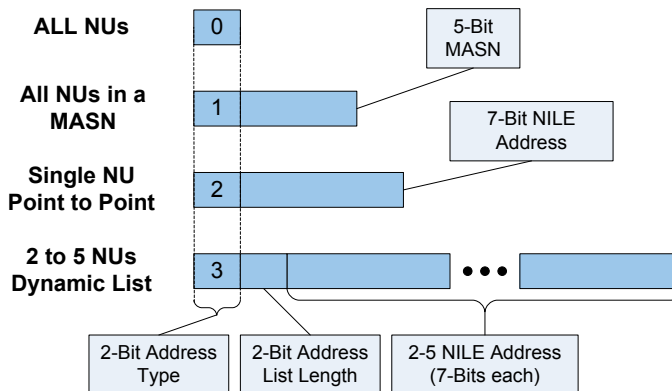


Figure 3C.11-27 Address Group Structure

❑ **Communication Service Message (CSM) Structures**

Service Header 7 is used to transmit CSMs, and the structure of a CSM is as shown in Figure 3C.11-19. The 3-bit CSM ID field that follows the Service Header ID indicates which of the CSMs (0-7) is being used and this defines the contents of the CSM that optionally follows the field.

CSM 0: The Padding CSM is used to fill unused space at the end of a NP, and consists of three fields as shown in Figure 3C.11-28. The variable length (greater than or equal to zero) NP Authentication Code field, when the length is greater than zero is calculated from the used bits in the NP, which on reception is used to authenticate the received NP contents.

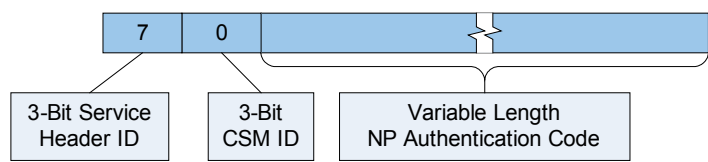


Figure 3C.11-28 Padding CSM 0 Structure

CSM 1: The Machine Receipt CSM is used to acknowledge the receipt of a MP when the MR protocol is being used.

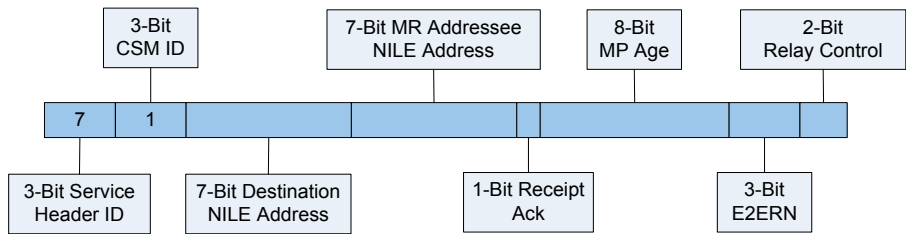


Figure 3C.11-29 Machine Receipt CSM 1 Structure

CSM 2: The Delivery Failure CSM is used to provide notification of failure to relay a MP by a reliable relay, as part of the Guaranteed Delivery protocol.

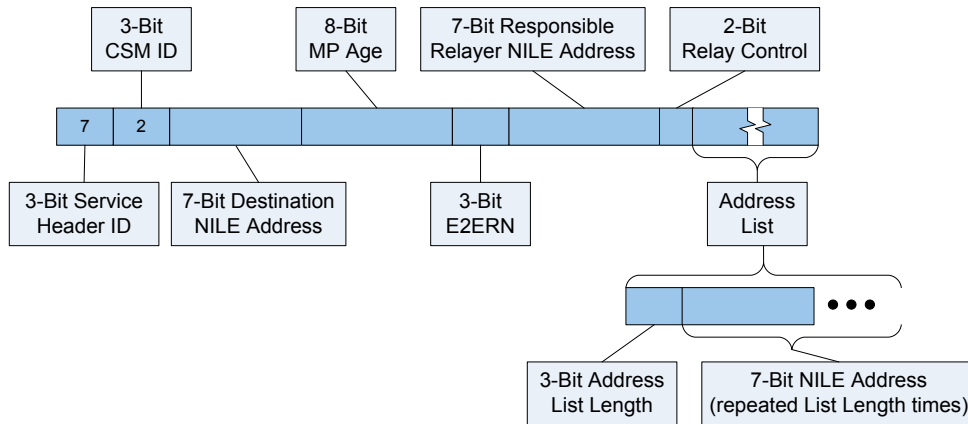


Figure 3C.11-30 Delivery Failure CSM 2 Structure

CSM 3: The Delivery Acknowledgment CSM is sent by a reliable relay to inform the source of an MP than it has received a Leg Acknowledgement from one or more units, as part of the Guaranteed Delivery protocol.

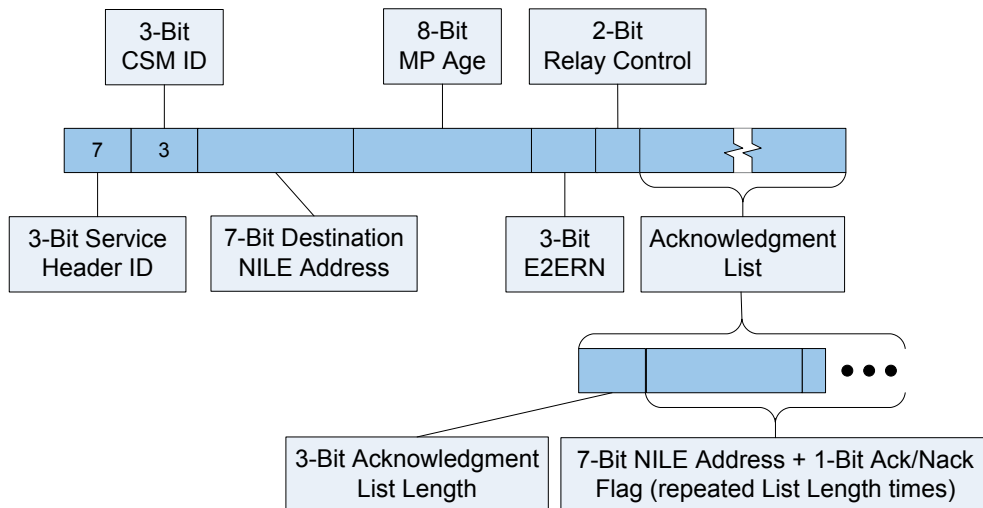


Figure 3C.11-31 Delivery Acknowledgment CSM 3 Structure

CSM 4: The Leg Acknowledgment CSM is sent to acknowledge the receipt of a MP, as part of the Guaranteed Delivery protocol. The optional Leg MPRN Extension field is only included when the previous Leg MPRN field contains 31 (all bits set to one).

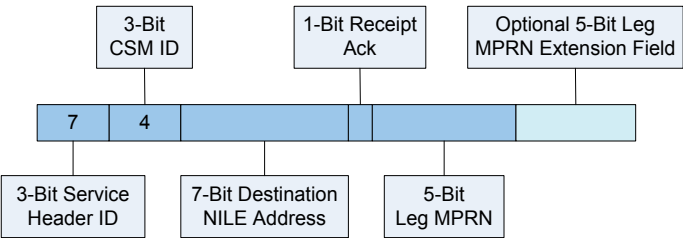


Figure 3C.11-32 Leg Acknowledgment CSM 4 Structure

CSM 5, 6 & 7: These CSMs are currently unused and are reserved for future use. To be backward compatible when they are used they are specified with destination and originator NILE Addresses and a Relay Control Value so that they can be routed and relayed though the system from the originator to the destination. They all have a length field that specifies how long the variable length content is. So as to be backward compatible the parsing of NPs containing these CSMs will just ignore the bits that they specify as being used, and not cause the NP to be discarded due to unknown contents. The structure of these currently unused CSMs is shown in as shown in [Figure 3C.11-33](#).

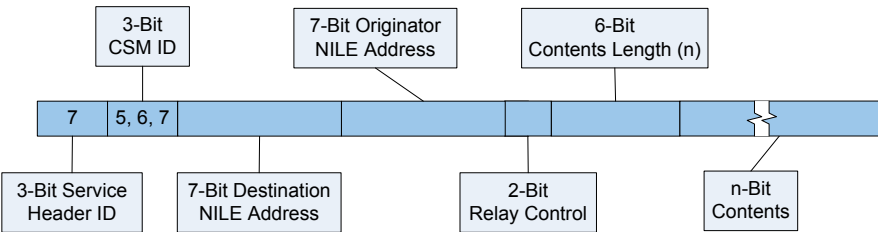


Figure 3C.11-33 Unused CSMs 5, 6 & 7 Structure

3C.12 Dynamic TDMA (DTDMA)

The Dynamic TDMA (DTDMA) protocol enables transmission capacity to be automatically reallocated to help relieve congestion in a NILE network. The DTDMA protocol occurs entirely between SNCs. No DLP or operator involvement is required (other than to enable DTDMA in a network). When DTDMA is enabled, the SNCs of congested units automatically request additional transmission capacity. Disabling DTDMA during operations only affects the start of new reallocations and does not affect reallocations already initiated.

Additional capacity can be requested on a temporary or permanent basis.

Temporary reallocation smoothes traffic imbalance during transient periods of congestion. When a unit has a qualified continuous need for capacity, it requests a permanent reallocation. This maximizes the use of the available capacity in the Operational Network Cycle Structure (ONCS).

The protocol was designed to minimize the use of bandwidth, as it is only performed when the unit is already congested. It uses a distributed approach in that communication is only between network neighbors and no central control is required. The protocol is also optimized to minimize unused timeslots during the exchange between units. The major units involved in the protocol are listed below.

- Recipient - Unit experiencing high traffic (congestion) and requesting capacity
- Donors - Units with spare capacity which may be donated to the Recipient

DTDMA is described in the following subsections.

- [Types of Capacity Reallocation](#)
- [Technical Message Exchange](#)
- [DTDMA Process](#)
- [Recipient Processing](#)
- [Donor Processing](#)
- [All Other Units](#)
- [DTDMA Parameters](#)

3C.12.1 Types of Capacity Reallocation

DTDMA uses four different forms of reallocation which are listed below.

- Timeslot Ownership Change (TOC)
- Swap Timeslots (SWAP)
- Adjacent Timeslot Hand-Off (ATH)
- Partial Timeslot Ownership Change (PTOC)

The following figures represent only a portion of the ONCS, showing only the area affected. A Donor cannot donate more than 25% of its capacity.

□ Timeslot Ownership Change

In a Timeslot Ownership Change (TOC) reallocation, the Donor gives up the ownership of a whole timeslot to another unit, as shown in [Figure 3C.12-1](#), where NU 1 gives up one of its timeslots to NU 3.

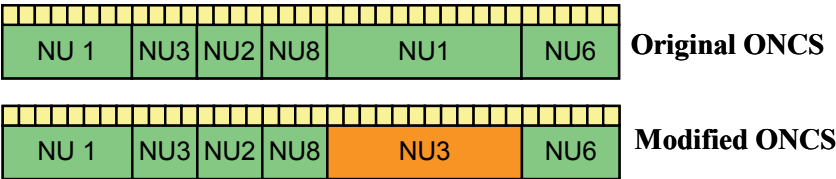


Figure 3C.12-1 TOC Reallocation

□ Swap Timeslots

In a Swap Timeslots (SWAP) reallocation, the Donor and Recipient exchange the ownership of timeslots, as shown in [Figure 3C.12-2](#), where NU 1 swaps one of its larger timeslots with a smaller timeslot of NU 3, thereby providing NU 3 with additional capacity.

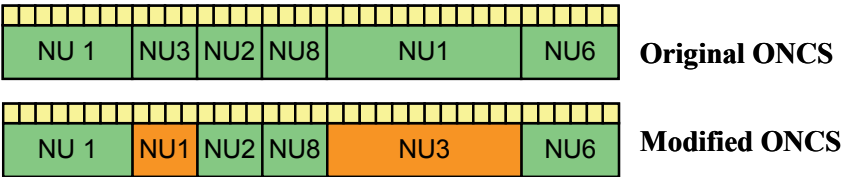


Figure 3C.12-2 SWAP Reallocation

□ **Adjacent Timeslot Hand-Off**

In an Adjacent Timeslot Hand-Off (ATH) reallocation, the Donor timeslot is shortened by transferring the ownership of a portion of the timeslot to the Recipient with an adjacent timeslot. The donated minislots can be on either side of the Recipient timeslot. The preferred case for the Recipient is when the minislots handed off follow the timeslot of the Recipient, so that the timeslot of the Recipient is extended in length but maintains the same start time (ATH-After). [Figure 3C.12-3](#) shows a reallocation using ATH-After, where NU 1 donates to NU 8 the first portion of its timeslot, which is adjacent to and follows NU 8's timeslot.

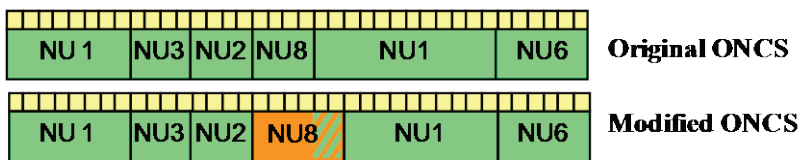


Figure 3C.12-3 “ATH-After” Reallocation

The second case is when the minislots handed off precedes the timeslot of the Recipient, so that the timeslot of the Recipient starts with the donated minislots (ATH-Before). [Figure 3C.12-4](#) shows a reallocation using ATH-Before, where NU 1 donates to NU 3 the end portion of its timeslot, which is adjacent to and precedes NU 3's timeslot.

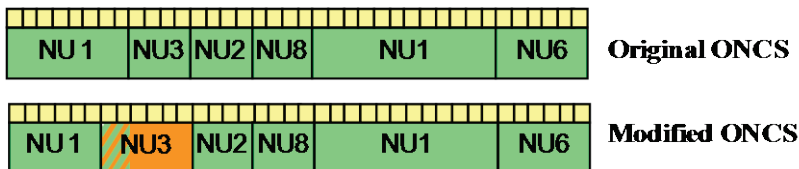


Figure 3C.12-4 “ATH-Before” Reallocation

□ **Partial Timeslot Ownership Change**

In a Partial Timeslot Ownership Change (PTOC) allocation, as for ATH, the Donor timeslot is shortened. A new timeslot is created at the end of the donor's timeslot and the ownership is transferred to the Recipient, as shown in [Figure 3C.12-5](#), where NU 1 gives up the end of one of its timeslots to NU 3.

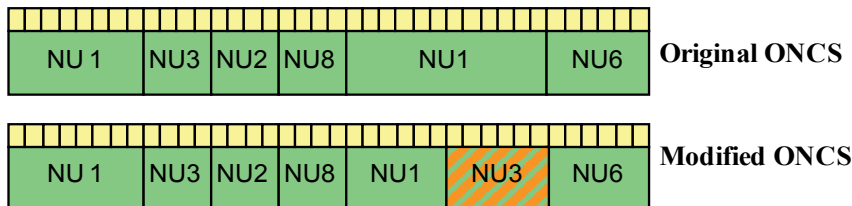


Figure 3C.12-5 PTOC Reallocation

3C.12.2 Technical Message Exchange

The overall flow of technical messages involved in DTDMA is shown in [Figure 3C.12-6](#) and it may be summarized by the following steps.

- When the congestion reaches defined thresholds, the Recipient transmits CAPACITY NEED technical messages to RF neighbors to request additional capacity
- The Potential Donors respond with a GRANT technical message.
- The Recipient collects up to three offers. Multiple offers can be used, although multiple SWAPs involving the same Recipient timeslot are not permitted
- If any of the selected offers is of the form ATH or PTOC, the Recipient advertises all the selected ATH or PTOC reallocations with a RELIABILITY ACKNOWLEDGEMENT technical message

When the RELIABILITY ACKNOWLEDGEMENT technical message is received, a potential Donor needs to check if its offer of ATH or PTOC is selected. If the offer is selected, the Donor retransmits this RELIABILITY ACKNOWLEDGEMENT technical message.

All technical messages involved in the exchange can be transmitted in any network to reach the intended destinations and are not restricted to the network on which the reallocation occurs.

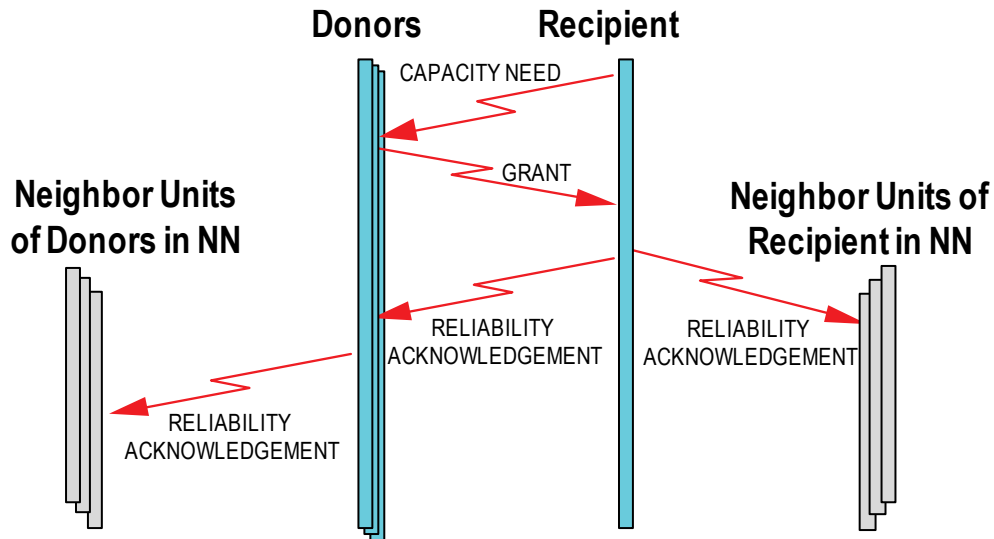


Figure 3C.12-6 Technical Message Exchange

The Recipient SNC determines whether to request a temporary or a permanent reallocation. If the Recipient has requested three temporary allocations within the last 126 NCTs, a permanent reallocation is requested. When a permanent reallocation occurs, the Recipient sends a STATUS ACKNOWLEDGEMENT technical message to the NMU for all types of reallocations. The SNC of the NMU sends a NCS DESCRIPTION technical message to all units in the network to notify changes in the ONCS. All units in the network, including the NMU and the Recipient, notify their DLP using the 'Permanent Reallocation' (412h) message, as detailed in [Figure 3C.12-7](#).

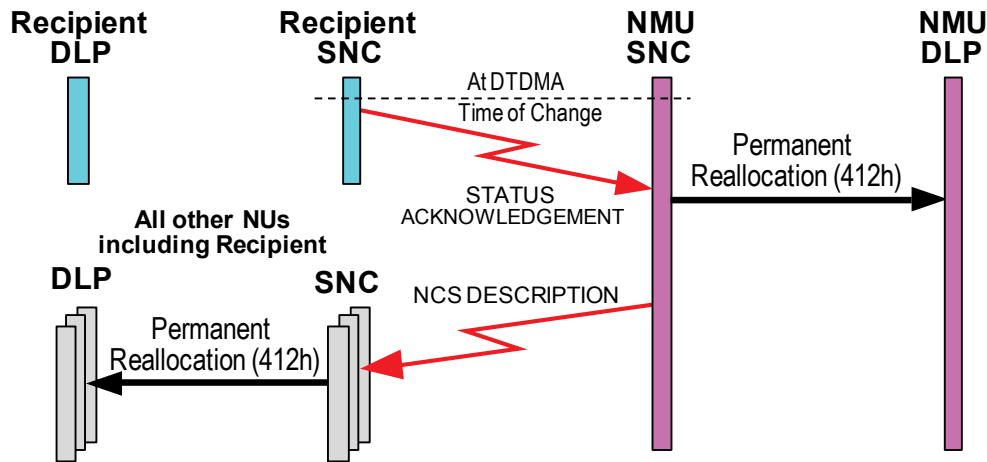


Figure 3C.12-7 Permanent Reallocation Notification

The following list summarizes the technical messages involved in the DTDMA protocol.

- CAPACITY NEED
- GRANT
- NCS DESCRIPTION
- RELIABILITY ACKNOWLEDGEMENT
- STATUS ACKNOWLEDGEMENT

Figure 3C.12-8 summarizes the information of interest in the CAPACITY NEED technical message, which will aid in understanding the rest of this section.

Field	Explanation
Need Amount for each priority	Indicates the number of Tactical Message Words (TMWs) needed for each priority
Temporary/Permanent Flag	Permanent if the Recipient has made three temporary requests within the last 126 NCTs. Temporary otherwise
Message Reference Number	Updated with each transmission, used to distinguish between requests
Grant Collection end TOD	The TOD at which the Recipient ends the collection of GRANT technical messages; approximately 3 NCTs (2 NCTs of delay, plus one NCT for processing)

Figure 3C.12-8 CAPACITY NEED Technical Message Information

Figure 3C.12-9 summarizes the information of interest in the GRANT technical message, which will aid in understanding the rest of this section.

Field	Explanation
Dynamic Reallocation Type	Type of reallocation being granted: TOC, SWAP, ATH, or PTOC
TOD	Time that the reallocation can take place, which depends on the type of reallocation involved
Duration	Length of time of the donation 0 for permanent donations 1-15 minutes for temporary donations
NCS Pointer of donated slot	First minislot within the ONCS of the donated slot
Size of donated slot	Used only for ATH or PTOC - Number of minislots donated
NCS Pointer of Recipient's slot	Used only for SWAP. First minislot within the ONCS of the Recipient's slot that is being swapped with the donated slot

Figure 3C.12-9 GRANT Technical Message Information

3C.12.3 DTDMA Process

The DTDMA process can be broken down into seven intervals, as shown in Figure 3C.12-10.

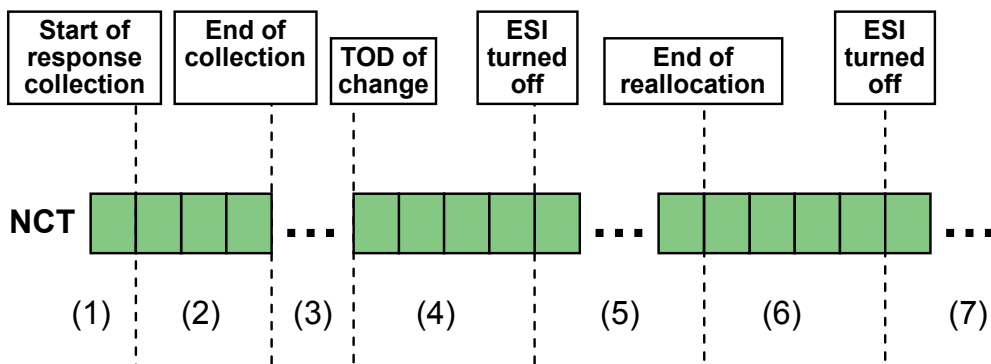


Figure 3C.12-10 DTDMA Process Intervals

Interval (1): The Recipient transmits a CAPACITY NEED technical message indicating a need for additional capacity, and includes the TOD at which it will stop collecting GRANT technical messages.

Interval (2): The Recipient collects responses from other units in the network. These responses are DTDMA donations or “offerings” in the form of a GRANT technical message. At the end of this time period, the Recipient determines which donations it will accept.

Interval (3): The Recipient waits until the TOD indicated in the GRANT technical message for the reallocation.

Interval (4): The Recipient and the Donor execute the timeslot change, transmitting in the new timeslot arrangement with Explicit Source Identification for four NCTs. The recipient also sets the DTDMA flag in the NP, when transmitting in any selected offer. The use of these two flags is described in the [Recipient Processing](#) sub-section.

Interval (5): The Recipient and the Donor transmit until the end of the DTDMA reallocation with Explicit Source Identification turned off.

Interval (6): After the reallocation has expired, the Recipient reverts to the original ONCS and transmits with Explicit Source Identification on for four NCTs. This is functionally similar to Interval (3), but using the original pre-DTDMA ONCS.

Interval (7): The Recipient continues transmitting in the original pre-DTDMA ONCS, but without Explicit Source Identification.

3C.12.4 Recipient Processing

Recipient processing involves the following.

- [DTDMA Control Activation](#)
- [Received Offer Management](#)
- [Start of Reallocation](#)
- [End of Reallocation](#)
- [Use of Explicit Source Identification](#)
- [Use of DTDMA Control Flag](#)

□ **DTDMA Control Activation**

The Recipient unit sends two consecutive CAPACITY NEED technical messages requesting a reallocation when the following list of conditions is met.

- The unit's Congestion Index (refer to section 3C.9 Congestion) for at least one priority is two or higher on the network
- The unit is not already engaged as Recipient of capacity in a temporary dynamic reallocation for the network
- At least one bi-directional RF neighbor exists

The decision flowchart is shown in Figure 3C.12-11.

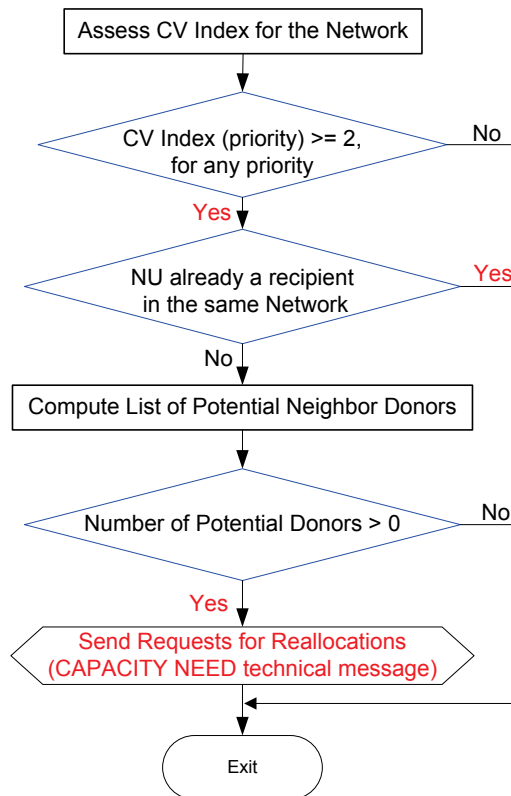


Figure 3C.12-11 DTDMA Activation Control

The capacity need for each priority in the CAPACITY NEED technical message represents the number of Tactical Message Words (TMWs) (72 bits per word) which the Recipient predicts it will have for each priority in the TSR queue, two NCTs in the future.

□ ***Received Offer Management***

The Recipient evaluates all Grant offers received and can select multiple offers to satisfy its capacity need. All selected reallocations are the same type as the original request, either Permanent or Temporary.

The preferred order for selecting offers is the following.

- TOC
- SWAP, where the timeslot of the Recipient is not currently involved in another ongoing SWAP
- ATH-After, where the minislots handed off are after the timeslot of the Recipient, so the timeslot of the Recipient is extended in length maintaining the same start time
- ATH-Before, where the minislots handed off by the Donor are before the timeslot of the Recipient, so the timeslot of the Recipient starts with the donated minislots
- PTOC, where the Donor offers the minislots at the end of its timeslot

The Recipient creates a list of offers of the highest available preferred order. From this list, the SNC selects the most suitable offer, as follows.

- The smallest offer that satisfies the capacity need
- If no offer satisfies the capacity need, the largest offer available

If there are equivalent candidate offers, a selection is made as described below.

- The protocol compares the Link Reception Quality (LRQ) with the potential Donors and selects the Donor with the highest LRQ
- If there is still a tie, a random selection is made

The protocol repeats until the capacity need is satisfied, or there are no more offers available.

□ ***Start of Reallocation***

For each offer, the Recipient awaits the TOD indicated in the GRANT technical message. If the indicated TOD is not exactly the beginning of a new net cycle, the Recipient waits for the first new net cycle after the indicated TOD. At the indicated TOD, the Recipient updates its ONCS according to the reallocation.

If the reallocation is of the permanent type, at the start the Recipient also generates and transmits a STATUS ACKNOWLEDGEMENT technical message to the NMU, in order to inform that a permanent reallocation has been performed.

The use of the offers depends on the type of reallocation, which can be grouped into the cases below.

- SWAP and TOC
- ATH and PTOC

■ ***SWAP and TOC***

For SWAP and TOC offers, regardless of whether the Recipient selects the offer, the Recipient uses the offered timeslots for two NCTs for temporary reallocation, and four NCTs for permanent reallocation, indicating in the DTDMA Control Flag of the Network Packet whether or not the offer was selected.

In case of SWAP, the Recipient initially uses both of the swapped timeslots for two NCTs for temporary reallocation, and four NCTs for permanent reallocation, and then only uses the donated timeslot.

If the offer is selected, the Recipient continues to transmit in the offered slots for the duration of the reallocation, as indicated in the GRANT technical message.

■ ***ATH and PTOC***

When a reallocation of ATH or PTOC is involved, the Recipient sends a RELIABILITY ACKNOWLEDGEMENT technical message to indicate which offers were accepted. The RELIABILITY ACKNOWLEDGEMENT technical message is sent twice at an interval of one NCT.

The Recipient uses the offers it accepted, but does not transmit in the minislots of the offers it did not accept.

□ ***End of Reallocation***

At the end of the reallocation, the Recipient stops transmitting in the borrowed timeslots. The Recipient restores the ONCS to the conditions prior to the reallocation. If the reallocation was of the form SWAP, the Recipient starts using its own timeslot again (the one which had been swapped with the Donor).

□ ***Use of Explicit Source Identification***

Explicit Source Identification is used for all timeslots affected by DTDMA, for the first four NCTs at the beginning of a reallocation, and for the first four NCTs after the end of a temporary reallocation, by both the Recipient and by the Donor. This allows all other units to detect the change in the ONCS and allows for successful decryption through the crypto device, which requires knowledge of the message source.

This concept makes the protocol less dependent on the NCS DESCRIPTION technical message in case of a permanent reallocation. After the end of a temporary reallocation, this concept allows all units to update their ONCS information to the original ONCS.

□ ***Use of DTDMA Control Flag***

When the Recipient accepts an offer and uses any donated timeslot or portion, it sets the DTDMA flag in the Network Packets to indicate that the donor offer was accepted. The Donor based on the flag knows if the offer was selected or not.

3C.12.5 Donor Processing

Donor processing involves the following.

- Determine an Offer
- Start of Reallocation
- End of Reallocation

□ ***Determine an Offer***

Any unit is a potential Donor if both of the following criteria are satisfied for the relevant network.

- For all priorities, no Congestion Value of the Donor is greater than ten percent of its allocated capacity for the network
- The Donor and the Recipient have a direct bi-directional link in the same network on which a reallocation is requested

A potential Donor determines the following information for a reallocation.

- Capacity Need of Recipient
- Capacity Donor is Able to Handoff
- Type of Reallocation
- Duration of Reallocation
- Start Time of Reallocation

■ ***Capacity Need of Recipient***

The capacity to be handed off by the potential Donor depends on the capacity need of the Recipient. The potential Donor only takes into account the capacity need of the Recipient for priorities higher than the highest priority message currently in the queue at the potential Donor. This amount is known as the Recipient Need Amount.

■ ***Capacity Donor is Able to Handoff***

The potential Donor calculates the total capacity that it can hand off, known as the Reallocation Total Capacity Amount (RTA).

For a temporary reallocation, the Donor may handoff up to 80% of its average unused capacity over the last 20 NCTs. For a permanent reallocation, the Donor may handoff up to 40% of its average unused capacity over the last 60 NCTs.

The amount handed off is limited to no more than 25% of the Donor's total capacity.

■ ***Type of Reallocation***

The offer must meet the following criteria.

- The amount handed off is limited to no more than 25% of a Donor's total capacity
- The timeslot or part of a timeslot cannot be offered if it is already involved in another reallocation
- ATH and PTOC offers must produce valid sized timeslots for the media constraints of an NCS

The Donor determines the form of reallocation to offer, which meets the above criteria, as detailed below in descending order.

- TOC
 - The largest timeslot which satisfies the hand off criteria
- SWAP

- Donor timeslot is larger than the Recipient timeslot chosen for swapping
- Chosen timeslot is such that the difference in swapped timeslot sizes is closest to RTA
- ATH
 - Handed off capacity is less than or equal to the RTA
 - ATH-After is preferred to ATH-Before
- PTOC
 - Handed off capacity is less than or equal to the RTA
 - When none of the above are possible and the available capacity exceeds the non reallocatable amount , a portion of the slot is donated

■ **Duration of Reallocation**

A Donor will only offer the same type of reallocation, temporary or permanent, as requested by the Recipient.

The Donor calculates the duration, in minutes, for a temporary reallocation as the ratio of the Recipient’s need (as calculated by the Donor above) to the Donor’s offer of capacity, using the following formula.

Duration = Recipient Need Amount / Donor Capacity Offered

The value is rounded to the nearest minute, and then constrained to be in the range of 2 to 16 minutes.

■ **Start Time of Reallocation**

In the GRANT technical message, the Donor supplies the TOD at which the offer starts, taking into account delays in transmitting the GRANT message, and processing delays in the rest of the reallocation protocol. The start time is constrained as shown in [Figure 3C.12-12](#). The SNC computes the shortest time rounded to start of the next NCT.

Parameter	Value for Temporary Reallocation	Value for Permanent Reallocation
Minimum Delay	2 NCTs for TOC and SWAP 3 NCTs for ATH and PTOC	3 NCTs for TOC and SWAP 4 NCTs for ATH and PTOC
Maximum Delay	5 NCTs	10 NCTs

Figure 3C.12-12 Reallocation Start Time Constraints

□ ***Start of Reallocation***

The Donor's actions at the start of reallocation depend on the type of reallocation, which can be grouped into the cases below.

- **SWAP and TOC**
- **ATH and PTOC**

■ ***SWAP and TOC***

With SWAP or TOC reallocation, the Donor stops transmitting in the offered timeslot at the indicated TOD. It starts listening for transmission from the Recipient for two NCTs for temporary reallocation, and four NCTs for permanent reallocation. For SWAP, the Donor also does not transmit in the swapped timeslot during this listening period.

If the Recipient does not transmit in the timeslot, or transmits with the DTDMA Control Flag set to indicate that it did not select the offer, the Donor takes back the offered timeslots after the listening period is complete.

If the Recipient sets the DTDMA Control Flag to indicate that it selected the offer, the Donor updates its ONCS according to the reallocation, and in the case of SWAP, starts transmitting in the swapped timeslot after the listening period is complete, using Explicit Source Identification for four NCTs.

■ ***ATH and PTOC***

When a reallocation of ATH or PTOC is involved, if the offer is listed in the received RELIABILITY ACKNOWLEDGEMENT technical message (which means the offer has been accepted), the Donor updates its ONCS according to the reallocation, stops transmitting in the donated minislots at the indicated TOD, and retransmits the RELIABILITY ACKNOWLEDGEMENT technical message. If the Donor's offer was not listed in the message (not selected by the Recipient); the Donor will continue to use its own minislots.

If no RELIABILITY ACKNOWLEDGEMENT technical message is received, the Donor will not use the minislots involved for two NCTs for temporary reallocation, and four NCTs for permanent reallocation, starting from the TOD of the reallocation. If the Donor does not detect any activity in the donated slots by the Recipient during this time, it will resume using the offered minislots. If the Donor does detect use of the donated minislots by the Recipient, it updates its ONCS according to the

reallocation, and does not use the offered minislots for the duration of the reallocation. This enables the correct use of the offered minislots by the Donor, even if the Donor does not receive the RELIABILITY ACKNOWLEDGEMENT technical message.

□ End of Reallocation

The end of a temporary reallocation is determined by adding the duration of the reallocation to the start time of the reallocation, as specified in the GRANT technical message.

If the Recipient temporarily transmits in a SWAP or TOC reallocation, indicating that it has not selected the offer, the reallocation is considered complete after two NCTs for temporary reallocation, or four NCTs for permanent reallocation.

When the end of the reallocation is reached, the Donor restores the ONCS to its original state prior to the reallocation. The Donor then uses Explicit Source Identification for four NCTs in its transmissions in the timeslot it previously offered.

3C.12.6 All Other Units

All neighbor units that receive RELIABILITY ACKNOWLEDGEMENT technical messages update the “current” copy of the ONCS with the owner of the affected minislots.

For temporary reallocation, each SNC uses the modified “current” ONCS for the duration of the reallocation, restoring the original owner when the temporary reallocation expires.

When a NP is received with Explicit Source Identification for a unit that is different than the owner indicated in the ONCS, the new owner is recorded. This is only valid for assigned slots.

The SNC maintains two copies of the ONCS: baseline and current. Baseline ONCS is the one generated as part of the OLM or changed through a reconfiguration or a re-initialization. The SNC initially makes a copy of the baseline ONCS and uses it as the current ONCS. The SNC applies all temporary changes based on technical messages or Explicit Source Identification to the current ONCS. The SNC applies all permanent changes to both baseline and the current ONCS.

When any unit requests the ONCS for realignment to the NMU, the NMU always sends the baseline ONCS.

3C.12.7 DTDMA Parameters

Figure 3C.12-13 is a summary list of all DTDMA parameters.

Parameter Description	Temporary Reallocation Value	Permanent Reallocation Value
The number of NCTs the Recipient waits for an offer (GRANT technical message)	2 NCTs	2 NCTs
The maximum number of offers (GRANT technical messages) collected by the Recipient	3 messages	3 messages
Non Re-allocatable Capacity is the percentage of capacity that a unit always maintains	75 %	75 %
The number of NCTs the Donor listens in the offered minislots for activity of the Recipient	2 NCTs	4 NCTs
The number of NCTs in which the Donor or Recipient transmits NPs with the Explicit Source Identification in 'borrowed' minislots or minislots received back after a reallocation	4 NCTs	4 NCTs
Minimum duration (in NCTs) of a dynamic reallocation	2 NCTs	N/A
Maximum duration (in NCTs) of a dynamic reallocation	16 NCTs	N/A
Period of time for three temporary reallocations to allow for a permanent request	126 NCTs	N/A

Figure 3C.12-13 DTDMA Parameters

3C.13 SNC-to-LLC Protocols

The protocols on the SNC-to-LLC interface are:

- LLC Control & Status
- SPC Control & Status
- Transmission
- Reception

This section covers only the LLC Control & Status, with the remaining three involving the SPC being covered in the next section ([3C.14 LLC-to-SPC Protocols](#)). Coordinated information exchange between the SNC and the LLC, as well as between the LLC and the SPC, are based on a request/response dialog using the full duplex capability of the interface. Additionally unsolicited messages from the LLC and SPC may be generated to report errors or alarm conditions. The requests are initiated by the SNC for the SNC-to-LLC interface. Requests to the SPC pass through the LLC to the LLC-to-SPC interface. Although multiple requests can be posed without waiting for a response, the requests are handled successively by the LLC and/or the individual SPCs and executed based on their priority. Transmissions have priority over Reception and configuration commands have priority over all pending transactions, after the completion of the transmission or reception already in progress.

This section describes the following.

- [Sequence Identifier](#)
- [SNC-to-LLC Interface Initialization](#)
- [LLC Status Request](#)
- [LLC Configuration Request](#)
- [Key Management](#)

Note that the sequence Identifier affects both the LLC and the SPC.

Request/response messages for different transactions may be interleaved on either the SNC-to-LLC interface or the LLC-to-SPC interface.

Transmission and Reception requests can be aborted. The abort mechanism entails the generation of a superseding request that cites the sequence identifier for the request to be aborted in addition to the parameters for the new request.

3C.13.1 Sequence Identifier

To enable binding of the requests with responses, each request and response message has a **Sequence Identifier** (also referred to as the Sequence ID). The request, subsequent request messages related to an initial request, and the associated response messages all have the same Sequence Identifier. Messages with the same Sequence Identifier are collectively called a transaction.

The transaction Sequence Identifier values are between 1 and 255. The value 0 is reserved for special meaning in some messages. The uses of the value 0 as a sequence identifier are the following.

- 'No-abort': the request is a new request of this type, and will not abort any preceding request
- 'Unsolicited response': an error or alarm response message is unsolicited or unrelated to any preceding request or transaction

The Sequence Identifiers are managed by the SNC and are monotonically increased in successive transactions. When the sequence Identifier reaches its maximum value, the next sequence Identifier used is restarted at 1.

The SNC sends a different Sequence Identifier for each transaction request it sends to the LLC and/or the SPC. When a message contains information in both the crypto partition (i.e., management function message) and the bypass partition (i.e., bypass function message), the Sequence Identifier is the same for each partition.

The LLC makes no assumptions regarding the order of Sequence Identifiers in successive transactions.

Since Sequence Identifiers are used for all attached media, an SPC makes no assumptions regarding their order in successive transactions, particularly any assumptions regarding strict incremental order.

3C.13.2 SNC-to-LLC Interface Initialization

The SNC (client) requests a connection with the LLC (server) to initialize the SNC-to-LLC LAN interface. The LLC monitors connection attempts using the TCP protocol, and responds using the TCP protocol, establishing a connection on the SNC-to-LLC interface as shown in [Figure 3C.13-1](#). The LLC only allows one active SNC-to-LLC connection at a time. Additional connection requests at the same time are denied.

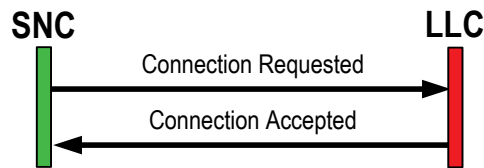


Figure 3C.13-1 SNC-to-LLC Initialization

3C.13.3 LLC Status Request

When the SNC sends an LLC Status Request (0100H) message to the LLC, the LLC responds with an LLC Status Response (F100H) message within 100 milliseconds, giving its status, as shown in [Figure 3C.13-2](#).

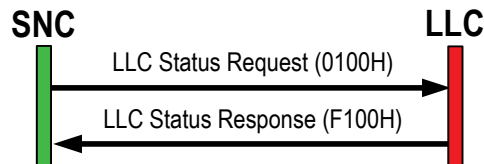


Figure 3C.13-2 LLC Status Message Flow

3C.13.4 LLC Configuration Request

When the SNC sends an LLC Configuration Request (8100H) message to the LLC, the LLC responds with an LLC Configuration Response (A100H) message within 45 seconds, as shown in [Figure 3C.13-3](#).

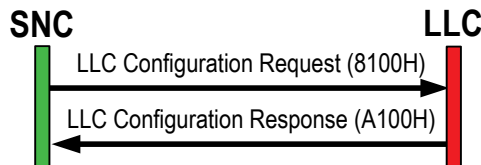


Figure 3C.13-3 LLC Configuration Message Flow

3C.13.5 Key Management

Crypto day rollovers occur under the direction of the SNC. The SNC sends a Key Management Request (8200H) message to an LLC specifying that the next crypto day is to be used by the LLC. The LLC responds to the SNC with a Key Management Response (E200H) message, within 50 milliseconds, confirming a successful rollover or not, as shown in [Figure 3C.13-4](#). Note that all NILE networks on the LLC roll over their crypto day simultaneously. The same crypto day is used for all SPCs.

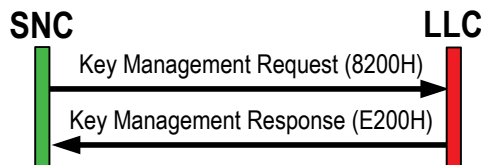


Figure 3C.13-4 LLC Key Management Message Flow

3C.14 LLC-to-SPC Protocols

The protocol used on the LLC-to-SPC interface is the same as that used on the SNC-to-LLC interface, as above, including the use of the Sequence Identifier.

SNC-to-SPC dialogs are mediated through the LLC and its trusted internal bypass. The LLC performs format translation and type translation between some interface messages on the SNC-to-LLC interface and on the LLC-to-SPC Interface. Many messages for SPC control are passed through the LLC unchanged.

When multiple SPCs are connected, the SNC does not depend on the responses being received in the order the requests were made.

There are four types of requests that affect the SPC.

- SPC Status Request
- SPC Configuration Request
- Transmission
- Reception

Request/response messages for different transactions may be interleaved on the LLC-to-SPC interface.

Transmission and Reception requests can be aborted. The abort mechanism entails the generation of a superseding request that cites the sequence identifier for the request to be aborted in addition to the parameters for the new request.

3C.14.1 SPC Status Request

When the SNC sends a SPC Status Request (0001H) to the SPC, the SPC responds with a SPC Status Response (00F1H) message, giving its status, as shown in [Figure 3C.14-1](#). The time that the SPC will take to send the responses depends on the characteristics of the SPC used, which is a national implementation decision.

Status information exchanged between the SNC and the SPCs are transmitted in the bypass partition with the crypto and data partitions empty.

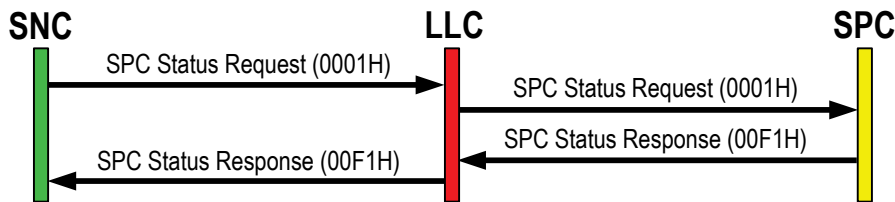


Figure 3C.14-1 SPC Status Message Flow

3C.14.2 SPC Configuration Request

When the SNC sends a SPC Configuration Request (00C1H) message to the SPC via the LLC, the SPC responds with a SPC Configuration Response (00E1H) message, as shown in [Figure 3C.14-2](#). The time that the SPC will take to send the response depends on the characteristics of the SPC used (manufacturers implementation), as long as it meets the requirement to be less than 10 seconds.

Configuration information exchanged between the SNC and the SPCs are transmitted in the bypass partition with the crypto and data partitions empty.

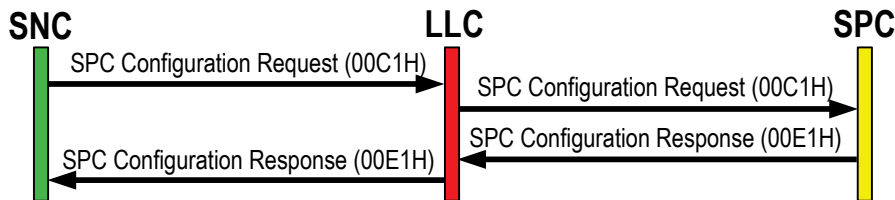


Figure 3C.14-2 SPC Configuration Message Flow

3C.14.3 Transmission

[Figure 3C.14-3](#) illustrates the message flow between the SNC, LLC, and SPC for the transmission of data in a transmission slot. To initiate a transmission on a network the SNC first sends a SPC Transmit Header Request (0002H) message to the SPC, via the LLC, for that network. The SNC then sends one or more LLC Transmit Network Packet Request (0303H) messages, which the LLC converts to SPC Transmit Network Packet Request (0003H) messages before sending them on to the SPC. One LLC Transmit Network Packet Request (0303H) will be sent for each Network Packet of data that must be encrypted with a different TOD parameter. When the data transmission is completed at the end of the transmission slot, the SPC sends a SPC

Transmit Response (00F2H) message to the SNC, via the LLC. During the transmission procedure, if the SPC receives a SPC Transmit Network Packet Request (0003H) message that is in error (for example, invalid checksum, control-field data, or received too late to transmit in the specified slot), it sends a SPC Reject Transmit Network Packet (00D3H) message (not shown in the figure) to the SNC for that particular SPC Transmit Network Packet Request (0003H) message.

The SNC sends unencrypted NPs and SPC/radio control information to the LLC in a single message. The NP is stored in the Data partition of the message. The SPC/radio control information is stored in the Bypass partition of the message. The information that is used by the LLC to encrypt the NPs is stored in the Crypto partition. When the message is received by the LLC, it passes on the SPC/radio control information to the SPC in the bypass partition. The LLC encrypts the NP and passes it to the SPC in the data partition. The message to the SPC never contains any data in the crypto partition. The SPCs use the bypass information to control the transmission of the encrypted NP over the air.

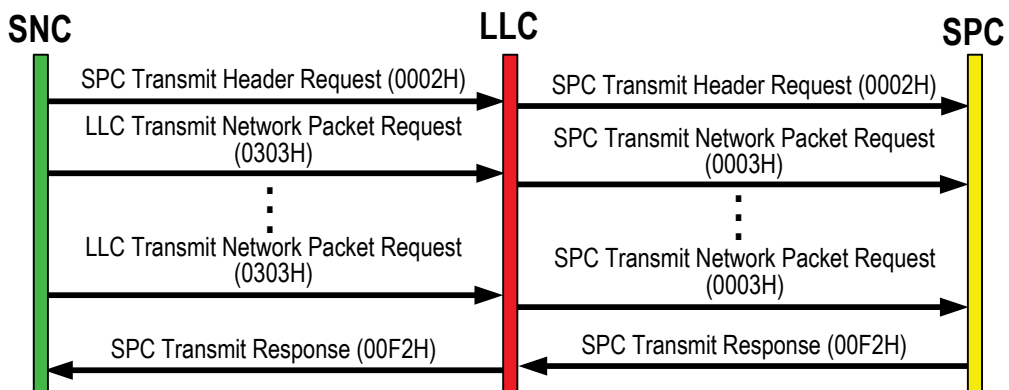


Figure 3C.14-3 Transmission Message Flow

3C.14.4 Reception

Figure 3C.14-4 shows the message flow between the SNC, LLC, and SPC for a reception slot. To initiate a reception on a network the SNC sends a LLC Receive Header Request (0404H) message to the LLC for that network, which the LLC converts to a SPC Receive Header Request (0004H) message before sending it on to the SPC for that network. When the time of the slot occurs, the SPC will switch the radio to reception and attempts to decode what it receives. If the media uses a

preamble and it is received, the SPC sends a SPC Receive Preamble Response (00F6H) message, followed by any received NPs. It sends the NPs to the LLC in a SPC Receive Network Packet Response (00F3H) message, which the LLC converts to a LLC Receive Network Packet Response (F5F3H) message. When a reception is completed, the SPC reports on the reception of the entire slot by sending a SPC Receive Response (00F4H) message to the SNC via the LLC.

The SNC schedules receptions by sending bypass messages to the SPCs (through the LLC) that have the information needed to receive and decrypt the received Network Packets. The encrypted NPs are sent from the SPC to the LLC for decrypting, in the Data partition of the message. Control information that is needed by the LLC to decrypt the received NPs is stored in the bypass partition. After decryption, the NPs are sent from the LLC to the SNC in the Data partition. The SNC unpacks the NPs, uses the technical messages for network management, and forwards the tactical messages to the DLP.

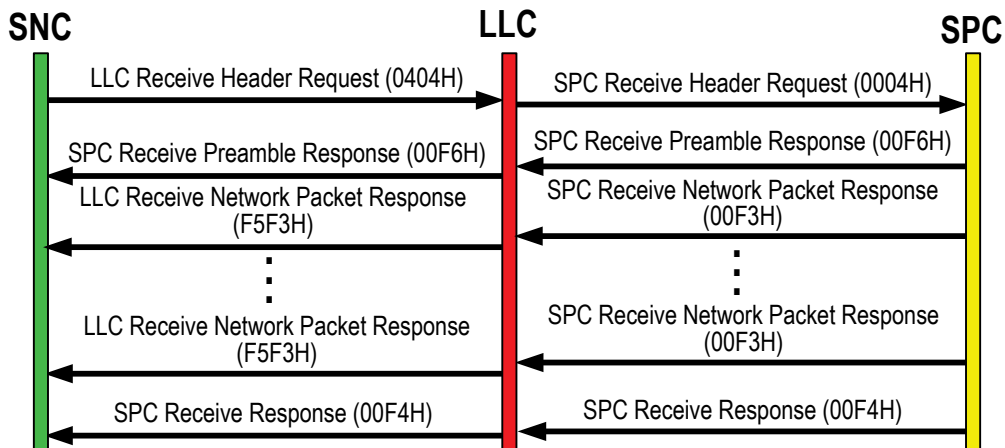


Figure 3C.14-4 Reception Message Flow

3C.15 Technical Messages

Technical messages are used for communication between SNCs and are originated by the Management function within the SNC. They are used to support the Management protocols. This section consists of the following subsections.

- Message List
- Message Structure
- Backward Compatibility
- Transmission Parameters

3C.15.1 Message List

Technical messages can be either fixed length, or variable length. The size of fixed length Technical messages is determined according to the Technical Message ID. The Technical Message ID consists of two fields, each of three bits, called the primary and secondary labels (“Pri” and “Sec” columns in [Figure 3C.15-1](#)). The size of variable length technical messages is determined according to the message contents (calculated from the size of the fixed fields plus the number of repeated fields times their size). Incomplete received technical messages are discarded. Received Technical messages are defined to be successfully processed after they have been passed to the appropriate management function. [Figure 3C.15-1](#) lists the technical message names, and the protocols for which the messages are used, ordered by their primary and secondary labels.

Pri	Sec	Technical Message Name	Protocol
0	0	SHORT LINK RECEPTION QUALITY	Routing/Relay
0	1	ROLE HEARTBEAT	Directory Maintenance
0	2	RETRANSMISSION REQUEST	Configuration/Initialization
0	3	Not Used	Not Used
0	4	ORDER COMPLIANCE	Network Management
0	5	Not Used	Not Used
0	6	Not Used	Not Used
0	7	Not Used	Not Used
1	0	CONGESTION INDEX	Congestion
1	1	STANDARD LINK RECEPTION QUALITY	Routing/Relay

Pri	Sec	Technical Message Name	Protocol
1	2	COMPACT LINK RECEPTION QUALITY	Routing/Relay
1	3	STANDARD LINK CONNECTIVITY DATA	Routing/Relay
1	4	COMPACT LINK CONNECTIVITY DATA	Routing/Relay
1	5	LRQ STATUS DEFINITION	Routing/Relay
1	6	RELAY SETTING	Directory Maintenance
1	7	Not Used	Not Used
2	0	CAPACITY NEED	Dynamic TDMA
2	1	GRANT	Dynamic TDMA
2	2	RELIABILITY ACKNOWLEDGMENT	Dynamic TDMA
2	3	STATUS ACKNOWLEDGMENT	Dynamic TDMA
2	4	MODIFIED MESSAGE	Backward Compatibility
2	5	SNC CAPABILITY	Backward Compatibility
2	6	Not Used	Not Used
2	7	Not Used	Not Used
3	0	LNE SLOT POSITION	Late Network Entry
3	1	SUPPORT UNIT SEARCH	Late Network Entry
3	2	SUPPORT UNIT RESPONSE	Late Network Entry
3	3	LNE REQUEST	Late Network Entry
3	4	LNE REQUEST ACK	Late Network Entry
3	5	LNE RESPONSE	Late Network Entry
3	6	NETWORK PARAMETER REQUEST	Late Network Entry
3	7	NU ENTRY REQUEST	Late Network Entry
4	0	NU ENTRY RESPONSE	Late Network Entry
4	1	TRANSMISSION CAPACITY REQUEST	Late Network Entry
4	2	TRANSMISSION CAPACITY RESPONSE	Late Network Entry
4	3	DIRECTORY COMPACT ADDRESS	Directory Maintenance
4	4	DIRECTORY COMPACT MASN	Directory Maintenance
4	5	DIRECTORY COMPACT STATUS	Directory Maintenance
4	6	DIRECTORY COMPACT RELAY	Directory Maintenance
4	7	DIRECTORY COMPACT ROLE	Directory Maintenance
5	0	MEDIA PARAMETER	Configuration/Initialization

Pri	Sec	Technical Message Name	Protocol
5	1	NCS DESCRIPTION	Multiple
5	2	NCT INFO	Configuration/Initialization
5	3	NU LIST	Configuration/Initialization
5	4	NU READY	Initialization (Probing Only)
5	5	NET START TIME	Configuration/Initialization
5	6	PROBING RECEPTION QUALITY	Initialization
5	7	NMU ACTIVE	Initialization
6	0	DTDMA ENABLE/DISABLE	Configuration/Initialization
6	1	DIRECTORY ADDRESS	Directory Maintenance
6	2	MASN CREATE	Directory Maintenance
6	3	MASN MODIFY	Directory Maintenance
6	4	MASN DELETE	Directory Maintenance
6	5	MASN COMPACT	Directory Maintenance
6	6	NU ROLES	Directory Maintenance
6	7	DIRECTORY REQUEST	Directory Maintenance
7	0	DIRECTORY STATUS	Directory Maintenance
7	1	NU STATUS	Directory Maintenance
7	2	DIRECTORY RESPONSE	Directory Maintenance
7	3	ORDER	Network Management
7	4	NOTIFICATION	Network Management
7	5	NU PERFORMANCE	Network Management
7	6	NCS NEEDS	Configuration/Initialization
7	7	Not Used	Not Used

Figure 3C.15-1 Technical Messages

3C.15.2 Message Structure

The structure of the technical messages is defined in [SNC SS] Appendix B. Technical messages include mandatory fields, optional fields, repeated fields, and optional repeated fields. Each field is a defined number of bits in length.

The sample of a message definition in Figure 3C.15-2 shows the colors used in [SNC SS] Appendix B to indicate optional fields (yellow), repeated fields (green) and repeated optional fields (yellowy green). The description of the fields provides the explanation, while the colors are mainly used to highlight the peculiarity of certain fields.

DFI:DUI	NAME	BITS	CONTROL/NOTES
SAB:TAA	PRIMARY LABEL	3	0
SAB:TAB	SECONDARY LABEL	3	0
SXX:TAX	Fixed Field A	3	Fixed Field always part of the message
SXX:TAX	Fixed Field B	7	Fixed Field always part of the message
SXX:TAX	SWITCH Field	2	Besides a protocol value, indicates whether a following section is included or not
SXX:TAX	Optional Field X1	24	Optional fixed fields, included based on the value of the SWITCH FIELD
SXX:TAX	Optional Field X2	7	
SXX:TAX	Optional Field X3	10	
SXX:TAX	Optional Field X4	5	
SXX:TAX	COUNTER Field	3	Provides the number of repetitions of the variable part
SXX:TAX	Repeat Field A1	10	Fields repeated the number of times provided in the COUNTER field
SXX:TAX	Repeat Field A2	5	
SXX:TAX	Repeat Field & Switch	2	Repeated Field, that is also a switch for following fields
SXX:TAX	Optional Counter Field	5	Optional COUNTER field only exists if the SWITCH field is set
SXX:TAX	Optional Repeat Field A3	10	Field repeated the number of times provided in the COUNTER field if any of the included switches is set to True or to the applicable value

Figure 3C.15-2 Technical Message Field Colors

As an example, the ‘LNE RESPONSE’ (3.5) technical message is shown in Figure 3C.15-3. The ‘CONFIRMED’ and ‘TX CAPACITY REQUEST’ fields are

switches that control the inclusion of other fields in the message, as indicated in the “CONTROL/NOTES” column. The ‘NUMBER OF SLOTS’ field is a counter, and indicates how many repeats of the ‘NCS POINTER’ and ‘SLOT SIZE’ fields exist in the message.

DFI:DUI	NAME	BITS	CONTROL/NOTES
SAB:TAA	PRIMARY LABEL	3	3
SAB:TAB	SECONDARY LABEL	3	5
SAA:TAA	ORIGINATOR	7	
SAO:TAA	LINK 22 ADDRESS	15	
SAJ:TAD	CONFIRMED	1	Defines whether the requested action was: - 0: FALSE: Protocol rejected - 1: TRUE: Protocol confirmed
SAJ:TAF	TX CAPACITY REQUEST	1	Defines whether transmission capacity is assigned and included in this message: - 0: FALSE - 1: TRUE
SAJ:TAJ	LNE PROTOCOL STATUS	1	Only included when CONFIRMED. (See Note 1)
SAA:TAC	REFERENCE	7	NILE address of the LNE unit, if assigned. Only included when CONFIRMED
SAD:TAA	NETWORK ID	3	Authorized Network. Only included when CONFIRMED. (See Note 2)
SAI:TAG	NUMBER OF SLOTS	5	Only included when CONFIRMED and TX CAPACITY REQUEST is True
SAI:TAB	NCS POINTER	10	Only included when CONFIRMED and TX CAPACITY REQUEST is True
SAI:TAD	SLOT SIZE	5	Repeated as described in NUMBER OF SLOTS field

Figure 3C.15-3 LNE RESPONSE Technical Message

Each field in a message is identified by a Data Field Identifier (DFI) and a Data Use Identifier (DUI). All fields with the same DFI:DUI have the same range and meaning of values, as defined in [SNC SS] Appendix B Section B.2 Data Field Definitions. The DFI defines the category of the field, such as Network Parameters. The DUI defines different types and uses of fields within the same DFI category. An example of a DFI:DUI entry is shown in Figure 3C.15-4.

DFI	NAME			
SAN	NETWORK PARAMETERS			
DFI:DUI	NAME	BITS	ALLOWED VALUES	COMMENTS/EXPLANATION
SAN:TAA	LLC INTEGRITY	1	0/1	A flag indicating whether cryptographic integrity will be/is enabled on a given network. Permitted values are: 0: Enabled, 1: Disabled. Note Values are inverted compared to the DLP IDD
SAN:TAB	FREQUENCY INDEX	24	0 - 16777215	Specifies the setting for the SPC for the frequency(ies) to be used. It consists of an index to the frequency set of the SPC
SAN:TAC	MEDIUM PARAMETER INDEX	8	0-255	Specifies the setting of SPC parameters: Waveform, Modulation, Guard Time, Repetition Rate, and EDAC parameters. It consists of a reference for the SPC to the appropriate set. This reference is uniquely defined for different media. These values are defined in the individual media documentation. Note: DLP IDD uses MSN name for this field

Figure 3C.15-4 DFI:DUI Entries

3C.15.3 Backward Compatibility

Backward compatibility is provided between SNCs at the technical message level. Backward compatibility allows a SNC to recognize messages that are an older format than the SNC’s version, and to recognize when a message is newer, or contains fields that are newer than the SNC’s version. The received technical messages are processed as much as possible. Technical messages or parts of technical messages that are unknown to the SNC can be safely discarded. Each SNC at version 9.3 or later will transmit the SNC CAPABILITY technical message indicating the version number it is using. This enables the newer versions of the SNC to adapt their behavior based on the version of the other units in the Super Network.

Backward compatibility allows for the following changes.

- New Messages
- Modified Messages

□ New Messages

Any new future technical messages will include the message length (in bits) after the primary and secondary labels, as shown in Figure 3C.15-5. The message length allows older SNCs to discard the correct number of bits of a message they do not recognize. Older messages do not contain the message length field.

DFI:DUI	NAME	BITS	CONTROL/NOTES
SAB:TAA	PRIMARY LABEL	3	N/A
SAB:TAB	SECONDARY LABEL	3	N/A
SAS:TAB	MESSAGE LENGTH	10	The Length in bits of the message, including these 3 fields

Figure 3C.15-5 New Technical Message Format

□ **Modified Messages**

When a technical message is expanded (modified), the SNCs of older versions are able to interpret the portion of the technical message associated with its version or earlier versions, while new fields in a message will only be used by the newer SNCs. The 'MODIFIED MESSAGE' technical message is used to send a new version of an existing technical message in the form of the original message plus additional new fields, as shown in [Figure 3C.15-6](#).

DFI:DUI	NAME	BITS	CONTROL/NOTES
SAB:TAA	PRIMARY LABEL	3	2
SAB:TAB	SECONDARY LABEL	3	4
SAS:TAB	MESSAGE LENGTH	10	The Length in bits of the message
	EXISTING TECHNICAL MESSAGE FIELDS		The primary and secondary labels of the existing message. See details of each technical message for the message fields
	NEW FIELDS		.. to be defined

Figure 3C.15-6 Modified Message, Technical Message Format

3C.15.4 Transmission Parameters

The transmission service request of each Technical Message has required parameters, which may depend on the use of the message. These parameters consist of the following information.

- Source – Which NUs may transmit the technical message
- Pri – The priority of the transmission request
- Reliab – The reliability of the transmission request
- Forced Network – whether the message must be transmitted only on the specified network
- Type – The type or address
- Address – The address appropriate to the type
- ESI – Whether Explicit Source Identification is required

The transmission parameters for each technical message used in the various protocols are defined in the following figures. The parameters are defined on the same line as the message name when there is only one use of the message. Where there are multiple uses of the message the different uses are on the lines following the message name. The Technical messages are grouped into the protocols for which they are used, in the following order.

- | | |
|----------------------------------|-------------------|
| ■ Late Network Entry | (Figure 3C.15-7) |
| ■ Routing/Relay | (Figure 3C.15-8) |
| ■ Dynamic TDMA | (Figure 3C.15-9) |
| ■ Configuration & Initialization | (Figure 3C.15-10) |
| ■ Directory Maintenance | (Figure 3C.15-11) |
| ■ Network Management | (Figure 3C.15-12) |
| ■ Congestion | (Figure 3C.15-13) |
| ■ Backward Compatibility | (Figure 3C.15-14) |

□ *Late Network Entry*

Technical Message Name	Use	Source	Pri	Reliab	Forced Network	Type	Address	ESI
LNE SLOT POSITION								
Initiation/Termination	NMU	4	STD	No	MASN	Network	Yes	
Operation	NU	4	STD	Yes	Neigh	--	Yes	
SUPPORT UNIT SEARCH	LNE	1	STD	Yes	Neigh	--	Yes	
SUPPORT UNIT RESPONSE	SU	1	STD	Yes	Neigh	--	Yes	
LNE REQUEST	LNE	1	STD	Yes	Neigh	--	Yes	
LNE REQUEST ACK	SU	1	STD	Yes	Neigh	--	Yes	
LNE RESPONSE	SU	2	STD	Yes	Neigh	--	Yes	
NETWORK PARAMETER REQUEST								
IJ LNE	SU	4	HR	No	MASN	NMU	No	
AJ LNE	NU	4	HR	No	MASN	NMU	No	
NU ENTRY REQUEST	SU or NU	2	GD	No	MASN	SNMU	No	
NU ENTRY RESPONSE								
IJ LNE	SNMU	2	GD	No	P2P	SU	No	
AJ LNE	SNMU	2	GD	No	P2P	LNE NU	No	
TRANSMISSION CAPACITY REQUEST								
IJ LNE	SU	2	GD	No	MASN	NMU	No	
AJ LNE	NU	2	GD	No	MASN	NMU	No	
TRANSMISSION CAPACITY RESPONSE	NMU	2	GD	No	P2P	SU	No	
DIRECTORY RESPONSE	SU	3	STD	Yes	Neigh	--	Yes	
MEDIA PARAMETER								
IJ LNE	SU	1	HR	Yes	Neigh	--	No	
AJ LNE	NMU	1	GD	No	P2P	LNE NU	No	
IJ LNE – Alternative Network	NMU	1	GD	No	P2P	SU	No	
NCS DESCRIPTION								
AJ LNE	NMU	1	GD	No	P2P	LNE NU	No	
IJ LNE	SU	1	HR	Yes	Neigh	--	No	
IJ LNE – Alternative Network	NMU	1	GD	No	P2P	SU	No	
DIRECTORY RESPONSE	SU	3	STD	Yes	Neigh	--	Yes	
DIRECTORY COMPACT ADDRESS	SU	3	STD	Yes	Neigh	--	Yes	
DIRECTORY COMPACT ROLE	SU	3	STD	Yes	Neigh	--	Yes	
DIRECTORY COMPACT STATUS	SU	3	STD	Yes	Neigh	--	Yes	
DIRECTORY COMPACT RELAY	SU	3	STD	Yes	Neigh	--	Yes	
DIRECTORY COMPACT MASN	SU	3	STD	Yes	Neigh	--	Yes	

Technical Message Name	Use	Source	Pri	Reliab	Forced Network	Type	Address	ESI
SNC CAPABILITY								
	IJ LNE	LNE	1	STD	Yes	Neigh	--	Yes
	SU	SU	2	STD	Yes	Neigh	--	No

Figure 3C.15-7 LNE Technical Message Transmission Parameters

□ Routing/Relay

Technical Message Name	Source	Pri	Reliab	Forced Network	Type	Address	ESI
SHORT LINK RECEPTION QUALITY	NU	2	STD	No	Neigh	--	No
STANDARD LINK RECEPTION QUALITY	NU	2,4	STD	No	Neigh	--	No
COMPACT LINK RECEPTION QUALITY	NU	2,4	STD	No	Neigh	--	No
STANDARD LINK CONNECTIVITY DATA	NU	3,4	STD	No	Neigh	--	No
COMPACT LINK CONNECTIVITY DATA	NU	3,4	STD	No	Neigh	--	No
LRQ STATUS DEFINITION	SNMU	2	GD	No	P2P	NU	No

Figure 3C.15-8 Routing / Relay Technical Message Transmission Parameters

□ Dynamic TDMA

Technical Message Name	Source	Pri	Reliab	Forced Network	Type	Address	ESI
CAPACITY NEED	Recipient	1	STD	No	Neigh	--	No
GRANT	Donor	1	STD	No	Neigh	--	No
RELIABILITY ACKNOWLEDGMENT	Recipient & Donor	1	STD	No	Neigh	--	No
STATUS ACKNOWLEDGMENT	Recipient	4	GD	No	MASN	NMU	No
NCS DESCRIPTION	NMU	3	GD	No	MASN	Network	No

Figure 3C.15-9 DTDMA Technical Message Transmission Parameters

□ Configuration & Initialization

Technical Message Name	Use	Source	Pri	Reliab	Forced Network	Type	Address	ESI
PROBING RECEPTION QUALITY								
Local messages	NU	3	FL	No	--	--		Yes
Relayed messaged	NU	4	FL	No	--	--		Yes
NMU ACTIVE	NMU	2	FL	No	--	--		Yes
NU READY	NMU	2	FL	No	--	--		Yes
MEDIA PARAMETER								
Re-Initialization	NMU	2	GD	No	MASN	Network		No
Re-Initialization (Retransmission)	NMU	2.3*	HR/MR	No	**	Network		No
Initialization with Probing	NMU	2	FL	No	--	--		Yes
NCS DESCRIPTION								
Reconfiguration & Re-Initialization	NMU	2	GD	No	MASN	Network		No
Reconfiguration & Re-Initialization (Retransmission)	NMU	2.3*	HR/MR	No	**	Network		No
Reconfiguration & Re-Initialization (Retransmission after OST)	NMU	2	HR	No	TC	Network		No
Initialization with Probing	NMU	2	FL	No	--	--		Yes
NCT INFO	NMU	4	HR	No	TC	--		No
NU LIST								
Re-Probe	NMU	2	FL	No	--	--		Yes
Re-Initialization with Probing	NMU	2	GD	No	MASN	Network		Yes
Re-Initialization with Probing (Retransmission)	NMU	2.3*	HR/MR	No	**	Network		No
NET START TIME								
Reconfiguration & Re-Initialization	NMU	1	GD	No	MASN	Network		No
Reconfiguration & Re-Initialization (Retransmission)	NMU	1	HR/MR	No	**	Network		No
Initialization with Probing	NMU	2	FL	No	--	--		Yes
DTDMA ENABLE/DISABLE	NMU	3	HR	No	MASN	Network		No
RETRANSMISSION REQUEST	NU	3	STD	No	MASN	NMU		No

Figure 3C.15-10 Configuration & Initialization Message Transmission Parameters

Note: * First Retransmission at Priority 2, subsequent retransmissions at Priority 3
 ** Original MASN is reduced to Dynamic List if the number of destinations is between 2-5 and reduced to Point-to-Point when a single destination

□ *Directory Maintenance*

Technical Message Name Use	Source	Pri	Reliab	Forced Network	Type	Address	ESI
DIRECTORY ADDRESS							
Change	SNMU	2	GD	No	TC	--	No
DLP Request (TC)	SNMU	2	STD	No	TC	--	No
DLP Request (P2P)	SNMU	2	STD	No	P2P	NU	No
SNC Realignment	SNMU	2	STD	No	P2P	NU	No
RELAY SETTING							
Change	SNMU	2	GD	No	TC	--	No
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
MASN CREATE							
Change	SNMU	2	GD	No	TC	--	No
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
MASN MODIFY							
Change	SNMU	2	GD	No	TC	--	No
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
MASN DELETE							
Change	SNMU	2	GD	No	TC	--	No
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
MASN COMPACT							
Change	SNMU	2	GD	No	TC	--	No
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
ROLE HEARTBEAT							
Role Unit	NU	1	STD	No	TC	--	No
Non-Role Unit	NU	3	STD	No	TC	--	No
NU ROLES							
Change	SNMU	2	STD	No	TC	--	No
DLP Request (TC)	SNMU	2	STD	No	TC	--	No
DLP Request (P2P)	SNMU	2	STD	No	P2P	NU	No

Technical Message Name Use	Source	Pri	Reliab	Forced Network	Type	Address	ESI
SNC Realignment	SNMU	2	STD	No	P2P	NU	No
DIRECTORY REQUEST	NU	3	STD	No	MASN	SNMU	No
DIRECTORY STATUS	SNMU	4	STD	No	TC	--	No
NU STATUS							
Change	SNMU	4	HR	No	TC	--	No
DLP Request (TC)	SNMU	4	STD	No	TC	--	No
DLP Request (P2P)	SNMU	4	STD	No	P2P	NU	No
SNC Realignment	SNMU	4	STD	No	P2P	NU	No
DIRECTORY RESPONSE							
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
DIRECTORY COMPACT ADDRESS							
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
DIRECTORY COMPACT MASN							
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
DIRECTORY COMPACT STATUS							
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
DIRECTORY COMPACT RELAY							
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No
DIRECTORY COMPACT ROLE							
DLP Request (TC)	SNMU	3	STD	No	TC	--	No
DLP Request (P2P)	SNMU	3	STD	No	P2P	NU	No
SNC Realignment	SNMU	3	STD	No	P2P	NU	No

Figure 3C.15-11 Directory Maintenance Message Transmission Parameters

□ **Network Management**

Technical Message Name Use	Source	Pri	Reliab.	Forced Network	Type	Address	ESI
ORDER							
SN CLOSEDOWN	SNMU	2	HR	No	TC	--	No
NN CLOSEDOWN	SNMU	2	HR	No	P2P	NMU	No
NN CLOSEDOWN	NMU	2	HR	No	TC	--	No
LEAVE SN	SNMU	3	HR	No	P2P	NU	No
LEAVE NN	SNMU or NMU	3	HR	No	P2P	NU	No
JOIN EXISTING NETWORK	SNMU	3	HR	No	P2P	NU	No
ASSUME SNMU ROLE	SNMU	2	HR	No	P2P	New SNMU	No
ASSUME STANDBY SNMU ROLE	SNMU	3	HR	No	DL	New & Old Standby SNMU	No
ASSUME NMU ROLE	SNMU	2	HR	No	DL	New & Old NMU	No
ASSUME STANDBY NMU ROLE	SNMU or NMU	3	HR	No	DL	New & Old Standby NMU	No
LNE SLOT (Insert/Remove)	SNMU	3	HR	No	MASN	NMU	No
RADIO SILENCE SN/NN NU	SNMU or NMU	2	HR	No	P2P	NU	No
RADIO SILENCE ON NN	SNMU or NMU	1	HR	No	MASN	Network	No
RADIO SILENCE ON SN	SNMU	1	HR	No	TC	--	No
RADIO SILENCE OFF NN	SNMU or NMU	2	HR	No	MASN	Network	No
RADIO SILENCE OFF SN	SNMU	2	HR	No	TC	--	No
RE-INITIALIZATION	SNMU	3	HR	No	P2P	NMU	No
RECONFIGURATION	SNMU	3	HR	No	P2P	NMU	No
NEW NETWORK	SNMU or NMU	3	HR	No	MASN	Network	No
Key Management (All)	SNMU	1	HR	No	TC	--	No
ORDER COMPLIANCE							
Radio Silence ON	NU	1	HR	No	MASN	SNMU or NMU	No
All Others	NU	3	HR	No	MASN	SNMU or NMU	No
NOTIFICATION							
Roles & Radio Silence	NU	2	HR	No	TC	--	No
All Others	NU	3	HR	No	TC	--	No
NU PERFORMANCE	NU	3	STD	No	TC or MASN	MASN 18	No

Technical Message Name Use	Source	Pri	Reliab.	Forced Network	Type	Address	ESI
MEDIA PARAMETER	SNMU	3	HR	No	As Order	As Order	No
NCS DESCRIPTION	SNMU	3	HR	No	As Order	As Order	No
NCS NEEDS	SNMU	3	HR	No	As Order	As Order	No
NU LIST	SNMU	3	HR	No	As Order	As Order	No

Figure 3C.15-12 Network Management Message Transmission Parameters

☐ ***Congestion***

Technical Message Name	Source	Priority	Reliab	Forced Network	Type	Address	ESI
CONGESTION INDEX	Any NU	See Figure 3C.9-1	STD	No	Two Legs	--	No

Figure 3C.15-13 Congestion Message Transmission Parameters

☐ ***Backward Compatibility***

Technical Message Name	Source	Pri	Reliab	Forced Network	Type	Address	ESI
MODIFIED MESSAGE	All attributes are those of the encapsulated message within the modified message						
SNC CAPABILITY	NU	4	STD	No	TC	--	No

Figure 3C.15-14 Backward Compatibility Message Transmission Parameters

Appendix A

Integration and Test Tools

The Link 22 community recognized the need to make test tools available for the development of all components unique to Link 22.

There are two systems available.

- **NILE Reference System (NRS)**, which is used in the following ways.
 - SNC-to-SNC compatibility testing
 - ◆ Verification and Validation of requirements
 - ◆ Automated regression testing
 - LLC and SPC Verification and Validation support
- **Multiple Link System Test & Training Tool (MLST3)**, which supports the development and testing of national DLPs in the following areas.
 - Conformance to Tactical Standards
 - Interoperability, in both single and multi-link environments
 - National DLP Integration and Testing

Both systems can also be used for Link 22 training, and allow several configurations which are detailed in the following sections. Most of the MLST3 or any other Link 22 test configurations require the approved use of SNC and NRS components, the distribution of which is managed by the NILE PMO.

The collection of software and hardware components that are required to form a particular test system configuration is shown in a grey shaded area to separate the test system from the actual system being tested. This does not imply that a particular test tool provides all the components needed to form the test system configuration.

Detailed instructions on *how* to construct the various configurations can be found in the NRS System Technical Manual [NRS STM] or in the MLST3 User Manual.

To test the complete Link 22 architecture either real or simulated components are required for each of the layers of the architecture as shown in Figure A-1.

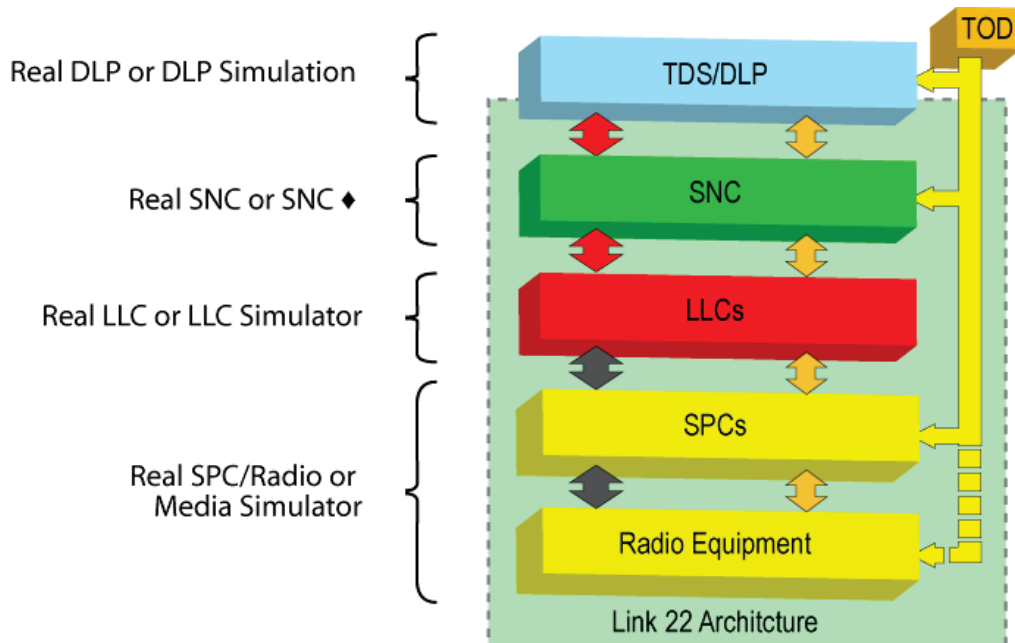


Figure A-1 Mapping of the Link 22 Architecture to Testing Components

The real SNC, the SNC♦, the LLC Simulator, and the Media Simulator are all software components, the distribution of which is managed by the NILE PMO.

A.1 NRS

The NRS is a suite of software applications and COTS hardware components designed to provide life cycle support and performance validation for the SNC, LLC and SPC. The NRS features data extraction and analysis tools which provide detailed analysis and replay capabilities. This section will cover the following topics.

- NRS Components
- NRS Configurations
- Scenario Generator (SG) Usage

A.1.1 NRS Components

The NRS consists of the following components.

- Scenario Generator
- SNC and SNC Diamond
- LLC or LLC Simulator
- Media Simulator

□ **Scenario Generator**

The Scenario Generator (SG) is a collection of tools for scenario development, test execution, data recording, and data analysis that are used to prepare, execute and analyze tests with the NRS.

The NRS allows the generation of expected responses that are checked using the SG Data Analysis (DA) program. Expected Responses are messages which DA expects to see in a Data Extraction (DX) file. By comparing the messages in a data extraction file with the expected responses, DA can automatically test functionality in the SNC. This simplifies regression tests for all components.

Further details of the SG tool usage are provided in section [A.1.3 Scenario Generator \(SG\) Usage](#).

□ **SNC and SNC Diamond**

The System Network Controller (SNC) is the operational software that Link 22 uses. In the test configurations it is referred to as the Unit Under Test (UUT).

The SNC Diamond (SNC♦) is a special multi-threaded version of the SNC which can simulate up to 32 SNCs per instance. The NRS can start up to four instances of the SNC♦ to simulate all 125 NILE units. The SNC♦s do not communicate directly with any LLCs, but with the Media Simulator which uses the NRS LLCs as necessary to encrypt and decrypt data that is transmitted to and received from the UUT. Communications between simulated units that are not connected to the UUT are not encrypted and decrypted. Some queue sizes are smaller in the SNC♦, so some tests need to be performed with multiple SNC UUTs using the Multiple Units Under Test (MUUT) configuration, instead of with SNC♦s.

□ **LLC or LLC Simulator**

The Link Level COMSEC (LLC) is described in section 3B.

The LLC Simulator provides a simulation of the LLC hardware. It is functionally identical to the real LLC and has an Ethernet connection to the SNC on one side and a serial port connection to the Media Simulator (or real SPC) on the other side. The LLC simulator only implements a simple encryption algorithm, which may produce different test results in cases where decryption would normally produce invalid data, such as during portions of Late Network Entry. Each instance of the LLC Simulator can simulate up to eight LLCs. Therefore multiple instances may be required when executing the NRS or MLST3, depending on the number of LLCs required. The LLC Simulator can replace real LLCs in all configurations described in this appendix.

□ **Media Simulator**

The Media Simulator (MS) simulates the SPCs/Radio and the LLC Interface in some configurations. The Media Simulator provides SPC simulation for up to six SNC UUTs and can map simulated SNC♦ units to a single LLC (simulator or real), by handling all of the communication with the LLC for the SNC♦ units. MS provides the serial connections to all LLCs to simulate the LLC/SPC connection. [Figure A.1-1](#) shows the MS providing LAN and Serial connections to an LLC for the SNC♦.

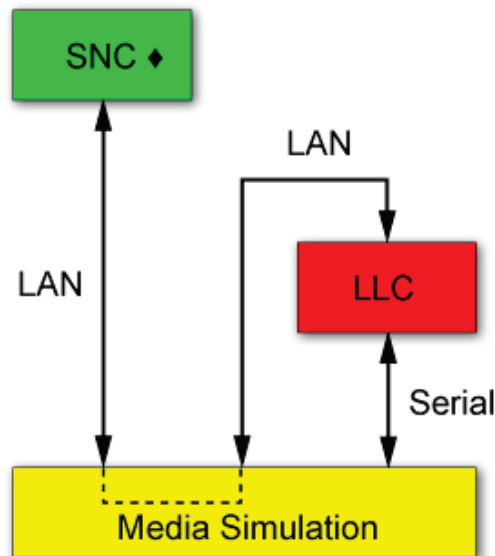


Figure A.1-1 SNC♦ to MS to LLC Connections

The Media Simulator is part of the NRS but also supports MLST3. It has some differences depending on which system it is used in. The system functionality to use is selected in the MS initialization file.

For the NRS, MS provides SPC simulation for one UUT and four SNC♦s or up to five UUTs. For MLST3, MS provides the capability to have combinations of real and simulated SPCs, for one SNC♦ and up to five UUTs, with a maximum of four units using real SPCs. Real and simulated SPCs cannot be combined on the same network.

A.1.2 NRS Configurations

The NRS configurations are the following.

- SNC Verification
- Multiple Units Under Test (MUUT)
- System Simulation
- Media Simulator (MS) Standalone

A configuration tool is provided with each Block Cycle Release to aid in the setup of NRS Components for each configuration. This tool is detailed in the [NRS STM]. The NRS components may be run on a single computer or multiple computers for each of the above mentioned configurations.

□ **SNC Verification**

SNC Verification is the primary NRS configuration used to verify the functionality of the SNC. SNC Verification involves a single SNC UUT being tested with up to 124 simulated units. The media connectivity is provided by the Media Simulator. [Figure A.1-2](#) depicts the NRS in SNC Verification mode.

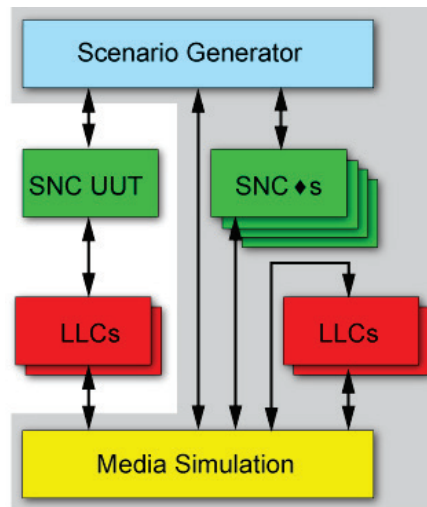


Figure A.1-2 NRS in SNC Verification mode

□ **Multiple Units Under Test (MUUT)**

The NRS Multiple Units Under Test (MUUT) configuration provides the ability to test between two and six real SNCs (UUTs), without the use of simulated units. This configuration also tests the functionality of the LLC. The normal configuration uses the Media Simulator. The purpose of this configuration is to ensure fidelity of testing between real SNCs, not between real and simulated SNCs. Functionally the NRS starts the real SNC software in place of one of the SNC♦s for the sixth UUT. [Figure A.1-3](#) depicts the Multiple Units Under Test (MUUT) configuration of the NRS.

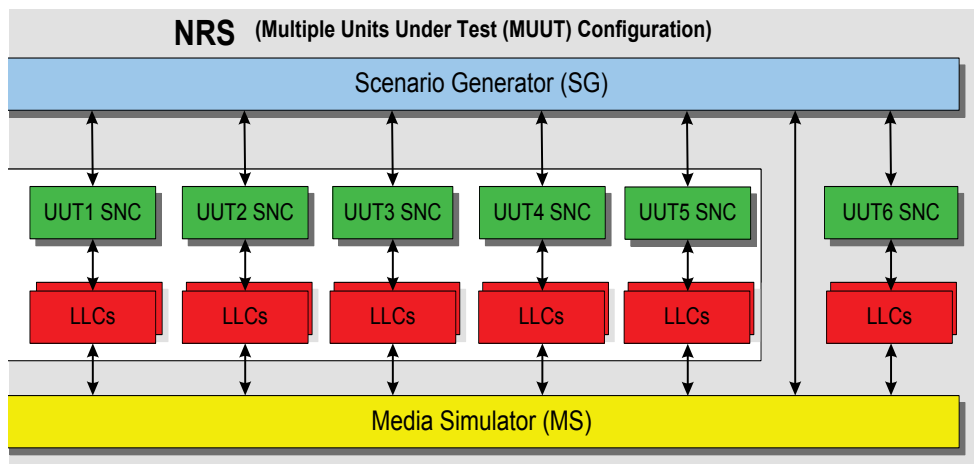


Figure A.1-3 NRS in Multiple Units Under Test mode

This configuration can also be used to test real SPCs or real SPCs with Radios (where MS is not used). If radios are not used then a simulated connection between SPCs has to be provided. For two units this can be a simple back to back wire connection between SPCs. When more than two units are used, there has to be one-to-many connectivity, which can be provided by a COTS matrix switch. [Figure A.1-4](#) shows an example of this configuration (with only five UUTs though six can be run), with the use of real radios.

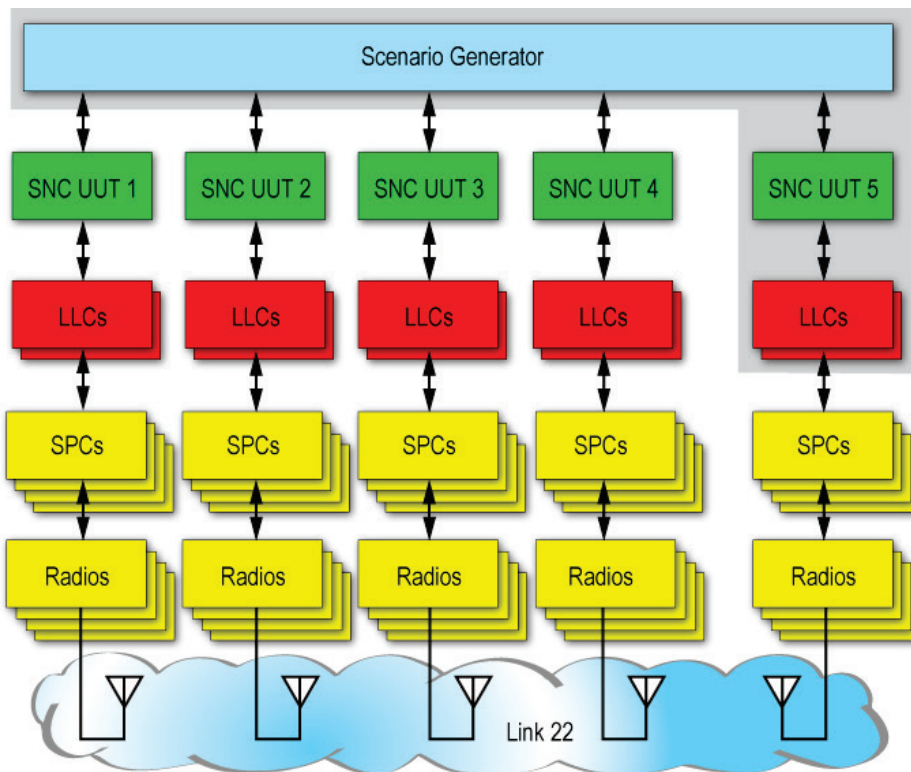


Figure A.1-4 NRS MUUT Used for SPC and Radio Testing

□ **System Simulation**

The System Simulation configuration is used to validate NRS test scenarios. This configuration uses multiple computers to ensure that sufficient computer resources are available, especially when running stress test scenarios. System Simulation involves only units simulated by SNC♦. In this configuration the Media Simulator also simulates the LLCs. System Simulation can support 1-125 simulated units in real time, or up to 25 units running a simulation at four times (4X) normal speed. This configuration is shown in [Figure A.1-5](#).

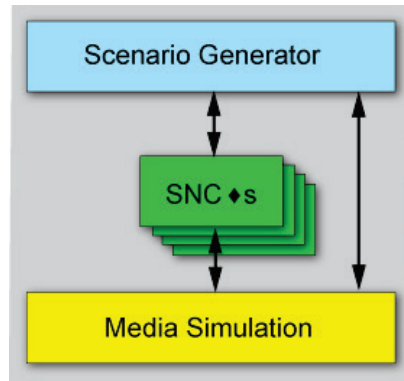


Figure A.1-5 NRS in System Simulation mode

The NRS can run in System Simulation mode entirely on a single computer (a “Single Computer NRS”). NRS versions 9.3 and below do not provide any data extraction capabilities when run on a single computer. In addition, this configuration may not be suitable for stress test scenarios. As computers become more powerful the performance may no longer be an issue.

□ **Media Simulator (MS) Standalone**

The MS Standalone configuration allows the testing of a national DLP without using real SPCs, which are replaced by the Media Simulator. The SG Server is used to initialize the Media Simulator with the appropriate media settings and network parameters. After the initialization has been completed, the SG Server can be terminated and the Media Simulator will await connection from the SNCs. Figure A.1-6 shows the MS Standalone mode of the NRS, using two units back to back. Note that there could be up to six units.

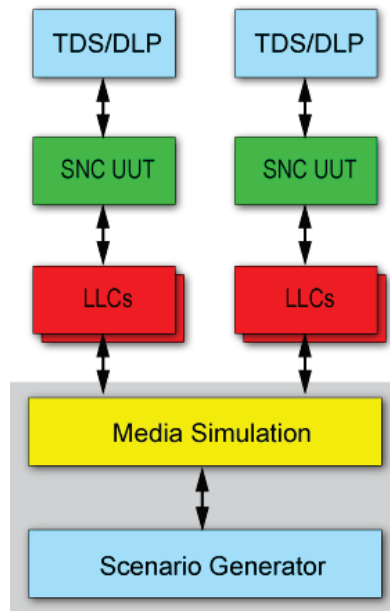


Figure A.1-6 NRS in MS Standalone mode with two units

A.1.3 Scenario Generator (SG) Usage

The Scenario Generator (“SG”) component is used in three phases of the NRS. The three phases of the NRS and their corresponding SG programs are listed below.

- **Pre-Test**
 - Scenario Developer (SD)
 - Scenario Generation (SG)
- **Test Execution**
 - SG Server (SGSV)
 - SG Workstation (SGWS)
 - SG Extractor (SGEX)
- **Post-Test**
 - Data Reduction (DR)
 - Data Analysis (DA)

□ **Pre-Test**

The Pre-Test phase consists of creating a text Scenario File (.SO) and using the Scenario Generation program to produce a binary Scenario File (.SF) from the .SO file. The text based .SO file can either be manually written with any standard text editor, or can be generated using the Scenario Developer's graphical user interface, or extracted from a pre-existing scenario file repository. Scenario Generation generates two output files from the text .SO file: a summary (.SUM) file and a binary Scenario File (.SF). The .SUM file is a text-based file containing a summarization of the scenario including track numbers and initialization information. The .SF file is used in Test Execution by the SG Server to run the scenario. The Pre-Test phase is depicted in [Figure A.1-7](#).

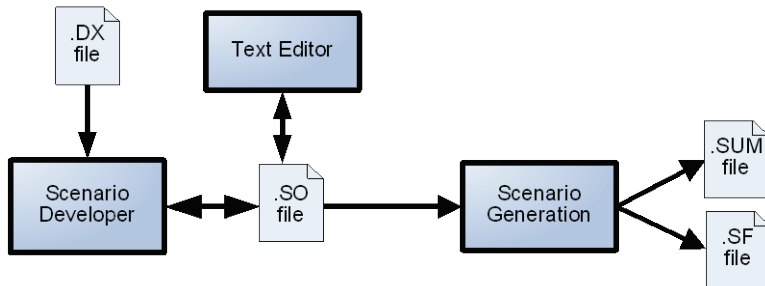


Figure A.1-7 SG Programs in the Pre-Test phase

□ **Test Execution**

The Test Execution phase involves the SG Server, SG Workstation and SG Extractor with other components of the NRS to execute a test scenario as defined in the scenario file. The SG Server reads the binary scenario file (.SF), simulates the DLPs, and controls the execution of the test. The SG Workstation provides the user interface. The SG Extractor records messages passed between the various NRS components into a Data Extraction (.DX) file for post-test analysis, and supplies them to SG Workstation for display.

The Scenario Generator portion of the Test Execution phase is depicted in [Figure A.1-8](#). Data is extracted and recorded from interfaces to other components, as well as interfaces between SG programs.

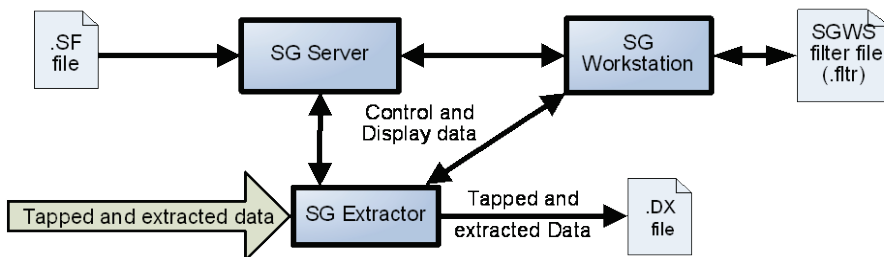


Figure A.1-8 SG Programs in the Test Execution phase

Test Execution can be performed with the different configurations, as detailed above in section [A.1.2 NRS Configurations](#).

□ **Post-Test**

Post-Test involves using the SG Data Reduction (DR) and/or SG Data Analysis (DA) programs on a Data Extraction (.DX) file from a previous Test Execution run.

Data Reduction uses a set of filters based on unit numbers, interfaces, networks and message types to produce an output file containing formatted messages. This output file is a simple text file with the extension of .DR.

Data Analysis is used to replay a Data Extraction file and to perform Expected Response comparisons to verify that expected events occurred within the applicable constraints. A summary list of expected response results is produced as a .TXT file. The Post Test phase is depicted in [Figure A.1-9](#).

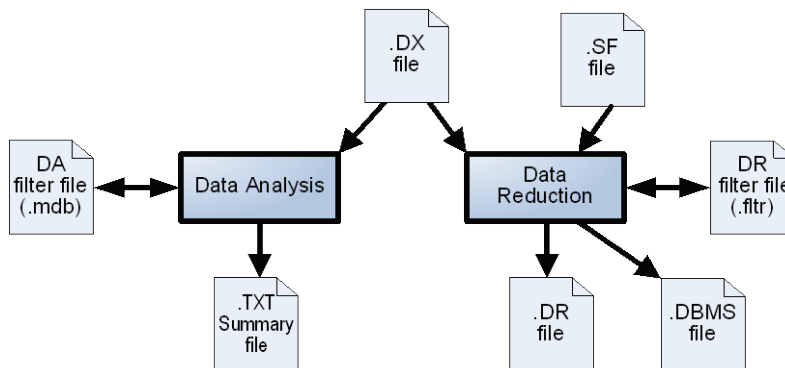


Figure A.1-9 SG Programs in the Post-Test phase

A.2 MLST3

The goal of the Multiple Link System Test & Training Tool (MLST3) is to provide a test tool that supports the development, life cycle support, and performance validation of the tactical data link systems employing Link 22, Link 16, JREAP and Link 11, as well as other communication interfaces. MLST3 provides capabilities to support the following test types.

- Conformance Tests
- Interoperability Tests
- System Integration Tests

MLST3 allows conformance and interoperability tests to be performed to verify the compliance of tactical data link systems implementation with the requirements set forth in the agreed standards and specifications. In addition, MLST3 provides facilities for developmental testing activity to achieve integration of tactical data link system components (for example, Host/Data Link Processor (DLP), System Network Controller (SNC), and communications equipment).

MLST3 was designed to re-use existing NRS components, to take advantage of the existing capabilities to the maximum extent possible, and to reduce development costs. The MLST3 standard hardware configuration for Link 22 is also suitable as an NRS. MLST3 and NRS/SNC software distribution and the authorization to use them are managed by different organizations.

This section covers the following topics.

- MLST3 Components
- MLST3 Configurations
- MLST3 Programs

A.2.1 MLST3 Components

The MLST3 provides multiple test configurations for different purposes, most of which require the approved use of SNC and NRS components, the distribution of which is managed by the NILE PMO. Similar to the NRS, MLST3 provides tools for scenario development, test execution, data recording and post-test analysis.

MLST3 provides active recording of the DLP-SNC Interface and the information exchanged between MLST3 and MS. It can also re-use the NRS SGEX, but does not provide the capability to verify expected responses. MLST3's post-test Automated Data Analysis Tool (ADAT) focuses on aspects of the Tactical Data Link message generation including recurrence rate. Scenarios generated for NRS are not interchangeable with MLST3, even though the differences are minor.

MLST3 can interface with a single SNC♦, providing DLP simulation for up to 32 simulated units. It can support up to five additional UUTs, for a total of 37 NILE units.

MLST3 can reuse the following NRS components previously described in the NRS section.

- SG Extractor program
- SNC and SNC Diamond
- LLC or LLC Simulator
- SPC/Radio or Media Simulator

A.2.2 *MLST3 Configurations*

The different MLST3 configurations are the following.

- Multiple Units
- Live Link
- System Simulation
- NCE Simulation
- Single

All of the above configurations require the approved use of SNC and NRS components, the distribution of which is managed by the NILE PMO. The NRS and MLST3 components may be run on a single computer or multiple computers for all relevant configurations.

MLST3 when used in standalone mode, mainly used as a training tool, does not require any other Link 22 HW or NRS SW.

Due to the serial connection speed requirements between LLCs and SPCs, or between LLCs and MS, LLCs and SPCs/MS are recommended to be co-located. When a SNC UUT is not co-located with MLST3, one of the following physical hardware schemes is typically used.

- LLCs and real SPCs/Radio co-located with SNC UUT
- SNC UUT LLCs and MS all co-located with MLST3
 - The SNC UUT- LLC connection must be provided by a secure transmission mechanism that meets timing requirements

□ **Multiple Units**

In this configuration, up to five SNC UUTs can be run with up to 32 simulated units provided by the SNC♦. Each SNC UUT is connected to a Host/DLP. MLST3 simulates the DLPs for the SNC♦ units.

Figure A.2-1 shows an example of the Multiple Units configuration of the MLST3, with three SNC UUTs and their Host/DLP remotely located from the MLST3, with secure communication between SNC and LLC.

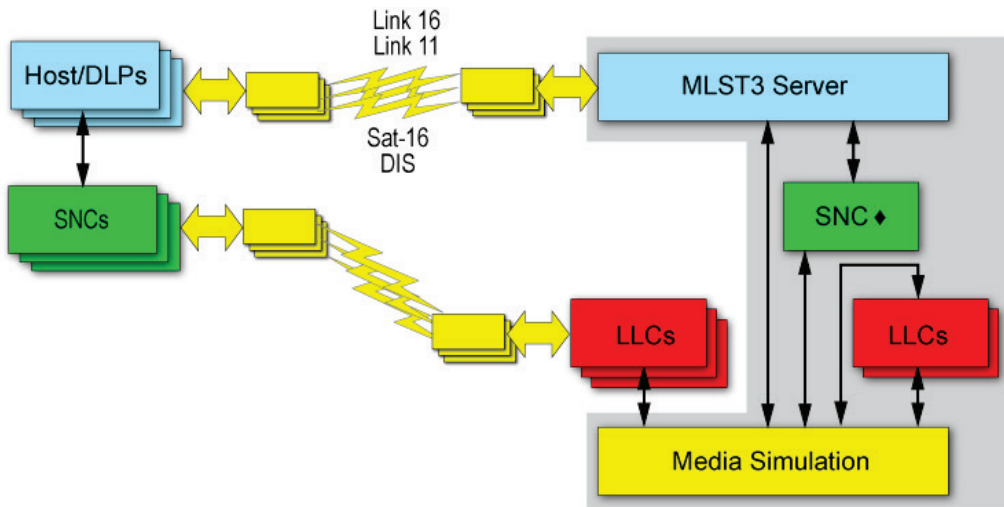


Figure A.2-1 MLST3 Single against MLST3 Server configuration

The main purpose of this configuration is to test national DLPs using a real SNC, with the MLST3 providing the remainder of the test environment. The DLP/SNC UUT may or may not be co-located with the MLST3. The DLP and SNC can be separated, but the feasibility of such a configuration is subject to security requirements and timing issues related to the physical network distribution.

□ **Live Link**

The MLST3 Live Link configuration is similar to the Multiple Units configuration except that real SPCs are used to provide connectivity between the units on any Live Network. In this configuration the MLST3 can support both Live Networks using real SPCs, and simulated networks using MS. Real SPCs and MS SPC simulation cannot be combined on the same network. Only two units can be present per Live Network, one being simulated by the MLST3 and the other being a real DLP or a MSLT3 Single. Up to four Live Networks can be defined. MLST3 simulates the DLPs for the SNC ♦ units. Physically, the Media Simulator associates a specific port of the LLC to a simulated unit defined in the scenario to be live on a network. Figure A.2-2 depicts the MLST3 in Live Link mode with one Live Network, in addition to simulated networks.

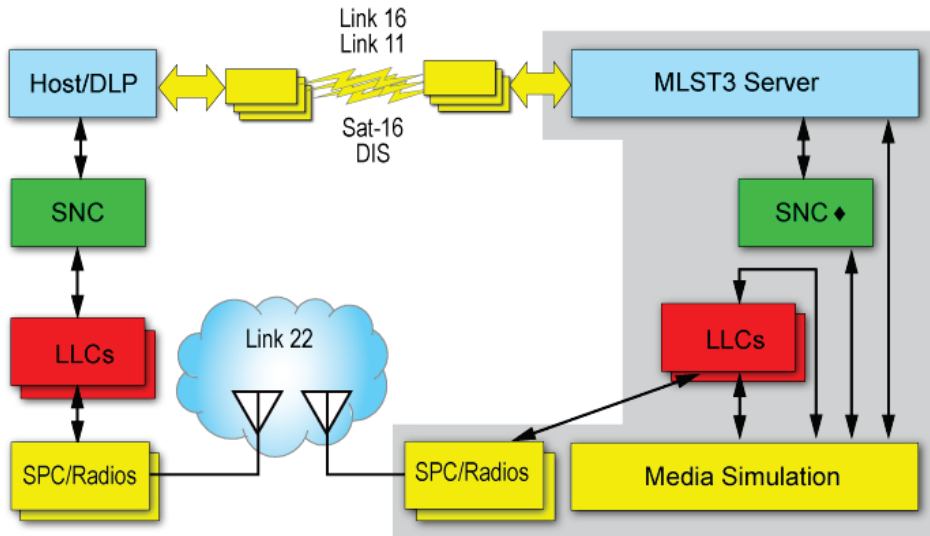


Figure A.2-2 MLST3 Live Link Configuration

□ **System Simulation**

The System Simulation configuration is a lightweight simulation environment that requires just the SNC♦, Media Simulator and the MLST3 software to achieve a Link 22 simulation for up to 32 units. MLST3 simulates all of the DLPs. These three applications can all run on a single PC without any extra hardware (such as serial rocketports), making this configuration portable and rapidly deployable. Active MLST3 data recording can be used to verify tactical traffic and the DLP-SNC♦ interface. [Figure A.2-3](#) shows the System Simulation configuration of the MLST3.

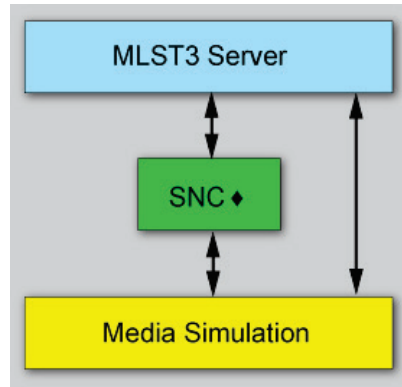


Figure A.2-3 MLST3 in System Simulation mode

□ **NCE Simulation**

The NCE Simulation configuration is an extension of the System Simulation configuration. When using NCE Simulation, the MLST3 provides a proxy layer by assigning up to five Host/DLPs to their own unique simulated SNC♦ unit, through an SNC-to-SNC♦ adaptation layer. This proxy layer is transparent to the DLP because it connects to the MLST3 exactly the same way as it would an SNC UUT. This configuration supports the testing of a newer version of the DLP-SNC interface by using a newer version of the SNC♦, even when the interface version is not supported by MLST3. Additional simulated DLPs can be provided by MLST3, for a total combination of up to 32 units. This configuration shares the portability and lightweight advantages that the System Simulation provides. By enabling testers and integrators to “plug” a real DLP into a single-computer Link 22 simulated environment, the NCE Simulation configuration provides a rapid, lightweight DLP-SNC interface testing environment. Like the System Simulation configuration, NCE Simulation can be run entirely on one computer. [Figure A.2-4](#) shows the NCE Simulation configuration of the MLST3.

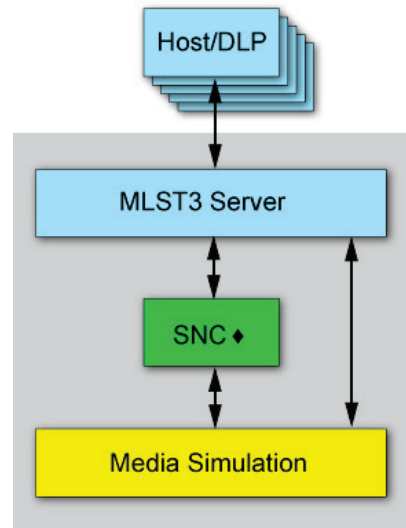


Figure A.2-4 MLST3 in NCE Simulation mode

□ *Single*

MLST3 can also be used as a single unit DLP. In this manner, up to 125 separate instances of the MLST3 could be used, each controlling a unique SNC, to simulate up to 125 units. Real DLPs and MLST3 Single can be combined as in [Figure A.2-5](#) to provide a Link 22 environment.

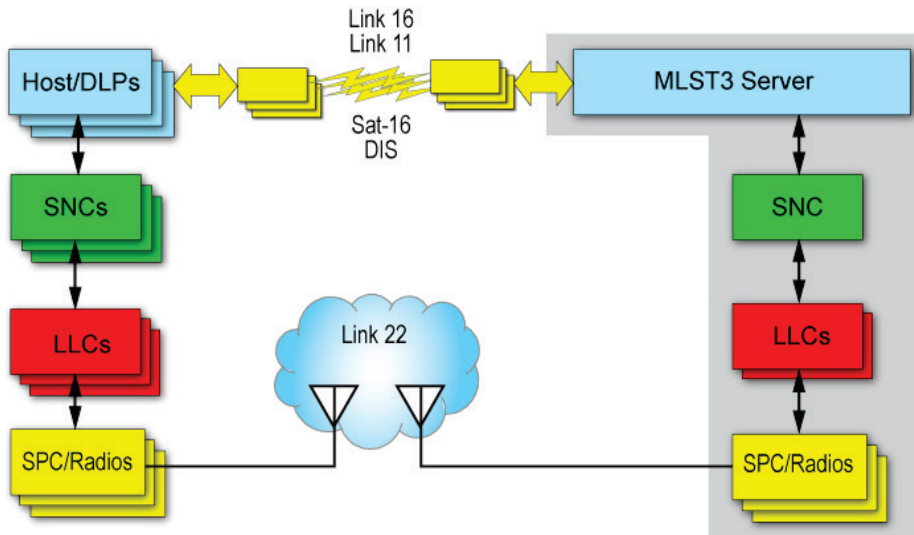


Figure A.2-5 MLST3 Single and Real DLPs

A.2.3 *MLST3 Programs*

Similar to the NRS, the MLST3 software includes several applications for use before, during, and after a test run, as detailed below.

- **Pre-Test**
 - Multi-Link Scenario Developer (MLSD)
 - File Conversion Utility
 - Product Configuration
 - Network Configuration
- **Real-Time Test**
 - Multiple Link Test System (MLTS)
 - DLSSEdit (Default text editor)
 - Documents (SUMs)
- **Post-Test**
 - Data Reduction (MLDR)
 - Automatic Data Analysis Tool (ADAT)

□ **Pre-Test**

The Multi-Link Scenario Developer (MLSD) program is used to create (or update existing) scenario text files (.SO) and to generate scenario binary files (.SF) for execution, as shown in [Figure A.2-6](#). Capabilities in MLSD are also available on-line during exercise conduct.

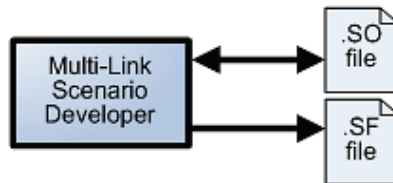


Figure A.2-6 MLST3 Pre-Test

The terminal load file conversion utility allows conversion of Link 16 terminal initialization data files into a number of different formats for use by the real time program.

The Product Configuration utility allows setup and customizing the configuration of all available links and options, including Distributed Interactive Simulation (DIS).

□ **Real-Time Test**

The MLTS Real Time consists of two programs, the Data Link Server, and the Test Controller User Interface (TCUI), as shown in [Figure A.2-7](#). The MLTS Data Link Server program provides for the following capabilities.

- Maintains track databases
- Performs Message Processing
- Provides data to TCUI for display
- Extraction of MLST3/DLP – SNC (or SNC♦) interface

The Test Controller User Interface program is responsible for the following.

- Provides the Human Machine Interface
- Displays the Tactical messages
- Provides the Tactical Situation Display

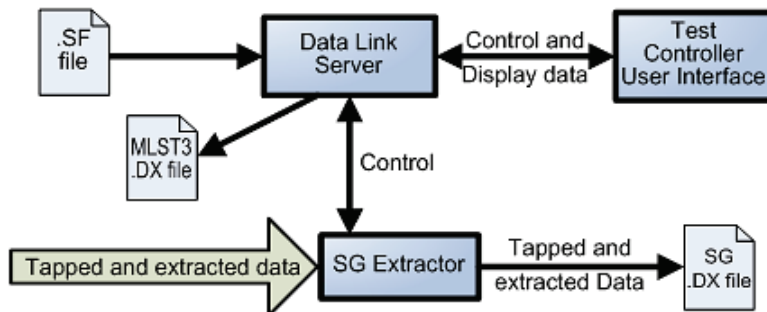


Figure A.2-7 MLST3 Real-Time

DLSSEdit is a text editor used to edit ASCII (scenario or configuration) files. MLST3 provides a convenient way of accessing an electronic version of the following Software User's Manuals (SUMs) through the help menu.

- Scenario Generator User's Manual (MLSG)
- Real Time User's Manual (MLTS)
- Post Test User's manual (MLDA)

□ **Post-Test**

Post test programs are used upon completion of the Real Time program, and process data extraction files (.DX) that have been created during real time, as detailed below, and shown in [Figure A.2-8](#).

Data Reduction converts binary data into a human-readable text formatted report. This report is output to a disk file or line printer. Data can be filtered in many ways selectable by the Operator.

ADAT analyzes messages for adherence to standard requirements. Input consists of data extraction files and output consists of an analyst data file (.ADF) and report file (.RPT).

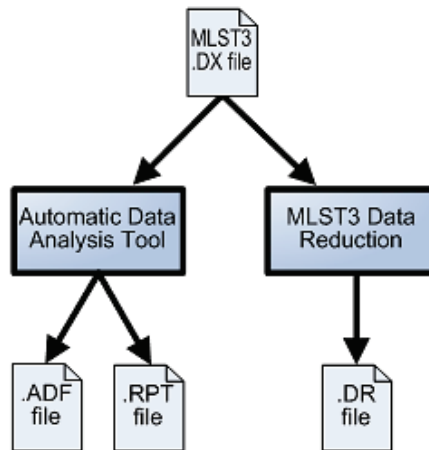


Figure A.2-8 MLST3 DX

Appendix B

Troubleshooting

This appendix provides useful information when establishing and troubleshooting Link 22, including the following topics of discussion.

- OLM Information Extraction
- Fault Management
- Error Rate Characteristics
- DLP
- SNC
- LLC/SPC
- Key Rollover
- TOD
- System Level Problems
- Frequently Asked Questions

B.1 OLM Information Extraction

Most systems will automatically determine their own unit information and hardware requirements from the OLM and hardware configuration files, so that the operator does not need to look at the OLM. For example, the software may automatically select the unit's Link 22 address from the OLM based on the unit's known Unit Designator. The selection of LLC/SPC may be automatically determined based on configuration files and the unit's inclusion in networks in the OLM. The system may also automatically display the required crypto information for the Crypto Operator.

If the system does not automatically determine all required initialization information, the operator may need to examine the OLM file. [Chapter 2, Section 2B.3](#) gives a general identification of the sets and fields in the OLM used by Link 22. This section explains how to manually determine the fields that apply to own unit, which may require operator action or entry. The fields in the OLM data sets that are of interest to the operator are shown in **red text**.

The OLM examples given in this guidebook are based on the OLM definition at the time of publication. Current OLM definitions may differ. The following topics are further expanded.

- Determining Own Unit
- Determining Network Membership
- Determining Media Requirements
- LLC/SPC/Radio Selection
- Determining Cryptographic Requirements
- Determining Day Of Week
- Radio Silence Network Initialization

B.1.1 Determining Own Unit

The Link 22 Address of a unit is contained in the OLM in an NUDATA set. The structure of a NUDATA set and the location of the Link 22 Address within it are shown in [Figure B.1-1](#). The Link 22 address is extracted from the set which has the Unit Designator and/or Callsign of the unit.

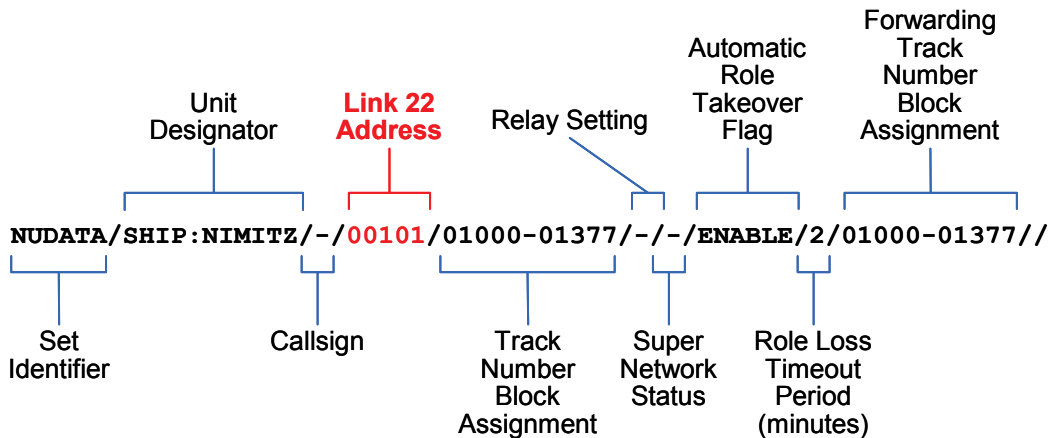


Figure B.1-1 Determining Own Unit Link 22 Address from the OLM

B.1.2 Determining Network Membership

The networks to which own unit is assigned are identified by a two step process, as described below.

- Find Network Membership
- Get NILE Network Identifier

□ Find Network Membership

First the NNETPART sets should be checked to find those that contain the own unit's Link 22 Address, as shown in [Figure B.1-2](#). This tells the operator that it is a member of a network, but not which network.

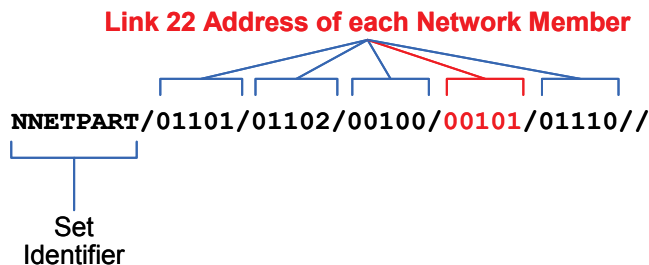


Figure B.1-2 Check Own Unit Participation from OLM

□ **Get NILE Network Identifier**

Next, the network identifier associated with the network is determined by looking at the Network Identifier field in the NNET set that immediately precedes the NNETPART set. The location of the Network Identifier in the NNET set is shown in Figure B.1-3.

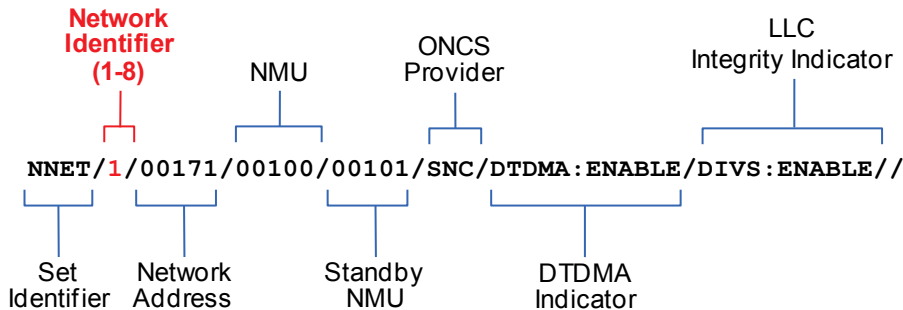


Figure B.1-3 Determining Network Identifier from OLM

Note: Network Identifiers in the OLM have a range of 1-8. Network Identifiers in the DLP-to-SNC interface and the SNC-to-SNC technical messages have a range of 0-7. Different national implementations of user interfaces may require a conversion from OLM network identifiers to DLP-SNC interface network identifiers by subtracting 1 from the OLM value.

B.1.3 Determining Media Requirements

Media requirements are determined by examining the OLM. A radio is needed to support the media type for each network for which own unit is a participant. Radio power is currently not specified in the OLM; it should be set in accordance with national procedures. Link 22 can automatically control the Radio power setting when the SPC and radio being used provide the capability. The radio procedures should be followed for setting the frequency and power of each radio manually, if necessary.

The Media requirements of the networks for which the unit is a participant are determined by looking at the Media Type and Frequency fields in the NNMEPARS set, as shown in Figure B.1-4.

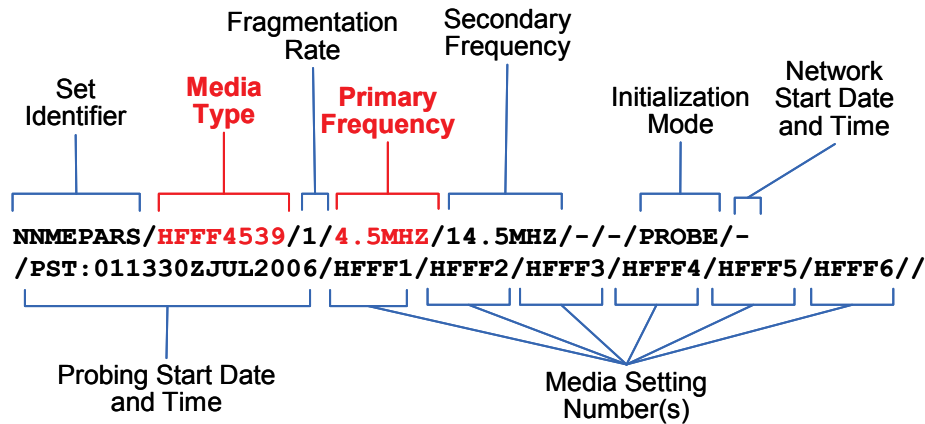


Figure B.1-4 Determining Media Requirements from OLM

B.1.4 LLC/SPC/Radio Selection

Each network in which the unit is participating needs to be associated with an LLC, SPC and radio.

The total number of available LLCs should be able to support the required throughput. A single LLC can handle up to four networks, with any combination of media type (HF or UHF). Each LLC is assigned an identifying number from 1 to 4, and a unique IP Address.

Each SPC is connected to one of four SPC ports (0-3) on the back of the selected LLC for each network. The radio selected is connected with the SPC.

The mechanism to pair LLC number (1-4) and SPC port (0-3) for each network in which the own unit is a participant may be automated. If manual assignment is required, the LLC (1-4) and SPC port (0-3) for each network for which the own unit is a participant needs to be selected.

B.1.5 Determining Cryptographic Requirements

Loading of the Cryptographic information is dependent on the key management plan and the manner in which keys are distributed nationally. This section includes the description based on the NILE LLC Device Key Management Plan [LLC KMP]. The crypto keys to be loaded into the LLCs are identified by the two sets described below.

- Link 22 Network Cryptographic Resource Description
- Link 16 and Link 22 Cryptographic Data

□ Link 22 Network Cryptographic Resource Description

The NCRYPLST set contains the Crypto Variable Logical Label (CVLL) and its start time, as shown in Figure B.1-5.

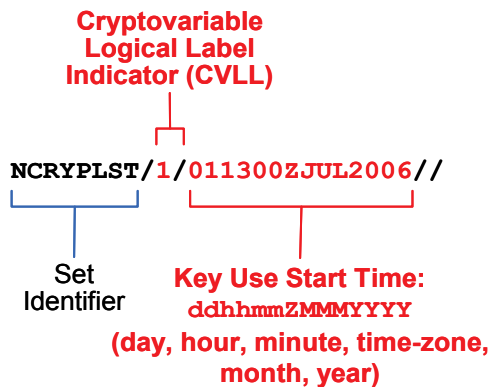


Figure B.1-5 Determining CVLL from OLM

□ Link 16 and Link 22 Cryptographic Data

The CVLL is further described in the Link 16 and Link 22 Cryptographic Data (JCRYPDAT) set, Key Short Title and Encryption Key Short Title fields, as shown in Figure B.1-6. These fields define which key information is to be loaded into the LLCs.

The optional Secure Data Unit (SDU) location number (0-63), if present, indicates what LLC Key Position the keys are expected to be loaded into the LLC.

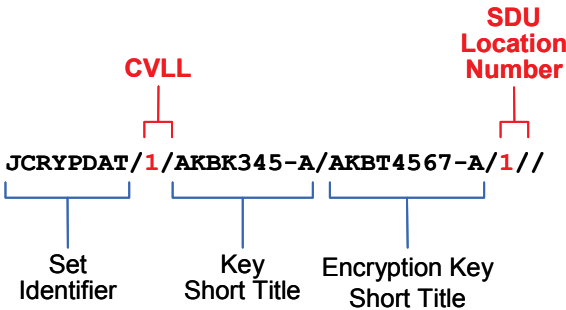


Figure B.1-6 Crypto Data in the OLM

B.1.6 Determining Day Of Week

The LLCs are loaded with the crypto keys that are valid for the current day prior to the time specified in the OLM. A single key is valid for 7 days. A full discussion of Crypto Key Management is included in Chapter 3, Section 3B.6.4.

The correct Day Of Week (DOW) is needed by the LLC for proper encryption/decryption processing. The Link 22 DOW is defined to start at 1 on the day specified in the Link 22 Super Network Information (NSNET) set, in the Operational Start Date and Time of the Super Network field, as shown in Figure B.1-7. In this example July 1, 2006 is considered to be DOW 1. If today is July 3, 2006, then the current DOW is 3. July 8, 2006 would be DOW 1 of Week 2.

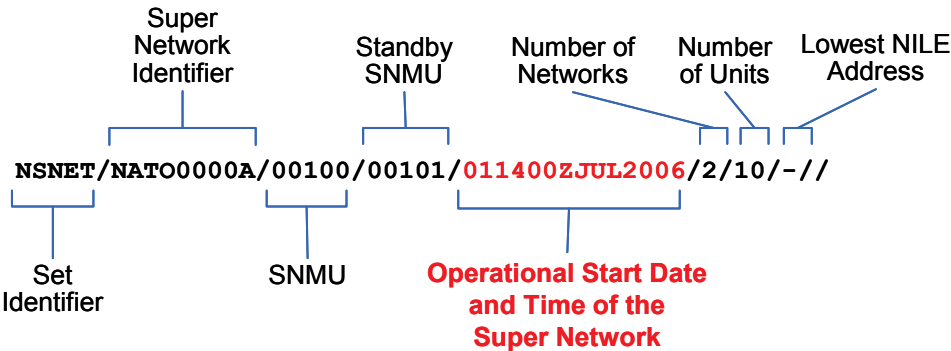


Figure B.1-7 Determining Day Of Week from OLM

Each LLC's current DOW (1-7) is initialized by the SNC to be the SN DOW that the DLP provides to the SNC. The SNC does this by ensuring that no ports are configured in the LLC and then configuring the LLC with the Reset Day Of Week flag set and the SN DOW field set appropriately, when the SNC is initializing the LLCs.

B.1.7 Radio Silence Network Initialization

The optional NUNNRS set may follow the NUDATA set, and refers to the unit specified in the NUDATA set. The NUNNRS set lists the networks that the unit should set in radio silence before the unit initializes the network, and is shown in Figure B.1-8.

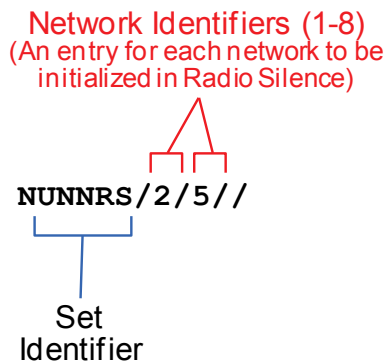


Figure B.1-8 Radio Silence Network Initialization

B.2 Fault Management

The SNC reports faults through the 800-series messages and ‘SNC Status’ (413h) message. If a nation’s DLP implementation does not handle the fault automatically, the operator should take corrective actions. The two following topics are further detailed.

- SNC Reported Conditions
- LLC/SPC Recovery

B.2.1 SNC Reported Conditions

When there is a fault the SNC will automatically report it to its DLP. The following is a list of faults that the DLP may receive from its SNC.

- LLC Disabled
- SPC Disabled
- LLC Configuration Failure
- SPC Configuration Failure
- SPC Alarms/Errors
- LLC Alarms/Errors
- Media Interface Congestion
- Built In Test Failure
- SNC Status
- TOD Failure
- TOD Degradation
- Timeslot Violation

Each fault is further detailed with possible corrective actions.

□ *LLC Disabled*

The SNC may report to the DLP that an LLC is disabled using a ‘LLC Disabled’ (807h) message in the following cases.

- If an LLC does not respond during initialization or re-initialization
- If an operational LLC develops a fault that causes it to become non-operational

- Each time the SNC fails to automatically restore the LLC to the operational state
- When the LLC has been removed from the SNC Media Segment configuration, due to a request from the DLP (as expected, not a fault)

In general, a reset of the LLC may solve this problem. Refer to the LLC Operator's Manual [LLC OPM] for actions. The system has been designed to minimize operator intervention, so the SNC will attempt to automatically re-establish the connection and set-up.

Alternately, the operator can use a different LLC. This requires that the operator perform the LLC/SPC Recovery Actions listed in [Figure B.2-1](#).

□ **SPC Disabled**

The SNC may report to the DLP that an SPC has become non-operational using a 'SPC Disabled' (803h) message, or that it does not respond during initialization, or re-initialization. This may be a hardware or software problem.

The operator can try to reset the SPC or use a different SPC. When using a different SPC the operator should perform the LLC/SPC Recovery Actions listed in [Figure B.2-1](#).

□ **LLC Configuration Failure**

The LLC may reject one or more configuration parameters that have been sent to it by the SNC. The SNC reports this failure to the DLP using a 'LLC Configuration Failure' (80Bh) message.

The DLP can request the status of a LLC using a 'LLC Status Request' (322h) message. The SNC will report a LLC Configuration Failure to the DLP when the current LLC Status values returned by the LLC to the SNC do not match the values the SNC previously supplied to the LLC.

The operator can request that the DLP try to reconfigure the same LLC with a different set of parameters, or the operator can use a different LLC, following the LLC/SPC Recovery Actions listed in [Figure B.2-1](#).

□ **SPC Configuration Failure**

The LLC may report the rejection of one or more SPC configuration parameters that have been sent to it by the SNC. This may be a hardware or software problem. The

SNC reports this failure to the DLP using a ‘SPC Configuration Failure’ (801h) message.

The operator can request that the DLP try to reconfigure the same SPC with a different set of parameters, or the operator can use a different LLC/SPC combination, following the LLC/SPC Recovery Actions listed in [Figure B.2-1](#).

□ **SPC Alarms/Errors**

The media may send an SPC Alarm report message to the SNC if it detects a fatal SPC hardware or software related fault, or it may send an Error Report message if it detects a fault that is not fatal. The SNC reports these alarms and errors to the DLP using a ‘SPC Alarm/Error Report’ (80Fh) message, which can then provide them for display to the operator.

Examples of SPC alarm conditions are include below.

- SPC has exited the TDMA mode
- SPC failure
- Radio failure

Refer to [LLC/SPC Section B.6](#) for further details about each SPC alarm and error.

The SNC automatically terminates transmission on the networks affected by the fault. If a power reset does not fix automatically the problem, the operator can fix the SPC or use a different SPC, following the LLC/SPC Recovery Actions listed in [Figure B.2-1](#).

□ **LLC Alarms/Errors**

The LLC may send an Alarm Report message to the SNC if it detects a fatal fault, or it may send an Error Report message if it detects a fault that is not fatal. The SNC reports these alarms and errors to the DLP using a ‘LLC Alarm/Error Report’ (806h), which may be able to provide them for display to the operator.

Alarms generally represent anomalies in SNC-to-Media operation for which recovery action should be taken by an operator or system maintainer, as described in the LLC/SPC Recovery Actions listed in [Figure B.2-1](#). Examples of alarm conditions include the following.

- COMSEC key-related alarms (e.g., no keys present)
- Hardware failures

■ Software failures

Alarms may affect operation of all media.

Errors generally represent anomalies in SNC-Media operation, such as problems with the partitions, checksums, unknown crypto or bypass message types, incorrect lengths, and so on (for example, BIA_BAD_CRYPTO_PARTITION). Transient error conditions in the LLC are reported as alerts, such as SYS_LOW_BATTERY_VOLTAGE_ALERT, or RIA_NP_INTEGRITY_FAILED. Most of these errors would only occur if new equipment is being integrated.

Some errors may be automatically recoverable by the SNC. Others may take an operator action to correct. Many represent transient conditions that do not preclude further operations, and require no action by the operator. Refer to [LLC/SPC Section B.6](#) for details on each error and alarm.

□ **Media Interface Congestion**

If the SNC detects that the media interface is congested, it will report this fact to the DLP using a 'Media Interface Congestion' (80Ah) message. This occurs when the SNC-to-SPC transmit or receive requests are failing. This usually indicates a failure with the LLC and/or SPC timing.

The operator may need to verify and make corrections to Time Of Day distribution. The operator may want to perform the LLC/SPC Recovery Actions listed in [Figure B.2-1](#).

Media Interface Congestion errors can also occur if the wrong minislot duration is used. For UHF EPM, the SNC gets the minislot duration from the CN2 value in the snc_classified_numbers.ini file, because it is a classified value. If the file is missing, the SNC defaults to an unclassified value that does not match the classified value. The snc_classified_numbers.ini file must be present and must have the correct <CN2> minislot duration value for UHF EPM to function correctly.

□ **Built In Test Failure**

The SNC itself does not perform the Built In Test. Rather, some other program runs a Built In Test and reports the results to the SNC through a shared memory mechanism, so the meaning of the 'Built In Test' (802h) message results are dependent on the Built In Test program. The SNC sends the results the DLP on a periodic basis, as defined in the 'MPT Specification' (301h) message. They may report a hardware or software failure.

□ **SNC Status**

The ‘SNC Status’ (413h) message is sent by the SNC to notify change of status, in the cases listed below.

- After the SNC completes the establishment of the TCP socket link with the DLP. The status indicates whether the initial BIT tests were successful or not. If not then the failure status is contained in the BIT Test Result field, and corrective action is as for Built In Test Failure above
- Whenever the TCP link is re-established (after a communications failure with the DLP due to either link or DLP failure). In this event the SNC Status field is set to indicate to the DLP that the SNC is running
- Whenever a software error occurs within the SNC. The SNC Status field indicates the type of error that has occurred (Error, Info, Warning, Debug), and additional error text may be supplied at the end of the message
- Whenever a condition exists that prevents automatic Role Takeover in the SNC (such as when the connectivity is lost, with all neighbors in one network or in the Super Network). The SNC Status field indicates if the Takeover Status applies to a single network or the overall Super network. The SNC also reports when the condition no longer exists

□ **TOD Failure**

The SNC and each SPC will detect the loss or re-establishment of its Time Of Day (TOD) supply. Each SPC will report the change of TOD supply to the SNC. The SNC reports a loss (by the SNC or an SPC) to the DLP in a ‘TOD Status’ (42Ch) message. The SNC reports a re-establishment (by the SNC or an SPC) in a ‘TOD Status’ (42Ch) message.

Refer to Section [B.8](#) for a full discussion of TOD.

□ **TOD Degradation**

The SNC and each SPC monitor the TOD quality provided by the external time reference system. Each SPC will inform the SNC if a change in the TOD quality affects its ability to transmit. The SNC sends a ‘TOD Status’ (42Ch) message to the DLP whenever transmission stops on any Network, as determined by the SNC, or as reported by an SPC. As soon as the time quality is sufficient for transmissions to resume on the network, as determined by the SNC, or as reported by an SPC, the SNC sends a ‘TOD Status’ (42Ch) message to the DLP.

Refer to Section [B.8](#) for a full discussion of TOD.

□ ***Timeslot Violation***

The SNC reports a ‘Timeslot Violation’ (804h) message to the DLP whenever the SNC detects that a different unit, rather than the authorized unit, transmits in an assigned timeslot without permission.

If DTDMA is on, this is not unexpected. It can occur due to lack of connectivity of all units as timeslots are reassigned. In this case the SNC modifies its internal ONCS to accommodate the change of ownership to the unexpected unit. This change is rolled back at the end of a temporary timeslot reallocation.

The SNC that donates a timeslot to another unit monitors that donated timeslot. If the SNC receives transmissions in the donated timeslot from a unit other than the one that it was donated to, this is unexpected, and the donor SNC reports a Timeslot Violation.

If DTDMA is off, then either the unit detecting the violation has the wrong ONCS, or the transmitting unit has the wrong ONCS. Internal SNC functionality will attempt to automatically correct the situation, by requesting the current ONCS from the NMU.

If the situation does not correct itself, the NMU operator may want to place the violating unit in radio silent mode, or request the unit to closedown on the network and restart with the correct ONCS or through LNE.

B.2.2 LLC/SPC Recovery

When the SNC reports an ‘LLC Configuration Failure’ (80Bh) or a ‘LLC Disabled’ (807h) message to the DLP; the SNC tries to automatically recover from the LLC problem. For example, if the LLC was not powered on, or a cable became unplugged, the operator could simply power on the LLC or plug in the cable, and the SNC would automatically connect to the LLC.

If automatic recovery of a LLC fails, or if there is a problem with a SPC, the operator may want to select a different LLC or SPC, or fix the LLC or SPC, and try again. Sometimes recovery can be obtained by power cycling the faulty hardware. The operator steps required to recover an LLC or SPC are listed in [Figure B.2-1](#), when configuration changes are required for the LLC or SPC. Additional information is provided in the [\[LLC OPM\]](#) and each SPC user manual.

Step	Action
1	The operator indicates that an LLC or SPC should stop being used.
2	The DLP will inform the SNC to closedown on the related network(s), and then remove the LLC from the SNC Media Segment configuration, if the LLC is to be replaced.
3	The operator replaces or repairs the bad LLC or SPC. If replacing a LLC and the DOW for the new LLC is known, the operator must ensure the correct Crypto Keys are loaded into the new LLC.
4	The operator indicates that the new or repaired LLC or SPC is ready to be used. The operator either supplies the known LLC DOW, or indicates that the DOW is unknown and requires a reset.
5	The DLP sends the SNC configuration information for the new or repaired LLC and/or SPC.
6	If the LLC DOW was unknown, after the DOW has been reset, the operator must reload Crypto Keys, because a DOW Reset clears the keys.
7	The DLP initializes itself on the network again.

Figure B.2-1 LLC/SPC Recovery Actions

The recovery protocol operator actions and message flow is shown in [Figure B.2-2](#).

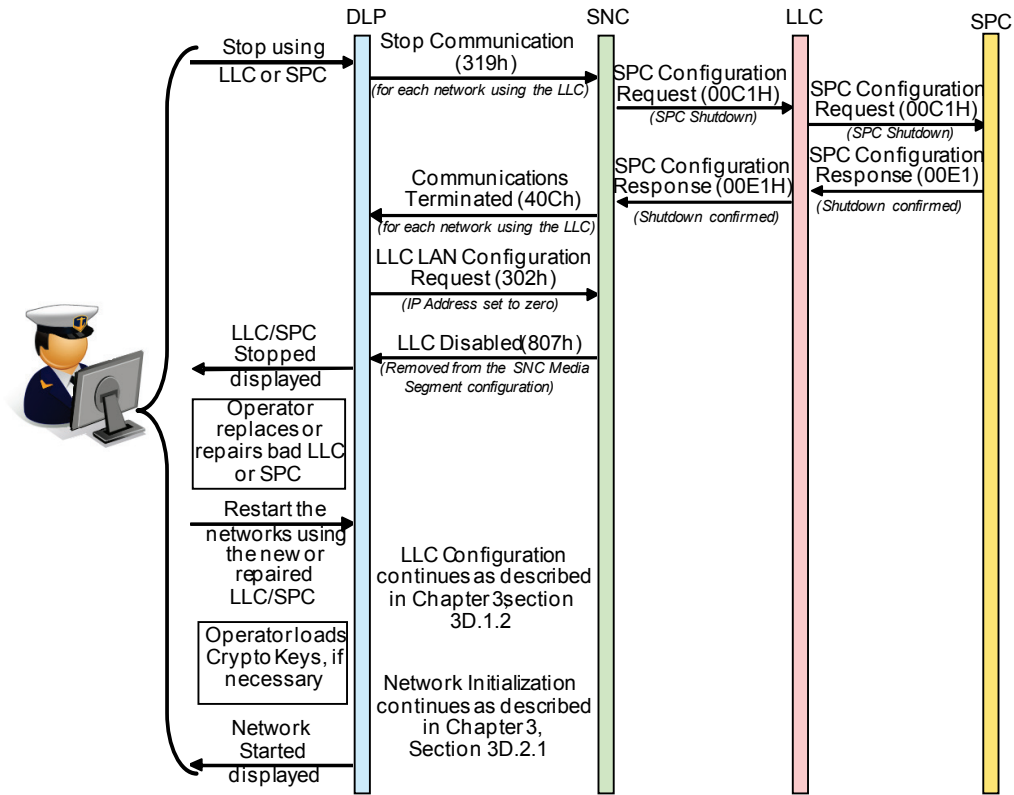


Figure B.2-2 Manual LLC/SPC Recovery

B.3 Error Rate Characteristics

For each network, at the end of each Network Cycle Time (NCT), the SNC reports the percent of Network Packets (NPs) received without errors, the percent of NP received with various types of errors, and the percent of NPs that were not received, as listed below.

- Percentage of NP with no errors
 - This should be the great majority of Network Packets. When this value decreases this indicates that the connectivity is becoming worse
- Percentage of NP with one or more corrected errors
 - The SPC used its Error Detection and Correction (EDAC) algorithms to correct errors. The Network Packet is flagged as corrected by the SPC so that the SNC is aware of the correction
- Percentage of NP with uncorrected errors
 - These are the Network Packets that the SNC does not receive because the SPC detected errors that it could not correct
- Percentage of NP not received
 - This occurs if a unit is not transmitting, or the transmitted data is not received if the two units are beyond the RF-range for the media
- Percentage of NP that failed LLC Integrity checks
 - Occurs only if LLC Integrity is on. It is the total percentage of all Network Packets that failed LLC Integrity. The next two fields give more details about these failures, and their sum will approximately equal this field's value. The total may be off slightly due to rounding
- Percentage of NP with no errors that failed LLC Integrity checks
 - No errors were reported by the SPC, but the NP still failed LLC Integrity
- Percentage of NP with one or more corrected errors that failed LLC Integrity checks
 - The SPC corrected some errors, but the NP still failed LLC Integrity
- Percentage of NP with no SPC detected errors that the SNC rejected due to invalid structure or content
- Percentage of NP with one or more corrected errors that the SNC rejected
 - This is reported if LLC Integrity was off, or if LLC Integrity was on and the NP passed LLC Integrity, and the SNC detected an error in the NP

The first four fields identified above should add up to 100%, although rounding may slightly affect the total. If there are a lot of errors, connectivity between this unit and other units may decrease.

Every unit operator can use the Error Rate Characteristics to detect possible errors. Large amounts of errors could indicate one of the following situations.

- RF conditions are not good
- LLC/SPC hardware problem
- This or another unit has the wrong media parameters
- This or another unit has the wrong ONCS

If the unit operator suspects a hardware problem, the operator may want to perform the LLC/SPC Recovery Actions listed in [Figure B.2-1](#).

If the unit operator suspects that the unit does not have the right media parameters or ONCS, the unit should stop communications on the network, and then perform Late Net Entry on the network, so that the unit can get the correct parameters and ONCS.

B.4 DLP

Any DLP implementation is a national responsibility in accordance the Link 22 specifications. This section discusses problems related to the DLP-SNC interface, as listed below.

- [Recovery after a Failed DLP-SNC Connection](#)
- [Recovery after a DLP or SNC Failure](#)

B.4.1 Recovery after a Failed DLP-SNC Connection

The DLP may fail to connect to the SNC for the following reasons.

- The SNC is not running or has failed to initialize itself
- Communications to the SNC not working
 - Network cabling failure
 - Network hub failure
- An incorrect SNC IP address or IP port number, is used

An existing connection between the DLP and SNC could fail for the following reasons.

- Hardware reset of the DLP or SNC processor
- Failure of the SNC software
- Failure of the DLP software
- Physical hardware failure
 - SNC or DLP Processor failure
 - Network cabling failure
 - Network hub failure

When the connection is lost, the DLP and/or SNC continue to the maximum extent allowed, storing messages to be sent after the connection has been re-established. If the storage area becomes full, the oldest messages are discarded.

After the DLP-to-SNC connection is re-established, one of the following options can be performed.

- Continue processing as though the network link did not fail. This technique is useful if only the connection failed, but both the DLP and SNC have continued to operate
- Continue processing, but clear any stored messages. This is useful if the DLP failed, but the SNC is still operational
- Reinitialize the SNC. This is necessary if both the DLP and SNC have failed

B.4.2 Recovery after a DLP or SNC Failure

If the DLP or SNC is restarted after a failure, and the current Link 22 SN Directory data is known to be different than the data in the original OLM, the changes from the original OLM can optionally be provided during SNC Initialization. Whether these changes are supplied automatically by the system or manually by the operator is a national implementation detail.

SN Directory data that may have been updated since the original OLM used to initialize the Super Network are listed below.

- Addition of NILE Unit Addresses
- Role changes
- NU Status and Relay Setting changes
- Mission Area Sub Network (MASN) changes

If the operator is supplying the changes manually to the DLP, for other than role changes, the operator has two options.

- Supply every change since the original OLM, and the order the changes occurred within each category listed above
- Supply only the current values, and inform the DLP that the history of changes is unknown

Supplying changes from the OLM may be useful if the unit may be acting as the SNMU in the future. The SNC maintains a number of changes for each of the above

components, except for the Roles, as detailed in [3B.1.3 Super Network Directory Configuration](#) and [3B.5 SN Directory Maintenance](#). After the system regains operational status, the DLP operator should send a request for SN Directory Update.

A restart requires that the current SN DOW be used in place of the OLM SN DOW. Network start times may need to be updated based on the 12 hours rule. Refer to [Chapter 2, Section 2C.1.4](#) for further details.

B.5 SNC

The SNC may produce errors due to incorrect input, unexpected events or software errors within the SNC itself. An SNC initialization file can optionally be used to control where any errors are reported. This section details the initialization file and lists the errors, and so consists of the following subsections.

- [Optional SNC initialization file \(snc.ini\)](#)
- [SNC Errors](#)

B.5.1 Optional SNC initialization file (snc.ini)

The SNC has an optional initialization file with the name `snc.ini` that is used to control certain SNC functions, by providing the following optional parameters.

- [Console Window Flag](#)
- [SNC Server IP Address](#)
- [SNC Timing Parameters](#)
- [Logging Information Flags](#)

□ Console Window Flag

This flag controls whether the SNC uses a console window for I/O. If set to true then the SNC will write error messages to the console window if any occur during TOD initialization, and will also output the HMI data (basic status line) periodically. For an embedded system without a console window the flag should be set to False.

□ ***SNC Server IP Address***

The SNC Server IP Address defaults to 0.0.0.0 if no snc.ini file exists, or there is no entry in the file. This is a valid default value, and an actual entry in the file is only needed if more than one SNC or more than one SNC♦ is run on the same computer. Each executable uses a unique IP port number, but if there is more than one instance then each needs to use a different IP Address.

□ ***SNC Timing Parameters***

The SNC has a set of timing parameters which have default values that do not need to be changed normally. The initialization file can contain different values for the timings which may need to be used for specific implementations, and thereby allow the tuning of the timing.

□ ***Logging Information Flags***

By default the SNC (when no snc.ini file exists, or there is no entry in the file) logs information by sending it to the DLP using a 'SNC Status' (413h) message. This can be changed to log the information to the console window or to a log file. The location of the log file can be specified in the initialization file. The initialization file can also contain a flag that controls the level of the information that is logged. When there are problems, changing the level of information logged may provide extra details about the problem. There are also flags that control the number of errors that can be logged to a file (controls file size) and the maximum number of log files to be used. The error information logged is described in the following section.

B.5.2 SNC Errors

The SNC can log error information either to its DLP (that can be displayed to the operator), to its display window, or to a log file. This section covers the following topics.

- SNC Console Window Errors
- SNC Initialization Errors
- Bad SNC Status
- Failure of SNC System
- Rejected Messages

□ SNC Console Window Errors

Figure B.5-1 lists the errors that the SNC may report to the console window, with corrective actions, if any.

Error Report	Corrective Actions
SNC-DLP: OFF or FAIL	Make sure the DLP is working properly, including the Ethernet cable
SNC-LLC with LLC 1-4: OFF or FAIL	Make sure the relevant LLC is working properly, including the Ethernet cable. No alarms should be present. Power cycle or replace LLC
Problem reading TOD, waiting for good data	Ensure ReadTOD.exe is running and external TOD working properly (if available)

Figure B.5-1 SNC Displayed Errors

□ SNC Initialization Errors

SNC initialization is composed of the following phases and sub-phases.

- Start of SNC Initialization
- LLC Configuration
 - LLC LAN Configuration
 - LLC Port Configuration
- Super Network Directory Configuration
 - SN Directory Initialization
 - SN Directory Update
- End of SNC Initialization

Failures during any SNC initialization phase (should be displayed to the operator) will cause the SNC initialization process to stop. Failures reported by the SNC can be corrected by the DLP without restarting the SNC, as shown in [Figure B.5-2](#).

Error Report	Corrective Actions
SNC negative acknowledgement of 'MPT Specification' (301h) message	Correct invalid parameters, then resend the 'MPT Specification' (301h) message
During LLC LAN Configuration sub-phase: LLC Disabled – TCP Connection Failure LLC Disabled – LLC Response Timeout	Fix LLC problem and try LLC LAN configuration again, by sending another 'LLC LAN Configuration Request' (302h) message, or remove the LLC from the configuration
During LLC Port Configuration sub-phase: LLC Configuration Failure LLC Disabled	SNC will try to automatically recover. Fix the LLC/SPC problem and let the SNC automatically recover, or force a retry of the Port configuration, by sending a 'LLC Port Configuration Request' (303h), or the LAN and Port configuration, by sending 'LLC LAN Configuration Request' (302h), followed by 'LLC Port Configuration Request' (303h). Optionally remove the LLC from the configuration.
SNC negative acknowledgement of any message during SN Directory Configuration or End of SNC Initialization phases	Correct invalid parameters and restart SN Directory Configuration phase from the beginning by sending a new 'Link 22 Super Network Participants' (304h) message.

Figure B.5-2 SNC Initialization Failures

A LLC is removed from the configuration by sending a 'LLC LAN Configuration Request' (302h) message with the IP Address of the LLC set to zero.

❑ Bad SNC Status

The SNC can report its own software and hardware failures. The operator may need to take manual actions to correct the problem, including possibly restarting the SNC, followed by normal SNC initialization.

❑ Failure of SNC System

During normal operation, it is possible that the SNC system will fail while the DLP remains operational. At this point the unit's connections to any networks are lost. After the SNC is restarted, the unit restarts the SNC communication protocol with normal SNC initialization, optionally with a SN Directory update, followed by either Short Network Initialization, or Late Network Entry.

❑ **Rejected Messages**

If the SNC receives a message that it cannot process, it sends a message to the DLP indicating the reason. Some of these errors may be displayed to the operator, which may require operator action. Others may be handled by the DLP.

Tactical message transmission request errors that the SNC can report are listed in [Figure B.5-3](#), including corrective actions that can be taken by the operator.

Error	Cause of Error	Possible Solution
Invalid MTV	Software (DLP)	Correct DLP implementation
Invalid SRID	Software	
Cancelled SRID	Normal occurrence – timing related	None
Invalid Acknowledgement Status	Software	
Invalid Acknowledgement Flag	Software	
Invalid Link 22 Address	Software or Operator	Reenter the correct address
Invalid Message	Software or Operator	Reenter the correct message
Link 22 Address not on Super Network	Automatically Recoverable	DLP should request an updated directory from the SNC

Figure B.5-3 Tactical Message Errors

If the SNC detects any errors in the control and status messages that the DLP sends to it, the SNC reports the errors in a negative ‘C&S Acknowledgement’ (412h) message, which contains the error. The errors that the SNC can report are listed in [Figure B.5-4](#). Many of the errors may be caused by operator entries or DLP software errors, such as placing an invalid number in a message. If the value was automatically generated by the DLP, then the software is incorrect. If the value was entered by the operator, the operator should reenter the correct value and try again. Some errors are time related. A command should always be generated with sufficient time to distribute it to other units. The operator can change the time to a later time and try again. Errors that can be automatically recoverable depend on each nation’s implementation of their DLP. If the DLP does not automatically recover, the operator should take action to force the indicated recovery.

#	Error	Cause of Error	Possible Solution
1	Unspecified Reason	Unknown	Unknown
2	Insufficient Time to Distribute Frequency Parameters	Software or Operator	Allow at least ten minutes for distribution
3	Insufficient Time to Distribute LLC Integrity Change	Software or Operator	Allow at least ten minutes for distribution
4	Insufficient Time to Distribute Re-initialization Parameters	Software or Operator	Allow at least ten minutes for distribution
5	Invalid Address	Software or Operator	DLP should request a directory update from its SNC or SNMU
6	Invalid All Networks Flag	Software or Operator	
7	Invalid BIT Rate	Software or Operator	
8	Invalid Capacity Need/Capacity Allocated	Software or Operator	
9	Invalid Channel Access Delay	Software or Operator	
10	Invalid Dynamic TDMA Flag	Software or Operator	
11	Invalid Frequency Change	Software or Operator	
12	Invalid Link Quality Code	Software or Operator	
13	Invalid LLC Integrity Flag	Software or Operator	
14	Invalid LLC Number	Software or Operator	
15	Invalid LNE Status	Software or Operator	
16	Invalid LNE Type	Software or Operator	
17	Invalid MASN	Software or Operator	
18	Invalid Media Fragmentation Rate	Software or Operator	
19	Invalid Media Setting Number	Software or Operator	
20	Invalid Media Type	Software or Operator	
21	Invalid Message	Software or Operator	
22	Invalid MPT	Software or Operator	
23	Invalid NCT Data	Software or Operator	
24	Invalid Network ID	Software or Operator	
25	Invalid NU Add/Remove Flag	Software or Operator	
26	Invalid Radio Silence Code	Software or Operator	
27	Invalid Receive Protocol	Software or Operator	
28	Invalid Relay Setting	Software or Operator	

#	Error	Cause of Error	Possible Solution
29	Invalid SPC Radio Power	Software or Operator	
30	Invalid Time Slot Size	Software or Operator	
31	Invalid Time/Day Of Week	Software or Operator	
32	Link 22 Address does not belong to the specified MASN	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
33	Link 22 Address not on the Super Network	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
34	MASN # not currently in use	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
35	MASN # already in use	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
36	Missing Fields	Software	
37	Network Not Operational	Software or Operator	
38	No. of Key Rollovers Out Of Range	Software or Operator	
39	No. of LLC Out Of Range	Software or Operator	
40	No. of Networks Out Of Range	Software or Operator	
41	No. of NUs Out Of Range	Software or Operator	
42	No. of Relayed Message Packets Out Of Range	Software or Operator	
43	No. of Time Slots Out Of Range	Software or Operator	
44	Not Currently Acting as NMU	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
45	Not Currently Acting as SNMU	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
46	Message incompatible with SNC state	Software or Operator	
47	Link 22 Address already belongs to the specified MASN	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
48	Invalid NCS	Manually Recoverable	Operator should enter a new NCS
49	NCS Computation Error	Manually Recoverable	Operator should enter a new NCS
50	Invalid Media Parameters	Software or Operator	
51	Link 22 Address already in SN	Automatically Recoverable	DLP should request a directory update from its SNC
52	No available NILE address	Real world problem	

#	Error	Cause of Error	Possible Solution
53	Invalid Address Version Number	Automatically Recoverable	DLP should request a directory update from its SNC
54	NU Already in Requested State	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
55	Inconsistent Network parameters	Software or Operator	
56	Missing Network Parameters	Software	
57	Incompatible Addressing Mode	Software or Operator	
58	Order Not Addressed To The NMU	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
59	Missing Order Start Time	Software or Operator	
60	Order Start Time Must Be Invalid	Software or Operator	
61	Order End Time Must Be Invalid	Software or Operator	
62	Order Start Time Too Close	Software or Operator	
63	End Time Earlier Than Start Time	Software or Operator	
64	Addressee Not Active	Automatically Recoverable	DLP should request a directory update from its SNC or SNMU
65	Message Not Queued	Cancel Command mismatch: Software or Operator	The command being cancelled did not exactly match the original command
66	Overlapping Message	Software or Operator	Remove a pending command from the queue
67	Inconsistent With Queued Messages	Software or Operator	Remove a pending command from the queue
68	Bad OLM Checksum	The checksum calculated from the DLP OLM data does not match the DLP supplied value	DLP should restart the SNC initialization, ensuring the data sent is correct

Figure B.5-4 SNC Control and Status Errors

B.6 LLC/SPC

LLC/SPC Errors and Alarms represent anomalies in SNC-Media operation as discussed in section [B.2.1 SNC Reported Conditions](#). If the LLC detects a security problem, it reports an Alarm. The generation/detection of any alarm will require an operator to clear the alarm condition. Refer to [Figure B.2-1](#) for steps needed to restart an LLC or SPC. If the alarm condition was a hardware fault then the operator action may require depot-level support.

Within the LLC-7M, the KIV-7M (KIV), the Red-side Interface Adapter (RIA), and the Black-side Interface Adapter (BIA) are capable of generating LLC Alarms. The numerical value and description of the LLC Alarms is listed [Figure B.6-1](#):

- Alarm codes starting with “KIV_...” are alert codes generated by the LLC's KIV-7M (KIV)
- Alarm codes starting with “RIA_...” are error codes generated by the LLC's Red-side Interface Adapter (RIA)
- Alarm codes starting with “BIA_...” are error codes generated by the LLC's Black-side Interface Adapter (BIA)

LLC ALARMS						
Name	Group	Alarm	Port	Value	Description	Action
KIV Group						
KIV_OFFLINE_TEST_FAILURE ¹	0	1	N/A	4	KIV Off-line Self-test Failure	1
KIV_ONLINE_TEST_FAILURE	0	2	N/A	8	KIV On-line Self-test Failure	1
KIV_RIA_HEARTBEAT_LOST ¹	0	3	N/A	12	KIV did not receive a Heartbeat from RIA	1
KIV_BIA_HEARTBEAT_LOST	0	4	N/A	16	KIV did not receive a Heartbeat from BIA	1
KIV_PROCESSOR_FAULT ¹	0	5	N/A	20	KIV reporting internal Processor Fault	1
KIV_HW_FAILURE ¹	0	6	N/A	24	KIV Hardware Failure. This failure includes internal board interface errors and memory read/write failures.	1
KIV_PCE_CHECK_FAULT ¹	0	7	N/A	28	KIV comparison error of the redundant PCE encryption engines during online operations.	1
KIV_PWR_TRANSIENT_DETECT ¹	0	8	N/A	32	KIV Power Transient detected on primary power.	5
KIV_RIA_AUTH_FAILURE ¹	0	9	N/A	36	BIA Off-line Self-test Failure, including failed authentication with the KIV-7M	1
KIV_BIA_AUTH_FAILURE ¹	0	10	N/A	40	BIA Off-line Self-test Failure, including failed authentication with the KIV-7M	1

LLC ALARMS						
Name	Group	Alarm	Port	Value	Description	Action
KIV_TOW_MAXIMUM	0	11	0	44	Port Alarm ²	3
			1	45	The KIV received a Transmit Network Packet where the	
			2	46	Time of Weekday (TOW) is the maximal value	
			3	47	(FFFFFFHex) when the DOW is 7. The TEK is automatically zeroized and the Port disabled.	
RIA Group						
RIA_OFFLINE_TEST_FAILURE ¹	2	1	N/A	132	RIA Off-line Self-test Failure, including failed authentication with the KIV-7M	1
RIA_KIV_HEARTBEAT_LOST	2	2	N/A	136	RIA did not receive a Heartbeat from KIV-7M	1
RIA_TAMPER_DETECT	2	3	N/A	140	RIA Tamper Detected	4
RIA_RED_2_BLK_BANDWIDTH_EXCEEDED	2	4	0	144	Port Alarm ² SNC to SPC Bypass Channel Bandwidth Exceeded; there is an Alarm for each port	2
			1	145		
			2	146		
			3	147		
RIA_SW/FW_DOWNLOAD	2	5	N/A	148	User has initiated a SW/FW Download from the HCI interface and communication to the SNC and SPC is terminated Note: Only allowed in the ACTIVE state.	6
BIA Group						
BIA_BLK_2_RED_BANDWIDTH_EXCEEDED	3	1	0	196	Port Alarm ² SPC to SNC Bypass Channel Bandwidth Exceeded; there is an Alarm Code for each port.	2
			1	197		
			2	198		
			3	199		
BIA_OFFLINE_TEST_FAILURE ¹	3	2	N/A	200	BIA Off-line Self-test Failure, including failed authentication with the KIV-7M	1

Figure B.6-1 LLC Alarms

Note¹: Alarm may not be reported to the SNC - listed here for completeness

Note²: A Port Alarm only disables the offending port; it does not disable the system. All other alarms disable the LLC unit until the alarm is cleared.

Figure B.6-2 lists the actions to be taken by an operator for each of the LLC alarm conditions. The Action column identifies the alarm condition associated with each entry as described in the LLC alarms figure above.

Action	Description
1	System alarm. Reset the system to attempt alarm recovery. If persistent, depot level support is needed. TEK is not zeroized from Black Flash Key Storage.
2	LLC has detected a bypass limit and has automatically disabled the violating Port. Operator to investigate the cause and re-configure the Port, if necessary. TEK is not zeroized from Black Flash Key Storage.
3	LLC has detected a TOD violation and has automatically disabled the violating Port. TEK has been zeroized. Operator to investigate the cause and send either an LLC Key Management Request to prompt a rollover to recover or re-configure the Port, if necessary.
4	LLC unit has been tampered. Return the unit to Depot
5	LLC has detected a power transient event (loss of power) and is performing shutdown operations. Operator to restore power to resume operation. Keys are not zeroized from Black Flash Key Storage.
6	User has initiated a SW/FW Download operations and communication to the SNC is terminated as a result. Wait until download is complete and reset the unit to resume operations.

Figure B.6-2 LLC Alarm Actions

Within the LLC-7M, the KIV-7M (KIV), the System Management Processor (SYS), the Red-side Interface Adapter (RIA), and the Black-side Interface Adapter (BIA) are capable of generating LLC Errors. LLC Errors do not require the SNC to perform error recovery.

Figure B.6-3 provides definitions for the error codes.

- Error codes starting with “KIV_...” are alert codes generated by the LLC's KIV-7M (KIV)
- Error codes starting with “SYS_...” are alert codes and errors generated by the LLC's System Management Processor (SYS)
- Error codes starting with “RIA_...” are error codes generated by the LLC's Red-side Interface Adapter (RIA)
- Error codes starting with “BIA_...” are error codes generated by the LLC's Black-side Interface Adapter (BIA)

LLC ERRORS						
Name	Group	Error	Port	Value	Description	Action
KIV Group						
Not Used				0-3		
KIV_CORRUPTED_RIA_MESSAGE	0	1	N/A	4	Message from RIA has invalid partition checksum or is otherwise not valid.	1
KIV_KEY_INVALID	0	2	0	8	The SNC will get this error when the TEK selected is invalid, has invalid checksum, invalid integrity, or is not available.	2
			1	9		
			2	10		
			3	11		
KIV_INVALID_NETWORK_ID	0	3	N/A	12	Message references a network ID that cannot be mapped to an enabled port.	5
KIV_TSN_ERROR	0	4	0	16	Errors with the Time Slot Number (TSN), including Transmit NP Request TOW is less than the corresponding TSN for the Network ID or if the DOW does not match.	6
			1	17		
			2	18		
			3	19		
KIV_MESSAGE_ERROR	0	5	0	20	Catch All/Miscellaneous Error Condition for command or traffic packet processing. If the KIV finds that the message is in error and it's not for reasons called out elsewhere, this error code is used.	7
			1	21		
			2	22		
			3	23		
KIV_NO_NEXT_KEY	0	6	0	24	This error is for the rollover scenario where the next key is not available or invalid.	8
			1	25		
			2	26		
			3	27		
KIV_CORRUPTED_BIA_MESSAGE	0	7	0	28	Message from BIA has invalid partition checksum or is otherwise not valid.	10
			1	29		
			2	30		
			3	31		
KIV_RX_SEQID_ERROR	0	8	0	32	Sequence ID of a Receive NP Request does not match a previous Receive Header Request and therefore the receive NP cannot be decrypted.	17
			1	33		
			2	34		
			3	35		
KIV_PORT_DISABLED	0	9	0	36	Message references a Port (via the network ID) that is not enabled, meaning that there is not a valid key.	5
			1	37		
			2	38		
			3	39		
Reserved for KIV errors				40-63		

LLC ERRORS						
Name	Group	Error	Port	Value	Description	Action
System Group						
Not Used			64-67			
SYS_LOW_BATTERY_VOLTAGE_ALERT	1	1	N/A	68	This is reported as soon as any of the three batteries fall below threshold.	14
SYS_ROLLOVER_ALERT	1	2	N/A	72	This is a status alert of when a rollover has occurred. Upon receipt of a key management request that increments the DOW from 7 to 1, we send this alert and perform a weekly rollover	15
SYS_NO_VALID_KEYS_ALERT	1	3	N/A	76	Status alert from the KIV during a configuration request, indicating that there are no keys in the system.	16
SYS_AUTO_CONFIG_ALERT	1	4	N/A	80	Status alert from the KIV upon detecting a key fill to key slot currently selected by a port (configured without a key). The LLC will initiate an internal configuration to load the key for use.	18
Reserved for System errors				81-127		

LLC ERRORS						
Name	Group	Error	Port	Value	Description	Action
RIA Group						
Not Used				128-131		
RIA_MISC_ERROR	2	1	N/A	132	This error code will be used as the catch all, miscellaneous error if an uncategorized error is found in the RIA SW/FW	7
RIA_UNDEFINED_MSG	2	2	N/A	136	Message from SNC has an invalid ID	11
RIA_DATA_LEN_EXCEEDS_LIMIT	2	3	N/A	140	Message from SNC has improper length	11
RIA_BAD_MSG_COMPOSITION	2	4	N/A	144	Message from SNC is improperly formatted. This applies to errors with the construction of the whole message, including invalid combo of crypto, bypass, and data partitions or bad socket header.	11
RIA_BAD_CRYPTO_PARTITION	2	5	N/A	148	Error found in evaluating the Crypto Partition of the message	11
RIA_BAD_BYPASS_PARTITION	2	6	N/A	152	Error found in evaluating the Bypass Partition of the message	11
RIA_BAD_DATA_PARTITION	2	7	N/A	156	Error found in evaluating the Data Partition of the message	11
RIA_CORRUPTED_KIV_MESSAGE	2	8	N/A	160	Message from KIV-7M has invalid checksum or is otherwise not valid.	1
RIA_INVALID_NETWORK_ID	2	9	N/A	164	Message from SNC references a network ID that cannot be mapped to an enabled port	5
RIA_NP_INTEGRITY_FAILED	2	10	0	168	Integrity Verification of Network Packet (when integrity is enabled) failed. Non-fatal, data partition is set to empty and sent to SNC, NNC continues processing.	4
			1	169		
			2	170		
			3	171		
RIA_PORT_DISABLED	2	11	0	172	Message references a Port (via the network ID) that is not enabled, meaning that there is not a valid key.	5
			1	173		
			2	174		
			3	175		
RIA_INTERNAL_BYPASS_VIOLATION	2	12	0	176	Internal Bypass Channel Bandwidth Exceeded; Non-fatal, the event is reported and operation continues without interruption or reconfiguration.	9
RIA_FIFO_OVERFLOW	2	13	0	180	RIA FPGA reports an overflow in the FIFO feeding the PCE and interrupts SW. This is reported by RIA SW.	19
Reserved for RIA errors				181-191		

LLC ERRORS						
Name	Group	Error	Port	Value	Description	Action
BIA Group						
Not Used				192-195		
BIA_MISC_ERROR	3	1	N/A	196	This error code will be used as the catch all, miscellaneous error if an uncategorized error is found in the BIA SW/FW	7
BIA_UNDEFINED_MSG	3	2	0	200	Message from SPC has an invalid ID	12
			1	201		
			2	202		
			3	203		
BIA_BAD_MSG_COMPOSITION	3	3	0	204	Message from SPC is improperly formatted. This applies to errors with the construction of the whole message, including invalid combo of crypto, bypass, and data partitions or bad socket header.	12
			1	205		
			2	206		
			3	207		
BIA_BAD_CRYPTO_PARTITION	3	4	0	208	Error found in evaluating the Crypto Partition of the message (i.e. should always be null)	12
			1	209		
			2	210		
			3	211		
BIA_BAD_BYPASS_PARTITION	3	5	0	212	Error found in evaluating the Bypass Partition of the message	12
			1	213		
			2	214		
			3	215		
BIA_BAD_DATA_PARTITION	3	6	0	216	Error found in evaluating the Data Partition of the message	12
			1	217		
			2	218		
			3	219		
BIA_DATA_LEN_EXCEEDS_LIMIT	3	7	0	220	Message from SPC has improper length	12
			1	221		
			2	222		
			3	223		
BIA_PORT_DISABLED	3	8	0	224	Error occurred when configuring or transmitting data through the referenced SPC port.	13
			1	225		
			2	226		
			3	227		
BIA_CORRUPTED_KIV_MESSAGE	3	9	0	228	Message from KIV-7M has invalid checksum or is otherwise not valid.	10
			1	229		
			2	230		
			3	231		
BIA_FIFO_OVERFLOW	3	10	0	232	BIA FPGA reports an overflow in the FIFO feeding the SPC and interrupts SW. This is reported by BIA SW.	19
			1	233		
			2	234		
			3	235		
Reserved for BIA errors				236-255		

Figure B.6-3 LLC Errors

Figure B.6-4 lists the actions to be taken by an operator for each of the LLC error conditions. The Action column identifies the error condition associated with each entry as described in the LLC Errors figure above.

Action	Description
1	Communication error between the RIA and KIV-7M, continue to observe for further occurrence. A system reset may be required.
2	Invalid key selection or key is corrupted. Operator to validate that the correct key slot is specified and there is a valid key.
3	Not used.
4	The packet failed to pass integrity checking.
5	Received message referenced a Port that is not configured. Operator should check the Network ID of the message and the current Port configuration status.
6	The TSN (DOW or TOW) is incorrect. Operator to validate the message parameters.
7	Internal error, continue to observe for further occurrence. A system reset may be required.
8	LLC attempted to perform a rollover but the next key is not available or is invalid. Operator to check the status of keys.
9	LLC has detected that transfer of internal messages have exceeded the rate limit threshold for normal operation. This may be caused by unusual activity within the LLC. Inspect the LLC for functional or physical changes. If this error is reported regularly, the unit may need to be serviced by reloading software and firmware.
10	Communication error between the BIA and KIV-7M, continue to observe for further occurrence. A system reset may be required.
11	RIA has detected an invalid message. Operator to verify the contents of the SNC message for correct composition, checksums, ID, and length.
12	BIA has detected an invalid message. Operator to verify the contents of the SPC message for correct composition, checksums, ID, and length.
13	SPC interface error. Operator to verify the asynchronous serial port parameters and make sure that the referenced SPC port is configured.
14	One of the three LLC batteries is below threshold. Operator to replace all three batteries with primary power applied.
15	Alert that a weekly rollover has occurred. No operator intervention is needed.
16	There are no keys in the system. Operator to load keys as needed.
17	The Sequence ID of a Receive NP from the SPC has invalid Sequence ID. Operator to validate the Receive Header Request that was used to set up the receive transaction.
18	Send an LLC Status Request to confirm that the newly loaded key is available in the port. Once confirmed this port is enabled for traffic operations.
19	The FPGA FIFOs are overflowed on the Red or Black IA, meaning that the LLC has reached maximum throughput or that there is a delay in the system. Verify traffic is still operational before proceeding.

Figure B.6-4 LLC Error Actions

Any fault condition that prevents the SPC from operating properly is regarded as an alarm event. The SPC Alarms are sent to the DLP by the SNC in a ‘SPC Alarm/Error Report’ (80Fh) message. The contents of the message may be displayed to the operator, and are listed in [Figure B.6-5](#).

Alarm	Description
Alarm Unknown	An undefined Alarm was detected by the SPC
SPC exits/has exited the TDMA mode	The SPC has stopped transmitting
SPC failure	An error was detected by the SPC which caused it to Fail
Radio failure	The Radio has failed

Figure B.6-5 SPC Alarms

SPC Errors are handled by the SNC and are also passed to the operator in a ‘SPC Alarm/Error Report’ (80Fh) message. The contents of the message may be displayed to the operator, and are listed in [Figure B.6-6](#).

Error	Result
SPC->SNC ‘SPC Status Response’ (00F1h) message indicating SPC Disabled	SNC->DLP ‘SPC Disabled’ (803h)
SPC->SNC ‘SPC Configuration Response’ (00E1h) indicating configuration NOT CONFIRMED	SNC requests SPC status, and then reports the failed parameters to DLP in ‘SPC Configuration Failure’ (801h)
Unsolicited ‘SPC Alarm Message’ (00BBh)	SNC->DLP ‘SPC Alarm/Error Report’ (80Fh)
No response from SPC and/or LLC	SNC->DLP ‘SPC Disabled’ (803h)

Figure B.6-6 SPC Initialization Errors

B.7 Key Rollover

The unit will successfully transmit and receive only when the LLC Day Of Week (DOW) and the LLC crypto key are the same as for all other units. If the LLC is using the wrong DOW or wrong key, the operator can request that a LLC Key Rollover be performed. During operations, a LLC Key Rollover causes the LLC's DOW to increase by one. If the DOW was at 7 before the rollover, the DOW will be reset to 1 and the LLC will rollover the key to the next week's key. After the rollover process is completed, the status of the rollover process can be made available to the operator, so that the operator will know if there was a failure to perform the roll over, as shown in [Figure B.7-1](#). The key rollover of a single non-operational LLC is described in section [3A.6.5 Crypto Time-of-Day \(TOD\)](#).

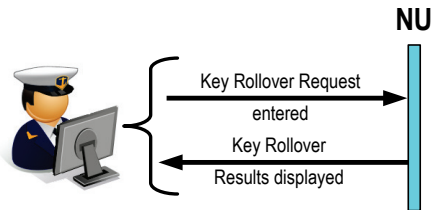


Figure B.7-1 Key Rollover

The Key Rollover Order is defined, but is not currently part of Link 22 procedures.

B.8 TOD

Time Of Day (TOD) is input to the TDS/DLP, the SNC and to each SPC. Frequency hopping radios may also require TOD input. The TOD is used to control the timing of transmissions and receptions.

The time is not needed by the LLC, even though a time-based sequence is used as part of encryption, because the LLC encrypts for a specified future timeslot and it decrypts data received in a previous timeslot.

The timing of the SNC is not critical; the SNC needs only to ensure that time does not drift, because it prepares data for future timeslots which it sends to the LLC for encryption, and receives decrypted data from the LLC from previous timeslots.

Time for the SPCs is more critical because the SPC has to control the radio in order to transmit and receive at the correct times.

The SNC and each SPC monitor the TOD supply, and report if it is lost, or re-established. Each SPC reports its TOD supply status in the TOD I/F bit of the TOD Quality field in the 'SPC Status Response' (00F1h) message. The DLP is informed of SNC and SPC TOD supply changes as discussed in section [B.2.1 SNC Reported Conditions](#).

The SNC and each SPC monitor the TOD quality. The SNC uses Time Figure Of Merit (TFOM) provided by the external time reference system, which represents the inaccuracy of the TOD from UTC. Each SPC may or may not use TFOM. The SNC does not check TOD quality if the TOD input is lost. Each SPC continues to calculate TOD quality even if TOD input is lost. If the TOD quality degrades, the unit may be unable to transmit or receive successfully. Each SPC reports its ability to transmit and receive in the Tx Status bit and Rx Status bit of the TOD Quality field in the 'SPC Status Response' (00F1h) message. The DLP is informed of SNC and SPC TOD quality failure changes as discussed in section [B.2.1 SNC Reported Conditions](#).

If the TOD supply fails, the SNC and SPC will continue using their internal clocks, which may slowly drift away from UTC time (depending on the clock accuracy). Transmissions may cease if the TOD quality degrades beyond the levels shown in [Figure B.8-1](#), whether or not there is a TOD supply.

TOD Quality	SNC/SPC Transmissions
< 1 millisecond	Transmissions continue
1-10 milliseconds	UHF transmissions stop
> 10 milliseconds	UHF and HF transmissions stop

Figure B.8-1 Transmissions during Degraded TOD Quality

The SPC may have the same TOD feed as the SNC, or it may have its own TOD feed. If the TOD feeds are separate, and only the SNC time quality degrades, the SPC will continue to transmit until the SNC ceases to request transmissions.

Since the SNC checks TOD quality only when it has a TOD supply, the SNC will continue to request transmissions when it loses its TOD supply unless the SPC reports that it can no longer transmit.

The operator should have the TOD input checked if a TOD failure or a TOD quality failure is reported. The operator may decide to stop transmissions (for example by going to Radio Silence) until a good TOD supply is re-established. However, it may be tactically disadvantageous to stop transmitting just because the TOD feed has a problem since each SPC will automatically stop transmitting if its TOD quality becomes too degraded.

B.9 System Level Problems

System level problems that may involve more than one unit include the following cases.

- [Change of Network Media Type](#)
- [Reception Problems](#)

B.9.1 Change of Network Media Type

When changing the media type, the operator should be aware of the capabilities of each unit to ensure that each unit is capable of using the new media type which requires an SPC, radio and antenna for the new media. Some SPCs may be able to automatically change media type, but others may require a manual change, or may be capable of only a single type of media.

Special considerations should be taken when changing the media type for a network from a media type with smaller minislot duration, such as UHF FF, to a media type with larger minislot duration, such as HF FF. For all units that will use the same SPC port for the new media type, this type of a change requires a reset of the LLC DOW and a reload of the crypto keys, which will affect all other networks using the same LLC.

The LLC uses a Time Slot

Number (TSN) to encrypt data on a network. The LLC keeps track of a different TSN for each network. The TSN includes the Day Of Week (DOW), and the Time Of Weekday (TOW). The TOW is represented by the number of Media Coding Frames (MCF) since midnight. The size of a Media Coding Frame is dependent on the media type, as shown in [Figure B.9-1](#) for UHF FF and HF FF.

The LLC will not encrypt data on a network if the specified TSN is not greater than the TSN of the previously encrypted data on the same network. The LLC will report KIV_TSN_LOAD Error in this case.

Media Type	MCF Duration (milliseconds)	12:00:00 p.m. in seconds	12:00:00 p.m. in MCF	12:01:00 p.m. in seconds	12:01:00 p.m. in MCF
UHF FF	48 ms	43200	900000	43260	901250
HF FF	112.5 ms	43200	384000	43260	384533

Figure B.9-1 Media Coding Frame Example

If a UHF FF network's last transmission was at 12:00:00 pm, the last transmission's TOW will be 900000 for the network. If the network is then changed to HF FF, and the next transmission is at 12:01:00 pm, the TOW for the transmission will be 384533. The LLC will reject this transmission because the TOW is smaller than the previous transmission's TOW.

The only way to alleviate this situation is to reset the LLC's internally-stored TSN for the network, if using the same SPC port. This can be done only by resetting DOW to 0 for the LLC, which affects all networks on the LLC.

B.9.2 Reception Problems

Problems in reception experienced by multiple units at the same time could be caused by any of the following.

- A unit is transmitting at the wrong time, possibly due to an incorrect NCS
- A transmitting unit is using the wrong crypto key
- A transmitting unit is using the wrong LLC Integrity setting
- Jamming / Spoofing

An incorrectly transmitting unit should stop transmitting and correct the problem.

B.10 Frequently Asked Questions

1. *Question:* Is a platform equipped with a SNC v8.0 interoperable with another platform equipped with an older version?

Answer: The SNC Version number, for example. 9.0, includes the Major Version (9), followed by the Minor Version (0), separated by a period “.”. Interoperability is provided between SNCs running with the same Major Version number, starting with SNC version 9.0. SNCs earlier than 9.0 are not guaranteed to be compatible with any other version. Example: Platform A equipped with SNC v9.3 will be interoperable with platform B equipped with SNC v9.0 and vice-versa. However, platform C with SNC v10.0 will not be fully interoperable with platform A or B.

2. *Question:* Why does the “Time Of Day” sometimes range from 0 to 86400 included (86401 different values), whereas a day is only composed of 86400 seconds?

Answer: The last value (86400) is used when there is an extra second in a day (called a positive leap second). By using the extended range the equipment can handle this “leap” second.

3. *Question:* How is the CRC-16 (DFI:712-DUI:001) field computed in the F01.7-0 message?

Answer: Unfortunately, this is currently undefined but remains important for interoperability. The definition should take into account any established implementations of the NILE nations. It is suggested that the version implemented by the MLST3 test tool be adopted as the standard.

4. *Question:* How are the Coarse and Fine Latitude (DFI:281-DUI:016 and DFI:281-DUI:018) and Longitude (DFI:282-DUI:012 and DFI:282-DUI:16) Data Fields computed?

Answer: The coarse value is the complete value, whereas the fine value is only the least significant part of the value. When a coarse value is received, the most significant part needs to be stored, so that when a fine value is received the complete value can be computed.

5. *Question:* How is a Link 22 timeslot different from a Link 16 timeslot?

- Is there an NTR in Link 22?
- Are Round-trip Timing transmissions required on Link 22?

- Do you have to load an initialization file containing timeslots into a terminal before operations?
- How is Dynamic Network Management performed in Link 22?

Answers:

- No
- No
- No initialization file is required for Link 22 operations. Only the OLM is required
- Dynamic changes to the TDMA structure are performed automatically by the SNCs. Other Network Management functions, such as adding a unit, or re-configuring a network, are initiated by the DLP, and then automatically performed by the SNCs

6. *Question:* How does Link 22 do NPGs, such as Air Control, EW, and F2F?

Answer: Link 22 does not segregate traffic into NPGs. It uses addressing mechanisms to reach all intended destinations.

7. *Question:* Which TDLs can data on Link 22 get forwarded to, and from?

Answer: STANAG 5616 defines data forwarding between Link 22 and Link 16 and Link 22 and Link 11/11B.

8. *Question:* Which equipment specific to Link 22 must a platform have to operate on Link 22?

Answer: The SNC, LLCs, and SPCs are all specific to Link 22. The DLP may handle multiple data links, and the radios are not specific to Link 22.

9. *Question:* Which equipment specific to Link 22 must a platform have to operate as a data forwarder on Link 22?

Answer: A unit acting as a data forwarder on Link 22 must have all of the Link 22 equipment, and equipment required by the data link(s) it is forwarding to/from.

10. *Question:* Does Link 22 have frequency hopping?

Answer: Link 22 frequency hopping is provided by the HF EPM and UHF EPM media types.

11. *Question:* What kind of inherent security does Link 22 have? E.g., Link 11 has MSEC via KG-40A, Link 16 has MSEC and TSEC via the Link 16 terminal.

Answer: The Link 22 crypto is part of the same family of Link 16 with an added layer of security to detect spoofing. TRANSEC is also provided by the HF EPM and UHF EPM media types. Modernization of the crypto for the future has been started.

12. *Question:* On which frequency band does Link 22 operate?

Answer: Each network can use either High Frequency (HF) in the 2-30 MHz band, or Ultra High Frequency (UHF) in the 225-400 MHz band.

13. *Question:* Does Link 22 have relay units?

- If so, what is the maximum possible number of relay hops for P2P communication to occur on Link 22?
- Must relay units have more timeslots than non-relay units?
- Does Link 22 support the role of Initial Entry JTIDS Unit (IEJU)?
- How do relay units affect the bandwidth of Link 22 communications?

Answer: All Link 22 units can perform automatic relay functions.

- There is no technical limit to the number of relay hops
- No. However, it is recommended that units expected to perform a lot of relay be assigned extra timeslots
- No requirement exists, as an external Time reference is used. Link 22 also allows for Late Network Entry
- The bandwidth is affected when relay traffic is present and depends on the connectivity. However, since no dedicated relay slots are required, bandwidth can always be used for other tactical traffic. Priority schemes also improve the ability to deliver high priority traffic

14. *Question:* Does Link 22 support the roles of Position Reference, Navigation Controller, and Secondary Navigation Controller?

Answer: These functions are not required in Link 22, simplifying operations.

15. *Question:* Does Link 22 support passive synchronization and Secondary Users?

Answer: These functions are not required in Link 22, simplifying operations.

16. *Question:* How many types of radio silence are possible on Link 22? (E.g., Link 16 has two: LTTI and Data Silent.)

Answer: A unit can be radio silent on a single network, multiple networks, or all of its networks. An entire network or multiple networks can be placed in radio silence. The entire Super Network can be placed in radio silence. A transmission can be made during radio silence by temporarily overriding the radio silence for that single transmission.

17. *Question:* Do Link 22 networks operate in accordance with a network design?

- Must networks be designed for Link 22?
- If so, are there network design files?
- If there are, which agency/agencies provide these?

Answer: Link 22 does not require a Network Design facility, which simplifies the process. The OLM is the only required input to Link 22. A Link 22 network definition in the OLM contains the units in the network, and either the timeslots allocated to each unit, or the transmission requirements of each unit (capacity need and access delay), which are then used by the SNC to automatically build an NCS.

18. *Question:* LNE process did not complete as expected. What are the possible causes?

Answer: Successful LNE requires the correct media type, frequency, network ID, crypto key, DOW, and accurate TOD. The Media Setting Number (from among a list of supplied choices) and LLC Integrity setting can be determined by the SNC. If LNE fails, it can be restarted with different values.

There are many reasons why LNE can fail, as listed below.

- Wrong media type
- Wrong frequency
- Wrong Media Setting Number
- Wrong LLC Integrity setting
- Wrong crypto key loaded
- Inaccurate TOW or wrong DOW
- Wrong network ID (which will cause decryption to fail)
- No connectivity to any supporting unit

Appendix C

Minimum Implementation

This appendix provides the minimum implementation for a DLP in terms of the DLP to SNC Interface messages, and the minimum tactical data exchange requirements for Link 22, as defined in [STANAG 5522]. The following topics are addressed.

- DLP-SNC Minimum Implementation
- Minimum Tactical Data Exchange

C.1 DLP-SNC Minimum Implementation

C.1.1 Introduction

This section provides the minimum implementation for a DLP in terms of the messages on the DLP to SNC Interface that must be supported. Within the NILE Super Network there are specific Roles that certain NUs will perform. These special roles are the Super Network Management Unit (SNMU), the Network Management Unit (NMU) (one for each NILE Network) and a standby unit for each primary role. The Standby Units have no special function other than they must be capable of performing the primary role which they will take over if the primary is lost. For a minimum implementation a DLP does not have to perform any of these special roles, and so those messages that are only associated with the special role are not required. The only caveat being that these roles must be available within the Super Network, and therefore some units must be able to perform them.

The DLP to SNC interface consists of the two functional interfaces as defined in Chapter 3. These are the Tactical Interface and the Control and Status Interface. These two functional interfaces are discussed in the following sections.

- [Tactical Interface](#)
- [Control and Status Interface](#)

C.1.2 Tactical Interface

The Tactical Interface is used to exchange and to control the exchange of Tactical Messages (as defined in [\[STANAG 5522\]](#)), which consists of 1 to 8 Tactical Data Words (TDW) each of which is 72 bits long. The Tactical Messages that are sent across this interface are treated as sealed envelopes. The Tactical Messages are encapsulated within messages exchanged over the Tactical Interface, which are called Tactical Interface messages. Most of the Tactical Interface messages do not contain Tactical Messages and are for the control of the various protocols. Tactical Messages for transmission are contained either in ‘Preparation Request Response’ (105h) or in ‘Transmission Service Request (TSR) with Data’ (102h) Tactical Interface messages. Tactical Messages that have been received are contained within ‘Received Tactical Messages’ (207h) Tactical Interface messages.

The rules for tactical transmission are contained in [\[STANAG 5522\]](#) and are not part of this document or this Appendix. A minimum implementation of a DLP assumes that the DLP is performing in a normal role (transmitting and receiving, not receive only), and so is an active member of the Super Network. Such a DLP must be able to handle all the tactical interface messages on this functional interface, with the exception of the two flow control messages ‘Ready to Receive’ (107h) and ‘Tactical Messages Available’ (206h) which it would not use, selecting the optimized protocol by setting the ‘Optimized Receive Protocol’ flag in the ‘MPT Specification’ (301h) message during initialization. This is shown in [Figure C.1-1](#) which lists the 100 series messages that the DLP generates and sends to the SNC and also lists the 200 series messages which the DLP receives from the SNC. The messages that a minimum implementation DLP must be able to handle are indicated by an “M” in the ‘Min. Imp.’ column.

Some DLPs may have special DLP level functionality such as being a Forwarding NU (FNU) which could forward tactical messages to and from Link 22 and some other network. This functionality is described in [\[STANAG 5616 Volume II\]](#) and [\[STANAG 5616 Volume III\]](#), but would not be part of the minimum implementation.

Message Title	Msg ID	Protocol	Min. Imp.	Note
Transmission Service Request	101h	TACT	M	
Transmission Service Request with Data	102h	TACT	M	
Cancel Service Request	103h	TACT	M	
DLP Cannot Comply	104h	TACT	M	
Preparation Request Response	105h	TACT	M	
Priority Change Request	106h	TACT	M	
Ready to Receive	107h	FLOW		Flow Control for received tactical messages
Message Preparation Request	201h	TACT	M	
Transmission Completed	202h	TACT	M	
SNC Cannot Comply	203h	TACT	M	
Confirm Cancellation	204h	TACT	M	
Acknowledgement	205h	TACT	M	
Tactical Messages Available	206h	FLOW		Flow Control for received tactical messages
Received Tactical Messages	207h	TACT	M	

Figure C.1-1 Tactical Interface Message Minimum Implementation

C.1.3 Control and Status Interface

The Control and Status Interface is used by the DLP for the management of the SNC, which is accomplished by the sending of control messages and the receipt of status messages.

A large number of the messages are required for initialization which requires that the DLP be supplied with the information in the OPTASK Link message so that it can provide the SNC with this information, or it needs to provide the facility for other higher level functions to provide the messages that the DLP needs to send to the SNC.

A minimum implementation of a Link 22 system could use reduced functionality, such as not using probing or never turning DTDMA on. This would mean that the minimum implementation DLP would not need to handle the messages associated with these protocols. This reduced functionality would require that all the missing functionality not be specified in the formation of the OPTASK Link message and would never be initiated during the running of the link. For interoperability, all nations that would be in the Super Network would have to agree on the limitations. However, the DLP minimum implementation presented in the figures assumes that the full functionality of the Link 22 system could be used, not a limited functionality. The messages that a minimum implementation DLP must be able to handle are indicated by an “M” in the ‘Min. Imp.’ column in the figures.

Figure C.1-2 lists all the DLP-to-SNC Interface messages that are generated by the DLP and sent to the SNC and indicates those which have to be generated by a minimum implementation DLP. Figure C.1-4 provides notes applicable to a DLP-SNC minimum implementation.

Message Title	Msg ID	Protocol	Min. Imp.	Minimum Implementation Note
MPT Specification	301h	CIS	M	SNC Initialization
LLC LAN Configuration Request	302h	CIS	M	SNC Initialization
LLC Port Configuration Request	303h	CIS	M	SNC Initialization
Link 22 Super Network Participants	304h	DIR	M	SNC Initialization
Super Network Special Duties	305h	DIR	M	SNC Initialization
Network Parameters (SNC NCS)	306h	CIS	M	Network Initialization
Network Parameters (Probing)	307h	IPROB	M	Network Initialization (see Note 1)
Radio Silence	308h	DIR	M	(see Note 2)
Operational NCS Request	30Bh	IPROB		Only NMU at end of probing
NCS Acknowledgement	30Ch	CIS		Only NMU
DLP NCS Description	30Dh	IPROB		Only NMU at end of probing
Network Parameters (DLP NCS)	30Eh	CIS	M	Network Initialization
Change Media Parameters	30Fh	REINIT		NMU Only
Network Reconfiguration Request (DLP NCS)	310h	RECONF		NMU Only
DLP DTDMA Change	311h	DTDMA		NMU Only
DLP Request Management Info	312h	CIS		
Create MASN	313h	DIR	M	SNC initialization, SNMU Only
Modify MASN	314h	DIR		SNMU Only
Delete MASN	315h	DIR		SNMU Only
DLP LNE Request	316h	LNE	M	
DLP LNE Response	317h	LNE		SNMU Only
Transmission Capacity Response	318h	LNE		NMU Only
Stop Communication	319h	CIS	M	
NU Leave	31Ah	CIS	M	
Role Change	31Bh	DIR	M	
Change Relay Settings	31Ch	DIR	M	SNC Initialization, SNMU Only
Relay Flow Response	31Dh	FLOW		
NILE Address Allocation Request	31Fh	DIR		SNMU Only
Key-Rollover Request	320h	CIS		
Key-Zeroization Request	321h	CIS		(see Note 2)

Message Title	Msg ID	Protocol	Min. Imp.	Minimum Implementation Note
LLC Status Request	322h	CIS		
LLC Error Report Request	323h	CIS		
LLC Alarm Report Request	324h	CIS		
Continue Processing	325h	CIS		Only sent after connection failure or DLP loss and SNC not rebooted.
Clear Requests	326h	CIS		As above
Network Late Initialization Request	327h	LNE	M	
Link Quality Status	328h	CONN		SNMU Only
Network Reconfiguration Request (SNC NCS)	329h	RECONF		NMU only
Insert LNE Slot	32Ah	LNE		NMU only
Remove LNE Slot	32Bh	LNE		NMU only
SNC Initialization Complete	32Ch	CIS	M	SNC Initialization
SPC Radio Power Request	32Dh	CIS		
Notify SN Directory	32Eh	DIR		SNMU Only
NU Status	32Fh	DIR	M	SNC Initialization, SNMU Only
SN Directory Update	330h	DIR		Recommended
Role Takeover Control	331h	NMC		Only for role NUs
NU Performance Data	332h	NMC		
Order	333h	NMC		Only SNMU and NMUs
Order Compliance	334h	NMC	M	(see Note 3)
Function Management Setup	335h	NMC	M	
DLP OLM Checksum	336h	CIS		SNC Initialization

Figure C.1-2 Control and Status Interface Message Minimum Implementation (DLP to SNC)

Figure C.1-3 lists all the DLP to SNC Interface messages that can be received by the DLP from the SNC and indicates which ones could be received by a minimum implementation DLP, and therefore have to be handled, even if just to discard them.

Message Title	Msg ID	Protocol	Min. Imp.	Note
Probing Results	401h	IPROB	M	Probing (see Note 1)
End of Probing	402h	IPROB	M	Probing (see Note 1)
Received Network Parameters(Probing)	403h	IPROB	M	Probing (see Note 1)
SNC NCS Description	404h	CIS	M	Multiple uses
Media Parameters	405h	REINIT	M	Network Initialization
Link Participants	407h	DIR	M	
SNC LNE Request	408h	LNE		SNMU Only
LNE Status	409h	LNE	M	
LNE Failure	40Ah	LNE	M	
Transmission Capacity Request	40Bh	LNE		NMU Only
Communication Terminated	40Ch	CIS	M	
Role Status	40Dh	DIR	M	
SNC DTDMA Change	40Eh	DTDMA	M	
NILE Address Allocated	40Fh	DIR	M	
NILE Address Availability	410h	CIS		SNMU Only
Acknowledgement Response	411h	CIS		SNMU/NMU only
Permanent Reallocation	412h	NCSC	M	
SNC Status	413h	CIS	M	
NU Status Changed	414h	DIR	M	
SNC Network Reconfiguration	415h	RECONF	M	
Received Network Parameters (DLP NCS)	416h	CIS	M	
SPC Radio Power Response	417h	CIS		
Relay Setting Change	418h	DIR	M	
Relay Flow Control	419h	FLOW		
Key-Rollover Response	41Ch	CIS	M	
Key-Zeroization Response	41Dh	CIS		(see Note 2)
LLC Status Response	41Eh	CIS	M	

Message Title	Msg ID	Protocol	Min. Imp.	Note
LLC Alarm Report Response	41Fh	CIS		
LLC Error Report Response	420h	CIS		
SNC C&S Acknowledgement	421h	CIS	M	
Network Initialization Complete	422h	CIS	M	
MASN Creation	423h	DIR	M	
MASN Modification	424h	DIR	M	
MASN Deletion	425h	DIR	M	
Radio Power Management Request	426h	CIS	M	
NU Performance Data	427h	NMC	M	
Received Order	428h	NMC	M	
Received Order Compliance	429h	NMC		SNMU/NMU only
Received Network Parameters (SNC NCS)	42Ah	NMC	M	
Received Notification	42Bh	NMC	M	
TOD Status	42Ch	TOD	M	
Network Information	42Dh	STAT		Only if 312h implemented
Network Congestion Indexes	42Eh	STAT		Only if 312h implemented
NU Capabilities	42Fh	NMC	M	
Channel Utilization	601h	STAT	M	Auto, each TS
Connectivity Information (LRQ)	602h	STAT		Only if 312h implemented
Congestion Alert	603h	STAT	M	Auto, each NCT
Error Rate Characteristics	604h	STAT	M	Auto, each NCT
DTDMA Participation	605h	STAT	M	Auto, each 10 NCTs
NU Data	606h	NMC	M	Every 60 seconds
Connectivity Information (LCD)	607h	STAT		Only if 312h implemented
SPC Configuration Failure	801h	ALERT	M	
Built in Test	802h	ALERT		(see Note 5)
SPC Disabled	803h	ALERT	M	
Timeslot Violation	804h	ALERT	M	

Message Title	Msg ID	Protocol	Min. Imp.	Note
LLC Alarm/Error Report	806h	ALERT		
LLC Disabled	807h	ALERT	M	
Media Interface Congestion	80Ah	ALERT	M	
LLC Configuration Failure	80Bh	ALERT	M	
SNC NP Rejection Error	80Eh	ALERT		
SPC Alarm/Error Report	80Fh	ALERT		

Figure C.1-3 Control and Status Interface Message Minimum Implementation (SNC to DLP)

Note #	Notes
1	Most current radios do not support or are not configured to support automatic control, which is needed by the Link 22 system for the SNC to be able to perform "Probing", and so it is unlikely that in the early stages of deployment that Link 22 will be able to use "Probing". A minimal implementation to be interoperable with Link 22 needs to be able to support "Probing" and therefore this message is mandatory, however for early implementations of Link 22 that do not implement "Probing" this message is not mandatory until the "Probing" in Link 22 starts to be implemented.
2	To be interoperable the Key Zeroization Request is not mandatory, however for security reasons it is unlikely that a minimum implementation would not include this message, and therefore also its response message.
3	Most order compliance messages could be configured so that the SNC automatically produces them, however there are a few that are not allowed to be configured in this way and so the DLP would need to send this message and so it is mandatory.
4	If a NU never wants to initiate Radio Silence itself, then the 'Radio Silence' (308h) message may not be mandatory as long as the Function Management Switch is set so that the SNC automatically performs the operation when ordered.
5	The 'Built in Test' (802h) message is not mandatory as long as the DLP sets the BIT Repetition Rate field to zero in the 'MPT Specification' (301h) message.

Figure C.1-4 Note on Control and Status Interface Message Minimum Implementation

Figure C.1-5 provides an expansion of the protocol column abbreviations.

Protocol	Description
ALERT	Alert/Alarms
CIS	Configuration/Initialization/Status/etc.
CONN	Connectivity Forcing/Easing
DIR	Directory Maintenance
DTDMA	DTDMA Activation/De-activation
FLOW	Flow Control/Metering
IPROB	Initialization with Probing
LNE	Late Net Entry / Late Traffic Entry
NCSC	NCS changes due to DTDMA & LNE NCS
NMC	Network Management Control
RECONF	Re-Configuration
REINIT	Re-Initialization
STAT	Statistics
TACT	Tactical Interface
TOD	Time of Day Status

Figure C.1-5 Protocol Abbreviations

C.2 Minimum Tactical Data Exchange

C.2.1 Introduction

This section identifies the minimum data exchange requirements, which must be implemented by National systems participating on the Link 22 Interface. The fulfillment of these data exchange requirements is mandatory to establish and maintain the Link 22 Interface, to participate within a specific functional area, and to prevent adverse effects on the interface. Although a system may implement more than the specified requirements (for example National system implementation requirements), this section describes only the mandatory minimum required for systems participating in specific functional areas. A system's implementation documentation must be referenced to determine further Minimum Implementation requirements. The minimum transmit and receive implementation specified in [STANAG 5522] Annex B Appendix 1, is that required to ensure a minimum level of interoperability at the operator level.

The MIN IMP requirements of Annex B of [STANAG 5522] apply to all interfacing systems participating on the Link 22 Interface. The applicability of these requirements is directed towards digital data exchange in a multinational environment where systems of two or more nations are involved. The implementation of these minimum requirements for data exchange is contingent upon the conventions, constraints, protocols and rules specified in Annex B of [STANAG 5522].

MIN IMP is defined in terms of the mandatory transmission and reception requirements that must be met at the following levels.

- Functional
- Related function
- Message
- Word
- Data element
- Data item

To meet MIN IMP requirements, a system must implement all items within each level that are specified as mandatory before being able to satisfy the MIN IMP requirements

of the next lower level. Both functional and related function MIN IMP requirements must be satisfied before message MIN IMP requirements are satisfied. Similarly, message MIN IMP requirements must be satisfied before word MIN IMP requirements are met.

The following topics are addressed.

- Functional Minimum Implementation
- Related Function Minimum Implementation
- Message Minimum Implementation
- Word Minimum Implementation
- Data Element Minimum Implementation
- Data Item Minimum Implementation

C.2.2 Functional Minimum Implementation

The Link 22 functional areas that are used to identify the minimum implementation information exchange requirements are the following.

- Participant Location and Identification (PLI)
- Air Surveillance
- Surface (Maritime) Surveillance
- Subsurface (Maritime) Surveillance
- Land (Ground) Surveillance
- Space Surveillance
- Electronic Warfare (EW)
- Intelligence
- Weapons Coordination and Management

Note that Information Management is not included in the list as a function. The minimum implementation for Information Management messages is contained within the minimum implementation for other functions.

Participation on the Link 22 Interface requires that all participating systems/platforms implement the following.

- PLI
- Transmission of their own Platform and System Status message

A system can elect to implement a function that is not mandatory for MIN IMP because of National requirements defined in their own system implementation documentation. When a system elects to implement a non-mandatory function, the MIN IMP requirements at all lower levels for that function must be met. A system cannot elect to implement a non-mandatory item at an intermediate level (e.g., message or word) unless it has first implemented the MIN IMP requirements of all higher levels of that function beginning at the functional level.

C.2.3 Related Function Minimum Implementation

When a system implements either a mandatory or non-mandatory function for transmission, certain related functions must also be implemented to allow the interface to operate.

The bullets in the following figure indicate the related functions that are mandatory for implementation if the corresponding function is implemented. The implemented functions are listed down the left column. The required related functions are listed in the column headers at the top of [Figure C.2-1](#).

	PLI	Air Surv	Sur (Mar) Surv	Sub (Mar) Surv	Lnd (Gnd) Surv	Space Surv	Intel	Wpns Coord & Mgmt	EW
PLI	•								
Air Surv	•	•							
Sur (Mar) Surv	•		•						
Sub (Mar) Surv	•			•					
Lnd (Gnd) Surv	•				•				
Space Surv	•	•				•			
Intel	•	•1	•1	•1	•1	•1	•		•
Wpns Coord & Mgmt	•	•2	•2	•2	•2	•2	•2	•	•2
EW	•	•1	•1	•1	•1	•1	•		•

Notes.

1. At least one of the indicated Surveillance functions must be implemented for transmission and reception.
2. At least one of these functions must be implemented for reception

Figure C.2-1 Related Function Minimum Implementation

C.2.4 Message Minimum Implementation

The specific functional area in which a system participates determines the messages mandatory for MIN IMP. The particular messages that must be implemented by a system that implements a given function are dependent on the role of the platform.

Figure C.2-2 provides the requirements for PLI message MIN IMP.

For the full list of FJ-Series message or unique F-Series word implementation requirements for each function, refer to the [STANAG 5522], Annex B, Appendix 1. For any function, requirements for any related function (as specified in Figure C.2-1 in the previous section) must also be implemented.

MESSAGE TITLE/ ABBREVIATION	APPLICABLE WORDS	MIN IMP
Indirect Participant Location and Identification (PLI)	F1-0; F02.0-0	T3/R
Air PLI	F1-1; F02.1-0; F02.2-0; F02.2-1	T4/R
Surface PLI	F1-1; F02.1-0; F02.3-0	T4/R
Subsurface PLI	F1-1; F02.1-0; F02.4-0; F02.4-1	T4/R
Land Point PLI	F1-1; F02.1-0; F02.5-0	T4/R
Land Track PLI	F1-1; F02.1-0; F02.6-0; F02.6-1	T4/R
Notes: FJUN = A unit communicating on Link 22 and Link 16 while forwarding information among Link 22 and Link 16 participants. T3 – Transmission mandatory but allows non-FJUNs to transmit only applicable values but requires FJUNs to be capable of transmitting any value received form another link. T4 – Transmission mandatory and requires that the applicable PLI messages for the type of unit must be implemented R –Reception is mandatory		

Figure C.2-2 Common Message Minimum Implementation

C.2.5 Word Minimum Implementation

When a system implements either a mandatory or non-mandatory message for transmission, certain words within the message must be implemented to allow the interface to operate. A system's implementation documentation must be referenced to determine what additional words, Data Elements, and Data Items must be implemented.

F and FJ-Series MIN IMP requirements at the word, Data Element and Data Item levels are contained in [[STANAG 5522](#)] Annex B, Appendix 1. The tables are arranged by message number order.

C.2.6 Data Element Minimum Implementation

The following Data Elements, if present, must always be implemented for transmission and reception when the F-Series word in which they are contained is implemented.

- Series Indicator
- Label Indicator
- Label, F-Series
- Sublabel, F-Series
- Word Number

The required MIN IMP of other Data Elements within a word is listed by message in the "Data Element Minimum Implementation" tables in [[STANAG 5522](#)] Annex B, Appendix 1. If all the data elements with the exception of those listed directly above are designated optional and the word itself is implemented, at least one data element in the word must be implemented. When a Data Element is non-mandatory for MIN IMP, No Statement or the value specified in the note is required for transmission if a system does not implement the Data Element.

In all cases, Spare fields within a message are transmitted with a zero value.

C.2.7 Data Item Minimum Implementation

Certain messages contain action value fields. When these action value fields are set to different values, the meaning or use of a message may change, as well as the mandatory MIN IMP of words within the messages, Data Elements within the words, and data items within the Data Elements. These changes are reflected in the appropriate “Data Element Minimum Implementation” tables in [[STANAG 5522](#)], Annex B, Appendix 1.

This page is intentionally left blank.

Appendix D

Initialization

Parameter Generation

The DLP sends messages to the SNC during SNC Initialization, as discussed in Chapter 3 section [3B.1 SNC Initialization & Set-Up](#), and to initialize a network, as discussed in Chapter 3 section [3B.2 Network Initialization](#). This section identifies the parameters needed for these messages, and indicates where to find the data. This section is intended for software engineers that may be writing code to fill in the initialization messages, or for experienced operators that may need to manually enter fields for the messages if the software does not automatically do so.

This section requires an understanding of the following areas.

- Fundamental Link 22 Parameters, as described in Chapter 2, section [2B.2 Determining the Key Parameters](#)
- DLP-SNC IDD messages and fields, as detailed in the [[DLP-SNC IDD](#)]
- OPTASK Link Messages (OLM) and fields, as discussed in Chapter 2, section [2B.3 Generating the OLM](#)
- How to read an OLM, as detailed in Appendix B, section [B.1 OLM Information Extraction](#)

Some of the parameters required for the messages sent from the DLP to the SNC during SNC Initialization and Network Initialization come from the OLM, and some come from other sources. This section is divided into the following three sections.

- [Super Network Level Data from the OLM](#)
- [Network Level Data from the OLM](#)
- [NU Data Not from the OLM](#)

D.1 Super Network Level Data from the OLM

The Super Network level data required for SNC Initialization that is contained in the OLM file is listed in [Figure D.1-1](#). The rows in the figure are listed in the same order as the SNC Initialization messages that are sent to the SNC. The Field Name is the long name of the field and the Field in the second column is the Field Name’s abbreviation, as defined in the [\[DLP-SNC IDD\]](#). The OLM Set/Field column shows which field in the OLM is used to determine the value of the DLP-SNC message field. When the OLM value requires some conversion or logic, it is indicated by the Note # column. The associated numbered notes are in [Figure D.1-2](#).

DLP-SNC message Field Name	Field Abrv.	Msg #	OLM Set	OLM Field	Note #
SN Day of Week	SNDOW	301h	NSNET	OPERATIONAL START TIME OF THE SUPER NETWORK = SNDOW 1	1
Link 22 Address (for own unit)	TNUA	301h		00001-77777 octal	2
Lowest Allocatable NILE Address	LANA	304h	NSNET	LOWEST NILE ADDRESS	3
Number of NILE Units in OLM	NNUO	304h	NSNET	NUMBER OF LINK 22 NILE UNITS	
NILE Unit Link 22 Address	NUA	304h	NUDATA	LINK 22 ADDRESS	4
SNMU Link 22 Address	SNMU	305h	NSNET	SNMU ADDRESS	
Standby SNMU Link 22 Address	SNMUS	305h	NSNET	STANDBY SNMU ADDRESS	
Number of Networks	NNET	305h	NSNET	LINK 22 SUPER NETWORK INFORMATION	
Network ID	NID	305h	NNET	NILE NETWORK IDENTIFIER	5
NMU Link 22 Address	NMU	305h	NNET	NMU ADDRESS	
Standby NMU Link 22 Address	NMUS	305h	NNET	STANDBY NMU ADDRESS	
SNC Role Automatic Takeover Flag	ATF	331h	NUDATA	ROLE AUTOMATIC TAKE OVER FLAG	
Role Loss Timeout	RLT	331h	NUDATA	ROLE LOSS TIME OUT	
Number of NILE Units	NNU	32Fh	NSNET	NUMBER OF LINK 22 NILE UNITS	
NILE Unit Link 22 Address	NUA	32Fh	NUDATA	LINK 22 ADDRESS	

DLP-SNC message Field Name	Field Abbrv.	Msg #	OLM Set	OLM Field	Note #
NILE Unit Status	NUS	32Fh	NUDATA	UNIT NETWORK STATUS	6
Number of NILE Units	NNU	31Ch	NUDATA	RELAY SETTING	7
NILE Unit Link 22 Address	NUA	31Ch	NUDATA	LINK 22 ADDRESS	8
Relay Setting	RST	31Ch	NUDATA	RELAY SETTING	
Mission Area Sub-Network number (Network Membership MASNs)	MASN	313h	NNET	NILE NETWORK IDENTIFIER	5, 9
Number of NILE Units (Network Membership MASNs)	NNU	313h	NNETPART	NILE UNIT ADDRESS	10
NILE Unit Link 22 Address (Network Membership MASNs)	NUA	313h	NNETPART	NILE UNIT ADDRESS	
Mission Area Sub-Network number (Non-Network MASNs)	MASN	313h	NMASN	MASN IDENTIFIER	
Number of NILE Units (Non-Network MASNs)	NNU	313h	NMASN	MASN UNIT ADDRESS	10
NILE Unit Link 22 Address (Non-Network MASNs)	NUA	313h	NMASN	MASN UNIT ADDRESS	

Figure D.1-1 Super Network Initialization Data from the OLM

Note #	Notes
1	Increase SNDOW as necessary if current day is later than SN OST
2	Choose from NUDATA OLM sets the one matching the Own Ship
3	If not present in NSNET, default the value to 1
4	Include all NUs in the NUDATA sets, in the same order
5	Subtract 1 from OLM value (1-8) to get DLP SNC value (0-7)
6	Recommended to supply NU Status of every NU during initialization
7	Number of NUDATA for which RELAY SETTING is not 1 (not automatic)
8	Link 22 Address of a NU for which RELAY SETTING is not 1 (not automatic)
9	One Create MASN (313h) must be sent for each NILE Network in the OLM
10	Equal to the number of NILE Unit Addresses in the NNETPART set for the network

Figure D.1-2 Notes on SN Initialization Data from the OLM

Note that there are two different types of MASN_s that are supplied during SNC Initialization:

- Network Membership MASN_s (1-8)
- MASN_s (9-31)

MASN_s (9-31) are defined with the NMSN sets in the OLM. Network Membership MASN_s (1-8) are not defined with the NMSN set in the OLM, but are created using the network members (for each defined network in the OLM) from the NNETPART set of the OLM.

D.2 Network Level Data from the OLM

The network specific data required for SNC Initialization or Network Initialization that is contained in the OLM file is listed in [Figure D.2-1](#). The Field Name is the long name of the field and the Field in the second column is the Field Name’s abbreviation, as defined in the [\[DLP-SNC IDD\]](#). When the OLM value requires some conversion or logic, it is indicated by the Note # column. The associated numbered notes are in [Figure D.2-2](#).

Field Name	Field Abrv	Messages	OLM Set/Field	Note #
Number of LLC(s)	NLLC	302h	NNETPART/ NILE UNIT ADDRESS NNMEPARS/ NILE NETWORK MEDIA TYPE	1
Number of SPCs	NSPC	303h	NNETPART/NILE UNIT ADDRESS	2
LLC Integrity Flag	LIF	303h	NNET/LLC INTEGRITY INDICATOR	
Message Type		306h 307h 30Eh After Probing: 30Bh 30Dh	NNET/INITIALIZATION MODE NNET/NCS PROVIDER	3
Network Parameter Function	NPF	306h 307h 30Eh	N/A	4
Network ID	NID	303h 306h 307h 30Eh 30Bh 30Dh	NNET/ NILE NETWORK IDENTIFIER	5
Media Type	MT	306h 307h 30Eh 30Bh 30Dh	NNMEPARS/MEDIA TYPE	

Field Name	Field Abrv	Messages	OLM Set/Field	Note #
Frequency/ Hopset	FHS	306h 307h 30Eh 30Bh 30Dh	HF FF & UHF FF : NNMEPARS/PRIMARY FREQUENCY HF EPM: NNMEPARS/HF LINK 22 HOPSET UHF EPM: NNMEPARS/UHF LINK 22 HOPSET	6
Number of MSN	NMSN	307h		
Media Setting Number	MSN	306h 307h 30Eh 30Bh 30Dh	NNMEPARS/MEDIA SETTING NUMBER	7
Media Fragmentation Rate	MFR	306h 30Eh 30Bh 30Dh	NNMEPARS/MEDIA FRAGMENTATION RATE	
LLC Integrity Flag	LIF	306h 30Eh 30Bh 30Dh	NNMEPARS/LLC INTEGRITY INDICATOR	
Dynamic TDMA Flag	DTF	306h 30Eh 30Bh 30Dh	NNMEPARS/DTDMA INDICATOR	
Operational Start Time	OST	306h 30Eh 30Bh 30Dh	NNMEPARS/NILE NETWORK START TIME	8
Probing Start Time	PST	307h	NNMEPARS	
Access Delay Tolerance	ADT	306h 30Bh	NUBWR/NCS ACCESS DELAY TOLERANCE	
Efficiency	EFF	306h 30Bh	NUBWR/NCS EFFICIENCY	
Number of NILE Units	NNU	306h 30Bh	NUBWR/NILE UNIT ADDRESS	9
NILE Unit Link 22 Address	NUA	306h 30Bh	NUBWR/NILE UNIT ADDRESS	
Number of NILE Units	NNU	307h	NNETPART//NETWORK MEMBERS LINK 22 ADDRESS	10
NILE Unit Link 22 Address	NUA	307h	NNETPART//NETWORK MEMBERS LINK 22 ADDRESS	
Channel Capacity Need	CCN	306h 30Bh	NUBWR/CHANNEL CAPACITY NEED	
Channel Access Delay	CAD	306h 30Bh	NUBWR/CHANNEL ACCESS DELAY	
Number of Time Slots	NTS	30Eh 30Dh	NNCS/TOTAL NUMBER OF LINK 22 TRANSMISSION SLOTS	
Timeslot Size (Minislots)	TSS	30Eh 30Dh	NNCS/LINK 22 TRANSMISSION SLOT SIZE	
Timeslot Owner (Link 22 Address)	TSO	30Eh 30Dh	NNCS/UNIT LINK 22 ADDRESS	

Figure D.2-1 Network Specific Initialization Data from the OLM

Note #	Notes
1	Based on the LLCs available and attached to SPCs for the media types of the networks the unit is a member of
2	One SPC per Network the NU participates in
3	<p>Network Initialization message transmission is determined by the following.</p> <p>Initialization Mode = Short and NCS Provider = SNC: 306h</p> <p>Initialization Mode = Short and NCS Provider = DLP: 30Eh</p> <p>Initialization Mode = Probing: 307h</p> <p>After probing is complete:</p> <p>NCS Provider = SNC: 30Bh</p> <p>NCS Provider = DLP: 30Dh</p>
4	Set to 1 = OLM Initialize
5	Subtract 1 from OLM value (1-8) to get DLP SNC value (0-7)
6	<p>Requires conversion:</p> <p>HF FF: $\text{OLM value (Hz)} * 10 + 1.5\text{E}6$</p> <p>UHF FF: $\text{OLM value (Hz)} * 100 + 2.25\text{E}8$</p> <p>HF EPM: Not used, set to 0</p> <p>UHF EPM: Remove the leading "A" or "B" from the OLM string to get the Hex value for FHS</p>
7	The last digit of the OLM value is the MSN value for the DLP-SNC message
8	<p>Convert to seconds.</p> <p>Operational Start Time in seconds = OLM Hours (hh) * 3600 + OLM Minutes (mm) * 60</p>
9	Number of NILE Unit Addresses in the NUBWR set
10	Number of NILE Units in the NNETPART set

Figure D.2-2 Notes for Network Specific Initialization Data from the OLM

D.3 NU Data Not from the OLM

Some of the initialization data that may be different for each NU is included in the OLM, such as Link 22 Address, Relay Setting, Network membership, and ONCS timeslot assignments. Other data that is NOT contained in the OLM file that can be different for each NU is listed in [Figure D.3-1](#). The Field Name is the long name of the field and the Field in the second column is the Field Name's abbreviation, as defined in the [\[DLP-SNC IDD\]](#). Data which rarely changes may come from a configuration file. Other data will require the user to make decisions based on the contents of the OLM.

Field Name	Field Abrv.	Msg #	Typical Location	Range/Values	Typical Value
Smallest Message Preparation Time	SMPT	301h	Configuration file	1-1000 ms	50
Largest Message Preparation Time	LMPT	301h	Configuration file	1-1000 ms	500
Optimized Receive Protocol	ORP	301h	Configuration file	0=off, 1=on	1
BIT Repetition Rate	BRR	301h	Configuration file	0-60 seconds	5
Major Version	MJV	301h	DLP platform specific value	9-255	9
Minor Version	MNV	301h	DLP platform specific value	0-255	3
SNMU Capability Flag	SCF	301h	Configuration file or DLP Software	0=not SNMU capable 1 = SNMU capable	1
NMU Capability Flag	NCF	301h	Configuration file or DLP Software	0 = not NMU capable 1 = NMU capable	1
LLC Number	LLCN	302h 303h	Chosen from list of LLCs in a configuration file	1-4	1
LLC IP Address	LLCN	302h	Configuration file	IP Address	
LLC IP Port Number	LIPN	302h	Configuration file (Fixed by LLC H/W)	0-65535	5000
LLC Port ID	PID	303h	Configuration file, and Network media type (NNMEPARS OLM set) (Port on the LLC that the required SPC/radio is plugged into)	0-3	0
Key Information	KINFO	303h	LLC Key Position into which the Crypto Operator loaded the crypto key	0-63	0

Field Name	Field Abrv.	Msg #	Typical Location	Range/Values	Typical Value
LLC Port Data Rate	PDR	303h	Configuration file, must match the setting that the SPC H/W is configured to	0 = 19200, 1 = 28800, 2 = 38400, 3 = 57600, 4 = 115200, 5 = 230400, 6 = 460800, 7 = (Possible Future Ethernet, Not currently allowed for DLP input).	7
Function Management Setup fields: Network Management Function (NMF)	NMF	335h	Configuration file	NMF = 0-33 (Refer to Chapter 3, section 3D.3, Orders for complete list.) (0 = All Functions)	0
Function Management Setup fields: Automatic Compliance Switch (ACS)	ACS	335h	Configuration file	0 = DLP has to respond 1 = SNC responds with WILCO	1
Function Management Setup fields: Automatic Perform Function Switch (APFS)	APFS	335h	Configuration file	0 = DLP has to start the function 1 = SNC automatically starts the function	1
SPC Radio Power	SRP	306h 307h 30Eh	Configuration file	0 = No Control 1 = Min Tx Power 2 = Max Tx Power / 8 3 = Max Tx Power / 4 4 = Max Tx Power / 2 5 = Max Tx Power	0 or 5

Figure D.3-1 Non-OLM NU Data

Note that the Crypto Key itself is not needed by the software. The Crypto Key is loaded into the LLC. Only the location of the Crypto Key (Key Information) is needed. Additional information concerning Crypto Key and its location can be found in Appendix B, section [B.1.5 Determining Cryptographic Requirements](#) and in [3A.6.4 Crypto Key Management](#).

Appendix E

Acronyms and Abbreviations

AAW	Anti-Air Warfare	CANTCO	Cannot Comply
ACK	Acknowledgement	CAS	Course And Speed
ACS	Automatic Comply Switch	CIS	Configuration, Initialization & Status
AD	Access Delay	CLRQ	Complementary Link Reception Quality
ADAT	Automated Data Analysis Tool	<CN>	Classified Number
ADatP	Allied Data Publication	CN	Capacity Need
AJ	Active Join	CN/AD	Capacity Need / Access Delay
ANSI	American National Standards Institute	COMSEC	Communications Security
APFS	Automatic Perform Function Switch	CONN	Connectivity Forcing/Erasing
ASCII	American Standard Code for Information Interchange	COTS	Commercial off the Shelf
AST	Air Specific Type	CQOL	Complementary Quality of Link
ASW	Anti-Submarine Warfare	CRC	Cyclic Redundancy Check
ATH	Adjacent Timeslot Hand-Off	Crypto	Cryptographic Unit
ATI	Altitude/Time Indicator	CSCI	Computer Software Configuration Item
ATO	Air Task Order	CSM	Communication Service Message
BIA	Black-side Interface Adaptor	CSR	Cancel Service Request
BIT	Built-In-Test	CT	Communications Transport
BLOS	Beyond Line-Of-Sight	CV	Congestion Value
bps	Bits Per Second	CVLL	Crypto Variable Logical Label
C²	Command and Control	DA	Data Analysis
C&S	Control and Status	DCE	Data Communication Equipment
CAM	Congestion Assessment Management	DECR	Decrypt

Dest	Destination	FLOW	Flow Control/Metering protocol
DFI	Data Field Identifier	FNU	Forwarding NILE Unit
DIF	DLP Interface	FNUA	Forwarding NILE Unit to from TDL A (Link 11)
DIR	Directory Maintenance	FNUAB	Forwarding NILE Unit to from TDL A and B
DIS	Distributed Interactive Simulation	FNUB	Forwarding NILE Unit to from TDL B (Link 11B)
DIVS	Data Integrity Validation Service within the LLC	FPU	Forwarding Participating Unit
DLP	Data Link Processor	FRU	Forwarding Reporting Unit
DLRP	Data Link Reference Point	GByte	Gigabyte
DOW	Day of Week	GD	Guaranteed Delivery
DR	Data Reduction	GDI	Global Data and Initialization
DRX	DLP Interface Reception	GHz	Gigahertz
DTD	Data Terminal Device	Gnd	Ground
DTDMA	Dynamic Time Division Multiple Access	GPS	Global Positioning System
DTE	Data Termination Equipment	GRU	Gridlock Reference Unit
DTX	DLP Interface Transmission	HF	High Frequency
DU	Data Unit	HMI	Human Machine Interface
DUCC	Data Unit Configuration Code	HR	High Reliability
DUI	Data Use Identifier	HUR	High Update Rate
DUR	Data Update Request	Hz	Hertz
DX	Data Extraction	ICV	Instantaneous Congestion Value
E2ERN	End To End Reference Number	ID	Identifier
EDAC	Error Detection and Correction	ID	Identity
EIP	Embedded INFOSEC Product	ID	Identification
EMCON	Emission Control	IDD	Interface Design Document
ENCR	Encrypt	IEEE	Institute of Electrical and Electronics Engineers
EPM	Electronic Protective Measures	IER	Interface Exchange Requirement
ESI	Explicit Source Identification	IJ	Inactive Join
EW	Electronic Warfare	ILM	Initialization, LNE and Configuration Management
FAM	Fault Management	IND	Indicator
FF	Fixed Frequency	INF	Infrastructure
FHS	Frequency Hopset		
FJU	Forwarding Link 16 MIDS Unit		

INFOSEC	Information Security	Mbps	Megabits per second
INIT	Initialization	MCF	Media Coding Frame
Intel	Intelligence	MCM	Media Control and Management
IP	Internet Protocol	MF	Management Function
IPROB	Initialization with Probing	MHz	Mega Hertz
ISO	International Organization for Standardization	MIDS	Multifunctional Information Distribution Systems
ISS	In-Service Support	MIF	Media Interface
IU	Interface Unit	MIL-STD	Military Standard
JCRYPDAT	Link 16 and Link 22 Cryptographic Data (OLM Set)	MIN IMP	Minimum Implementation
JREAP	Joint Range Extension Application Protocol	MLDA	Multi-Link Data Analysis
JTIDS	Joint Tactical Information Distribution System	MLDR	Multi-Link Data Reduction
JTRS	Joint Tactical Radio Systems	MLSD	Multi-Link Scenario Developer
JU	Link 16 MIDS Unit	MLSG	Multi-Link Scenario Generator
kHz	kiloHertz	MLST3	Multiple Link System Test & Training Tool
KMP	Key Management Plan	MLTS	Multiple Link Test System
LAD	Leg Acknowledged Delivery	MOD	Ministry of Defense
LAN	Local Area Network	MODEM	Modulation and Demodulation
LANA	Lowest Allocatable NILE Address	MOU	Memorandum of Understanding
LCD	Link Connectivity Data	MP	Message Packet
LED	Light-Emitting Diode	MP/NP	Message Packet to Network Packet ratio
Leg MPRN	Leg Message Packet Reference Number	MPA	Media Parameter Acquisition
LLC	Link Level COMSEC	MPE	Message Packet Expansion
LLS	Latitude/Longitude Scale	MPR	Message Preparation Request
LNE	Late Network Entry	MPRN	Message Packet Reference Number
LO BATT	Low Battery	MPT	Message Preparation Time
LOS	Line-Of-Sight	MR	Machine Receipt
LRQ	Link Reception Quality	MRX	Media Reception
LSB	Least Significant Bit(s)	MS	Media Simulator
LVT	Low-Volume Terminal	MSB	Most Significant Bit(s)
MASN	Mission Area Sub Network	MSN	Media Setting Number
		MTV	Message Time of Validity

MTX	Media Transmission	NPR	Network Packet Reception
MUUT	Multiple Units Under Test	NRS	NILE Reference System
N/A	Not Applicable	NSA	National Security Agency
NACK	Negative Acknowledgement	NSNET	Link 22 (NILE) Super Network Information (OLM Set)
NATO	North Atlantic Treaty Organization	NST	Network Start Time
NCE	NILE Communications Equipment	NU	NILE Unit
NCH	NCS Handler	NUBWR	Link 22 (NILE) Unit Bandwidth Requirement (OLM Set)
NCRYPLST	Network Cryptographic Resource Description (OLM Set)	NUDATA	Link 22 (NILE) Unit Data (OLM Set)
NCS	Network Cycle Structure	NULRQ	Link 22 (NILE) Unit Link Reception Quality (OLM Set)
NCSC	NCS Changes (due to DTDMA and LNE NCS)	OLM	OPTASK Link Message
NCT	Network Cycle Time	ONCS	Operational Network Cycle Structure
NILE	NATO Improved Link Eleven	OPORD	Operation Order
NMASN	Link 22 (NILE) Mission Area Sub Network (OLM Set)	OPTASK	Operational Tasking
NMC	Network Management and Control	OST	Operational Start Time
NMF	Network Management Function	OTC	Officer in Tactical Command
NMM	Network and Monitoring Management	P2P	Point-To-Point
NMU	Network Management Unit	PC	Personal Computer
NN	NILE Network	PI	Priority Injection
NNCS	Link 22 (NILE) Network Cycle Structure (OLM Set)	PII	Priority Injection Indicator
NNET	Link 22 (NILE) Network Information (OLM Set)	PLI	Participant Location and Identification
NNETPART	Link 22 (NILE) Network Participants (OLM Set)	PMI	Packed Message Indicator
NNMEPARS	Link 22 (NILE) Network Media Parameter Settings (OLM Set)	PMO	Project Management Office
NonC2	Non Command and Control	PMW	Program Management Warfare
Non-MR	Non Machine Receipt	POS	Position
NP	Network Packet	PPLI	Precise Participant Location and Identification
NPG	Network Participation Group	PPS	Pulses Per Second
NPP	Network Packet Production	PRNU	Potential Relay NILE Unit
		PRQ	Probing Reception Quality
		PRR	Preparation Request Response

PTOC	Partial Timeslot Ownership Change	SNC	System Network Controller
PTT	Push-to-talk	SNC♦	System Network Controller Diamond
PU	Participating Unit	SNMU	Super Network Management Unit
QoS	Quality of Service	SPAWAR	Space and Naval Warfare Systems Command
R/C	Receipt/Compliance	SPC	Signal Processing Controller
R2	Reporting Responsibility	SRID	Service Request Identifier
RCV	Routing Control Value	SS	Segment Specification
Ref	Reference	STANAG	Standardization Agreement
RF	Radio Frequency	STD	Standard
RIA	Red-side Interface Adaptor	SU	Supporting Unit
RPRNU	Reporting Potential Relay NILE Unit	SUB	Subsurface
RRM	Relay and Routing Management	SUMs	Software User's Manuals
RS	Reed-Solomon	SUR	Standard Update Rate
RTA	Reallocation Total capacity Amount	SUR	Surface
RU	Reporting Unit	SWAP	Swap Timeslots
Rx	Receive	TACT	Tactical Interface
RxD	Receive Data	TC	Totalcast
RxP	Reception Probability	TCP	Transmission Control Protocol
SCH	Scheduler	TCUI	Test Controller User Interface
SD	Scenario Developer	TDL	Tactical Data Link
SDU	Secure Data Unit	TDMA	Time Division Multiple Access
Sec	Seconds	TDS	Tactical Data System
SER	Series	TEG	Timing Event Generator
SG	Scenario Generator	TFOM	Time Figure of Merit
SGEX	Scenario Generator Extractor	TMW	Tactical Message Words
SGSV	Scenario Generator Server	TN	Track Number
SGWS	Scenario Generator Workstation	TOC	Timeslot Ownership Change
SHF	Super High Frequency	TOD	Time of Day
SIM	Simulation	TOW	Time of Weekday
SJ	Silent Join	TQ	Track Quality
SLURP	Slow Update Rate Protocol	TRANSEC	Transmission Security
SN	Super Network	TRH	Transmission Request Handler

TSDF	Time Slot Duty Factor	UTL	Utilities
TSN	Time Slot Number	UUT	Unit Under Test
TSR	Transmission Service Request	VME	Versa Module Europa
Tx	Transmission	WGS	Worldwide Geodetic System
TXC	Transmission Completed	WILCO	Will Comply
TxD	Transmit Data		
UDP	User Datagram Protocol		
UHF	Ultra High Frequency		
UK	United Kingdom		
US	United States		
UTC	Universal Time, Coordinated		

Appendix F

Glossary

Access Delay	Describes the recurrence of transmission opportunities in the ONCS for a NU.
Access Delay Tolerance	Defines the tolerance that is considered acceptable in the calculated ONCS access delay.
Accuracy	A measure of the errors between what is perceived and what actually exists.
Acknowledge	The act of notifying a unit transmitting a message that the message has been correctly received.
Active Join	When a LNE unit wants to join a network and it is already an active member of at least one other NILE Network
ADAT	Automatic Data Analysis Tool
Address	A number applied to an Interface Unit to associate information and directives with Interface Units or tracks for both digital and voice communications.
Addressee	A unit to which a message is addressed
ASCII	American Standard Code for Information Interchange
Assignment Slot (AS)	A transmission timeslot, which is assigned for the use of a NU. Constructed of a contiguous number of Minislots.
Backward Compatibility	<p>The ability of a DLP which is using an older definition of the DLP-SNC interface to use the latest version of the SNC software.</p> <p>When a technical message is expanded, the SNCs of older versions are able to interpret the portion of the technical message associated with its version or earlier versions, while new fields in a message will only be used by the newer SNCs.</p>
Baud	<p>A unit of modulation rate. One baud corresponds to a rate of one unit interval per second, where the modulation rate is expressed as the reciprocal of the duration in seconds of the shortest unit interval.</p> <p>2. A unit of signaling speed equal to the number of discrete signal conditions, variations, or events per second.</p>
BLACK Data	In cryptographic systems, data that has already been encrypted.
Broadcast (BC)	Generic term for the transmission of data to the Source's RF neighbors (i.e., no use of relay takes place).
C² platforms	Platforms that have the required equipment, mission and personnel to exercise command and control authority.

Cannot Comply (CANTCO)	A response message indicating that a function cannot perform a previously requested function.
Capacity Need	Specifies how many tactical data words per second a NU wants to be able to transmit.
Communications Security (COMSEC)	The security measures that protect user data against unauthorized disclosure & tampering.
Compatibility	The ability of two communications systems to exchange data. NOTE Although Compatibility is necessary to achieve Interoperability, Compatibility does not guarantee Interoperability since Compatibility does not imply that the users of the communications systems are able to understand the data exchanged.
Complementary Link Reception Quality (CLRQ)	The measure of correct reception probability in the opposite direction to Link Reception Quality.
Control and Status Interface	A partition of the DLP/SNC interface, for the transfer of control and status information.
Data Element (DE)	A basic unit (class) of information having a unique meaning and subcategories (Data Items) of distinct units or values. The Link 22 Data Element is the DUI. In Link 22 (and Link 16) DUI is synonymous with Data Element.
Data Field Identifier (DFI)	A category of data whose specification includes one or more DUI specifications. Each DUI's class of data must fall within the bounds of the DFI category.
Data Forwarding	The process of receiving data on one digital data link and outputting the data, using proper format and link protocols, to another type of digital data link(s). In the process, a message(s) received on one link is translated to an appropriate message(s) on another link. Data Forwarding is accomplished by the selected forwarding unit(s) simultaneously participating on more than one type of data link. The data that is forwarded is based on the data received and not dependent upon the local system data of the data forwarding unit or its implementation of the received message or the forwarded message. Data Forwarding is not covered by the NILE system specifications.
Data Link	Means of communication for transmission and receipt of a data message.
Data Link Processing (DLP)	The set of functions, which allow a TDS to interface to the Link 22 SNC. These functions include the formatting and generation of Link 22 format messages, data filters, correlation, determination of Reporting Responsibility, etc. In a Data Forwarding unit, the forwarding of data between Link 22 and other tactical data links (Link 16, Link 11) is part of the DLP function.
Data Link Server	An MLTS program which is responsible for maintaining track databases, performing message processing, providing data to TCUI for display, and the extraction of MLST3/DLP-SNC (or SNC♦) interface.
Data Message	A group of binary digits (bits) containing encoded tactical information.

Data Originator	The IU which first injects data onto a tactical data link. During multi-link operations, the Data Originator need not be a NU.
Data Use Identifier (DUI)	In Link 22 (and Link 16), DUI is synonymous with Data Element.
Delay	The time between initiation of a process and completion of that process.
Destination	A NU or group of NUs to which a Message is addressed.
Direct LRQ	The LRQ value which represents how well the unit is able to receive directly from the other units in the network. This LRQ value is calculated using the Reception Probability (RxP).
DIS	Distributed interactive Simulation
Duplicate Detection	Duplicate Detection is the process used to determine whether a Message Packet (MP) has already been received or not. In order for a MP to be a duplicate the following attributes all have to be the same: Message Time of Validity (MTV), Source (MILE Address), Type (Tactical or Technical), and Data Unit (Size and Contents).
Dynamic List Address	A means of addressing a message to a limited number of NUs. (Differs from MASN in that the members of the dynamic list are not predefined.)
Dynamic TDMA (DTDMA)	A form of TDMA where ownership of transmission capacity is transferred between NUs. (Note the length of the NCT remains unchanged by the DTDMA processes.)
Efficiency	The degree to which a system provides quality of service measured in terms of throughput, delay and reliability.
Electronic Counter Counter Measures (ECCM)	The division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of EW. (Used interchangeably with Electronic Protective Measures (EPM)).
Electronic Protective Measures (EPM)	The division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of EW. (Used interchangeably with Electronic Counter Counter Measures (ECCM)).
Electronic Warfare (EW)	Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action taken to retain its effective use by friendly forces.
Error Detection and Correction (EDAC)	A technique or scheme for coding information such that transmission errors can be detected and corrected.
FJ-Series Message	J-Series messages packed into a 72-bit word for use on Link 22.
FJ Unit	A unit communicating on Link 22 and Link 16 while forwarding information among Link 22 and Link 16 participants
Flexibility	The ability of a system to react positively to change.
Flooding	The relay of designated data by each NU receiving that data. Flooding is used to provide a high probability of reception of specified data by all NUs in a NILE network.

Forwarding NILE Unit (FNU)	A NILE Unit that has the responsibility for the transfer of data between Link 22 and one or more other data link(s). To achieve this, the FNU must be capable of concurrent operation on Link 22 and the other data link(s). This term and functionality are no longer used.
Fragment	An incomplete part of a message.
Frequency Hopping (FH)	An EPM technique in which the instantaneous carrier frequency of a signal is periodically relocated, according to a predetermined code, to other positions within a frequency band much wider than that required for normal message transmission. The receiver uses the same code to keep in synch with the hopping pattern.
F-Series Message	Digital message format employed in STANAG 5522.
Guaranteed Delivery (GD)	A NCE protocol whereby a message is automatically retransmitted until the destination confirms correct reception or the system determines that the destination is unreachable at an acceptable cost.
Guard Time (GT)	A time interval left vacant between transmissions, used for the switching and/or tuning of radios and used to account for propagation delay.
Header	Information to support the communications services required by an associated block of information (as opposed to the information itself).
High Reliability (HR)	A transmission service that provides a higher statistical probability of correct reception.
Hop	The dwell time of a frequency hopping system.
Host System	Also known as the Tactical Data System (TDS), which processes the received tactical messages and generates tactical messages for transmission in accordance with the unit's national requirements.
Inactive Join	When the LNE unit requests to join a network and it is not an active member of any NILE Networks.
Inactive NU Status	Any NU currently not part of the (Super) Network (Failure, Maintenance, etc.) with or without a Timeslot assigned.
Information Security (INFOSEC)	The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. INFOSEC includes COMSEC, NETSEC, and TRANSEC.
INFOSEC Subsystem	The set of functions, which provides the required level of INFOSEC for the Link 22 system.
Integrity	A characteristic of INFOSEC in which unauthorized modification, creation or deletion of information objects can be detected. Also referred to as LLC Integrity.
Interface Unit (IU)	A NU, JU, PU, or RU communicating (directly or indirectly) on the Data Link interface.
Interoperability	The ability of systems, units, or forces to provide services from other systems, units, or forces and to use these services so exchanged to enable them to operate effectively together.
J-Series Message	Digital message format employed in STANAG 5516.

Key Rollover	This rollover causes the Day Of Week (DOW) of the LLC (when 1 to 6) to increase by one, and if the DOW is at 7 this causes the DOW to be reset to 1 and the LLC to rollover the key to the next week's key.
Key Zeroization	Deletion of the key held by the LLC.
Late Network Entry (LNE)	The procedure required permitting a non-participant in an established NILE Network to become a member of the network.
Leg	<p>The communications link between a pair of NUs that are RF neighbors on one or more Networks. Also a unit of measure of the length of a communications path between NUs – the length, in legs, of the communications path between NUs is defined as:</p> $1 + \text{number of Relay NUs in the Path.}$
Leg Injection Packet (LIP)	A distinct block of information used to communicate a set of Messages and or Message Fragments requiring the same communications services. A LIIP is subdivided into a Data Unit (DU) and a Service Header (SH) where the DU contains the Message(s) or fragment of a Message and the SH contains the protocol information required to communicate the message.
Leg Reliability	The protocol used by the SNC to determine the number of transmissions required and the number of fragments allowed, to meet the requested reception reliability. This protocol is performed independently for each required leg.
Link 11	An automatic high speed HF/UHF data link exchanging picture compilation, command status, and control information. It uses M Series messages, a Roll Call protocol and kineplex waveform. Also referred to as TADIL A.
Link 16	A secure jam resistant nodeless data link that utilizes the Multifunctional Information Distribution System (MIDS) and the protocols, conventions, and fixed word message formats defined by STANAG 5516. Also referred to as TADIL J.
Link 22	A secure tactical data link which uses the NCE and the protocols, conventions and message formats defined by STANAG 5522.
Link 22 Address	A 15-bit number used by the TDS/DLP segments of the Link 22 system to uniquely identify each NU. The Link 22 Addresses are coordinated with those of other data links (e.g. Link 16) and are distributed to NUs via the OPTASK LINK message prior to the deployment of an SN. Link 22 tactical messages and DLP/SNC interface messages use the Link 22 Address to identify NUs. A NU must have been allocated a Link 22 Address before it can participate on Link 22.
Link Connectivity Data (LCD)	Represents the SN bi-directional connectivity between two NUs that are three legs away.
Link Level COMSEC (LLC)	A COMSEC function provided within the Link 22 Media segment. It provides both COMSEC and NETSEC for Link 22.
Link Quality (LQ)	The bi-directional measure of correct reception probability on a given RF link.

Link Reception Quality (LRQ)	The measure of correct reception probability on a given (unidirectional) RF link.
Live Link	An MLST3 test configuration similar to the Multiple Units configuration except that real SPCs are used to provide connectivity between the units on any Live Network.
Machine Receipt (MR)	A destination which requires an acknowledgement from the addressees. MR destinations may take precedence over Non-MR destinations. An end to end acknowledgement.
Major Version Number	One part of the SNC Version. The Major Version Number changes only when there is an incompatibility between major SNC versions.
Maximum Perishability	The maximum lifetime for a message.
Media	In the NCE system architecture, the Media segment provides the Data Link and Physical (Layer 1 & 2) functions. Its primary function is to provide a NP delivery service on each frequency band for which a NILE capability is required. The Link 22 Media segment includes the Link Level COMSEC, SPC and Radio subsystems.
Media Coding Frame (MCF)	The smallest unit of data, which is exchanged in peer to peer communications between NUs at the Data Link Layer.
Media Dependent	Having a different value when used with different NILE media.
Media Setting Number	Specifies the setting of SPC parameters: Waveform, Modulation, Guard Time, Repetition Rate, and EDAC parameters. It consists of a reference for the SPC to the appropriate set.
Message	The collection of information, which needs to be communicated to achieve a prescribed objective. A Link 22 Message consists of a number of fields in a fixed arrangement.
Message Packet	An entity used by the SNC to contain message data that is to be sent to a common set of addressees with a common service requirement.
Message Packet Store	The storage used by duplicate detection to save information about the message packets that have been received and their contents, so that it may detect whether a received message packet is a duplicate.
Message Preparation Request (MPR)	A message on the DLP/SNC control & status interface used by the SNC to request tactical message data from the DLP.
Message Preparation Time (MPT)	The time required by the DLP to produce tactical messages in response to a MPR.
Message Source	The NU from whom a message was received, i.e. the RF neighbor NU whose transmission has been received.
Message Time of Validity (MTV)	The TOV of an individual message.
Minislot	The smallest unit of time into which the NCS is allowed to be subdivided. A NCS consists of an integer number of Minislots. The size of a Minislot is media dependent.

Minor Version Number	One part of the SNC Version. The Minor Version number is used for all SNC changes which are backward compatible with previous Minor Versions for the same Major Version.
Mission Area Sub Network (MASN)	A group of one or more NUs sharing a common collective address.
MLSD	Multi-Link Scenario Developer
MLST3 Single	An MLST3 test configuration in which MLST3 is used as a single unit DLP.
MS Standalone	An NRS configuration which allows the testing of a national DLP without using real SPCs, which are replaced by the Media Simulator.
M-Series Message	Digital message format employed in STANAG 5511 Edition 2 (Edition 3 is in the process of ratification. After ratification, it will supersede Edition 2).
Multi-Link System Test & Training Tool (MLST3)	The interoperability test system which was extended to incorporate Link 22, and has multiple configurations available for testing.
Multiple Units	An MLST3 test configuration which can be run with up to five SNC UUTs with up to 32 simulated units, provided by the SNC ♦. The main purpose of this configuration is to test national DLPs using a real SNC, with the MLST3 providing the rest of the test environment.
Multiple Units Under Test (MUUT)	An NRS configuration which provides the ability to test between two and five real SNCs (UUTs), without the use of simulated units. This configuration also tests the functionality of the LLC.
NCE Simulation	An MLST3 test configuration which is an extension of the System Simulation configuration.
Neighborcast (NC)	Delivery of messages to all RF neighbors.
Net	Synonymous with Network.
Network	See NILE Network.
Network Connectivity	The topological description of a network, which specifies the interconnection of the transmission nodes in terms of circuit termination locations and quantities.
Network Cycle	A periodic, recurring sequence of Timeslots during which each active NU has at least one Assignment Slot.
Network Cycle Structure (NCS)	The partitioning and allocation of transmission capacity/opportunities within a Network Cycle.
Network Cycle Time (NCT)	The time taken to complete a Network Cycle.
Network Initialization (NI)	The processes required enabling a Network to become operational.
Network Management Unit (NMU)	The NU responsible for the management of a NILE Network during normal operations.

Network Packet (NP)	SNCs communicate information on NILE Networks using Network Packets. A NP consists of an integer number of LIPs together with a Network Packet Header. A NP is either received complete and correct or not received at all. The size of a NP is media dependent.
Network Packet Header	Information inserted into a NP to enable the LIPs contained in the NP to be packed efficiently in the NP and to be unpacked by receiving NUs. The NP Header size and contents are dependent on the capacity of the NP for which it is generated.
NILE	<ol style="list-style-type: none">1. NATO Improved Link 11 (NILE) is the former name for Link 22, and as such is used in some earlier documentation and is synonymous with Link 22.2. NILE is also used to refer to the international project organization to support the development of the NCE. See also NILE Communications Equipment.
NILE Address	A 7-bit number used by the SNC segment of the Link 22 system to uniquely identify each NU in a SN. NILE Addresses are automatically allocated to NUs during SN initialization. The SNMU will be responsible for managing the allocation of NILE Addresses to NUs that did not obtain a NILE Address during SN initialization. The SNMU may also allocate NILE Addresses to RUs to enable them to be identified as the source of data forwarded from other data links. The NILE Address is not visible to the TDS/DLP segments of the Link 22 system.
NILE Communications Equipment (NCE)	A communications system to support Link 22. NCE consists of a DLP interface, a System Network Controller (SNC), a Link Level COMSEC subsystem, and the appropriate Signal Processing Controller(s) / radio equipment.
NILE Network (NN)	A collection of NUs exchanging information in accordance with STANAG 5522 using a single medium and a unique set of network parameters.
NILE Reference System (NRS)	Test tool essential to the development, life cycle support, and performance validation of the Link 22 system. The NRS will verify the Link 22 system compliance with requirements established in the Link 22 System specification, the System Network Controller specification and other specifications associated with NILE development.
NILE Super Network (SN)	A deployed Link 22 system that may operate using one or more connected NILE Networks.
NILE Unit (NU)	A NILE node with a Link 22 address. It is capable of transmitting and/or receiving information in accordance with STANAG 5522.
Non- C² platforms	Platforms executing or supporting missions that receive information and may also contribute information to the picture.
Non Machine receipt Addressee (Non-MR Addressee)	An Addressee who is not required to respond with a Machine Receipt.

OSI Seven Layer Model	<p>A communications architecture model proposed by the internal Standards Organization, comprising the following layers:</p> <ol style="list-style-type: none"> 1. Physical Layer 2. Data Link Layer 3. Network Layer 4. Transport Layer 5. Session Layer 6. Presentational Layer 7. Application Layer
Overhead	<p>Digital information transferred across the functional interface separating a user and a telecommunications system (or between functional entities within a telecommunications system) for the purpose of directing or controlling the transfer of user information and/or the detection and correction of errors.</p> <p>NOTE: Overhead information originated by the user is not considered as system overhead. Overhead information generated within the system and not delivered to the user is considered as system overhead. Thus, user throughput is reduced by both overheads while system throughput is only reduced by system overhead.</p>
Participating Unit (PU)	A unit with a Link 11 address.
Perishable Message	A message, which is identified as having a finite lifetime.
Point-to-Point	A transmission mode that provides delivery of the associated message to a specific NU. (This does not mean that other NUs cannot receive and/or understand the message.)
Potential Relay NILE Unit (PRNU)	A NU that is capable of performing Relay in the current NILE Super Network configuration.
Preamble	Information about a call and its contents provided at the start of a digitized message. In addition, a name sometimes given to the initial training sequence of a Single Tone (HF) Modem.
Preparation Request Response (PRR)	A message on the DLP/SNC control and status interface used by the DLP to identify tactical messages being supplied in response to a MPR.
Priority	An attribute of a Message used by the SNC to schedule transmissions. Messages have a priority in the range 1-4, with 1 being the highest.
Priority Injection Indicator (PII)	The Priority Injection Indicator is a flag which can be set in only TSR's for a tactical message with Priority 1. The PII when set indicates that it is an important message which is eligible for early transmission in a Priority Injection slot. When the PII is set, the TSR is put at the bottom of any other PII TSRs which are at the top of the TSR Queue for Priority 1.
Priority Injection Slot (PI Slot)	A Timeslot not assigned to any NILE Address (has a NILE Address of zero). Only used for the transmission of Priority 1 Tactical messages that are eligible for additional early transmission. Used for an additional earlier transmission of important messages when the next assigned timeslot is more than 2.5 seconds later.
Priority Message	A message, which is eligible for transmission in an Interrupt Slot.

Probing	A mechanism to assess the quality of the radio channel in order to get the knowledge of the Network connectivity (used during Network Initialization).
Protocol	A set of unique rules specifying a sequence of actions necessary to perform a communications function. NOTE: Protocols may govern portions of a network, types of service, or administrative procedures. For example, a data link protocol is the specification of methods whereby data communication over a data link is performed in terms of the particular transmission mode, control procedures, and recovery procedures.
Quality of Service	A set of qualities related to the provision of a service, as perceived by a user.
Radio Silence Status	Any NU that has a Timeslot assigned, but by choice or order is not allowed to transmit. It is able to receive, but not send and acknowledge messages. It may break the 'Radio Silence' status and inject messages upon request of its own DLP.
Real Time	Real Time is when the delay introduced by a system is critical to the users of that system or an associated system.
Reallocation	The transfer of transmission capacity from one NU to another after it has been determined that the required conditions for making the Reallocation are met according to information held by the Donor NU.
Receive Only NU Status	Any NU that has NO Time Slot assigned and is only receiving messages on all networks.
RED Data	In cryptographic systems, data that has not been encrypted.
Relay	The retransmission of data received from another NU. Relay is intended to increase the range coverage of Link 22 and to increase the probability of correct reception by the intended recipient(s). Relay may take the form of retransmission on the same or different NILE network from the one on which they were received.
Relay Setting – Automatic	(R)PRNU status depends on the de-centralized Relay Status-determination protocol.
Relay Setting - Inhibited	NU is inhibited by the SNMU from acting as a RNU or a (R)PRNU.
Relay Setting - Preferred	NU is assigned by the SNMU as a preferred RPRNU.
Relay Unit	A NU, which is performing Relay.
Reporting Potential Relay NILE Unit (RPRNU)	RPRNUs are a special subset of PRNUs that are used to minimize injections when MPs are required to be routed to undetermined destinations and/or multicast addresses.
Reporting Responsibility	The requirement for the IU with the best positional data on a track to transmit track data on the interface.
Reporting Unit	A RU is the unit taking part in the exchange or transfer of tactical data on another digital data link (not Link 22) to which data can be addressed, and from which data can be identified as to source.

Resilience	The ability to recover quickly from undesired change.
RF Neighbor	A track who is within one leg of RF reception.
Role Loss Timeout	The number of minutes that the SNC should wait before declaring the loss of the (S)NMU.
Roll Call	Normal mode for current Link 11 operation. Unit polled by the net control station broadcasts its data, then relinquishes the network to the net control station, which then polls another unit in accordance with a predefined polling sequence.
Routing	The intelligent determination of the path to be followed by messages, from the Originator to the final Destination.
Scenario Generator (SG)	A collection of tools for scenario development, test execution, data recording, and data analysis that are used to prepare, execute, and analyze tests with the NRS.
Sequence Identifier	An ID which is used to bind requests with responses. The request, subsequent request messages, and the associated response message will all have the same Sequence Identifier. Messages with the same Sequence Identifier are collectively called a transaction. The Sequence Identifier is managed by the SNC and are monotonically increased in successive transactions.
Service Header	Part of a LIP containing the SNC protocol information that is required by the receiving NUs to process the accompanying Data Unit. The protocol information contained is dependent on the communication service options selected for communication of the message, e.g. High Reliability, Machine Receipt.
Service Request	A request for service from a client application to a service application.
Service Request Identifier (SRID)	An identifier used by the DLP/SNC interface to identify Transmission Service Requests (TSRs).
Signal Processing Controller (SPC)	The NCE segment which roughly corresponds to the Data Link and Physical Layers in the ISO 7 Layer Communications Model. The functions of the SPC include Error Detection and Correction, Signal Modulation/Demodulation and TRANSEC.
Silent Join	When the LNE unit is not an active member of any NILE Network and wants to listen to the network without making any transmissions
Slot	Timeslot
SNC Diamond (SNC♦)	A component of the NRS. The SNC♦ is capable of representing either a single SNC or a community of SNCs.
SNC Verification	The primary NRS configuration used to verify the functionality of the SNC. SNC Verification involves a single SNC UUT being tested with up to 124 simulated units. The media connectivity is provided by the Media Simulator.
Source	The NU from which a transmission is received.
Super Network (SN)	NILE Super Network

Super Network Directory	Information about Units in the Super Network including: a) Link 22 and NILE Addresses b) Mission Area Sub Network c) NU Status and Relay Setting of each NU d) Roles.
Super Network Management Unit (SNMU)	The NU responsible for the management of a NILE Super Network during normal operations.
Synchronization	The process of adjusting corresponding significant instants of two signals to obtain a desired fixed relationship between these instants.
System Network Controller (SNC)	The NCE segment that roughly corresponds to the Transport & Network Layers in the ISO 7 Layer Communications Model. The primary function of the SNC is to provide a basic end to end message communications service between NUs which are members of a deployed NILE Super Network.
System Simulation	An NRS configuration which is used to validate NRS test scenarios. This configuration uses multiple computers to ensure that sufficient computer resources are available, especially when running stress test scenarios.
Tactical Data System	The source and sink for Link 22 tactical messages. In Link 22, TDS is used as a generic term for a command and control system that uses Link 22.
Tactical Interface	The partition of the DLP/SNC interface used for passing tactical messages.
Tactical Message	A functionally oriented, variable length, string of one or more words in fixed word format.
Takeover	The ability of the Standby (S)NMU to assume the role of (S)NMU, if a loss is detected.
TDL Management	TDL Management is the function performed by the unit responsible for initiation, operation, and termination of data link operations. This unit may delegate management of portions of the architecture, including portions of the link 16 network, to subordinate units.
Technical Message	A functionally oriented, variable length group of related fields containing information for the maintenance and optimization of the network (Network Management)
Test Controller User Interface (TCUI)	An MLTS program which is responsible for providing the Human Machine Interface (HMI), displaying the tactical messages, and providing the tactical situation display.
Time Division Multiple Access (TDMA)	A communication technique that utilizes a common channel (multipoint or broadcast) for communications among multiple users by allocating unique timeslots to the different users.
Time Figure of Merit (TFOM)	Defines the inaccuracy of the Time of Day in regards to the Universal Time.

Time Index	The index into the MP and E2ERN data structures. The Time index is calculated using the modulus function and the Message Time of Validity, taking into account any midnight boundaries that have been crossed and the length of the circular buffer.
Time of Validity (TOV)	The reference time at which data is considered to be valid. The SNC uses the time of occurrence of a Timeslot to determine this reference time; either the Timeslot in which the message is received or an offset from that Timeslot as indicated in the Service Header.
Timeslot	A period of time during which messages may be transmitted or received. An integer number of Minislots.
Totalcast (TC)	The transmission mode where the Destination is all the NUs in the NILE Super Network.
Track	A collated set of data associated with a track number for the purpose of representing the position and/or characteristics of a specific object, point or bearing.
Track Number Block	A defined range of consecutive track numbers assigned to an IU.
Track Quality (TQ)	A scale of numbers, which indicates a system's estimate of the accuracy of the reported position of a track.
Transmission Security (TRANSEC)	The component of INFOSEC that results from all measures designed to protect transmissions from interception, jamming, transmission detection, and traffic flow analysis.
Transmission Service Request (TSR)	A message on the DLP/SNC control & status interface used by the DLP to indicate a requirement to transmit a tactical message.
Update Rate	The frequency at which a specified category of message is to be retransmitted.

This page is intentionally left blank.

Appendix G

References

The documents referenced within this guidebook relate to the layered architecture of Link 22 as shown in [Figure G-1](#).

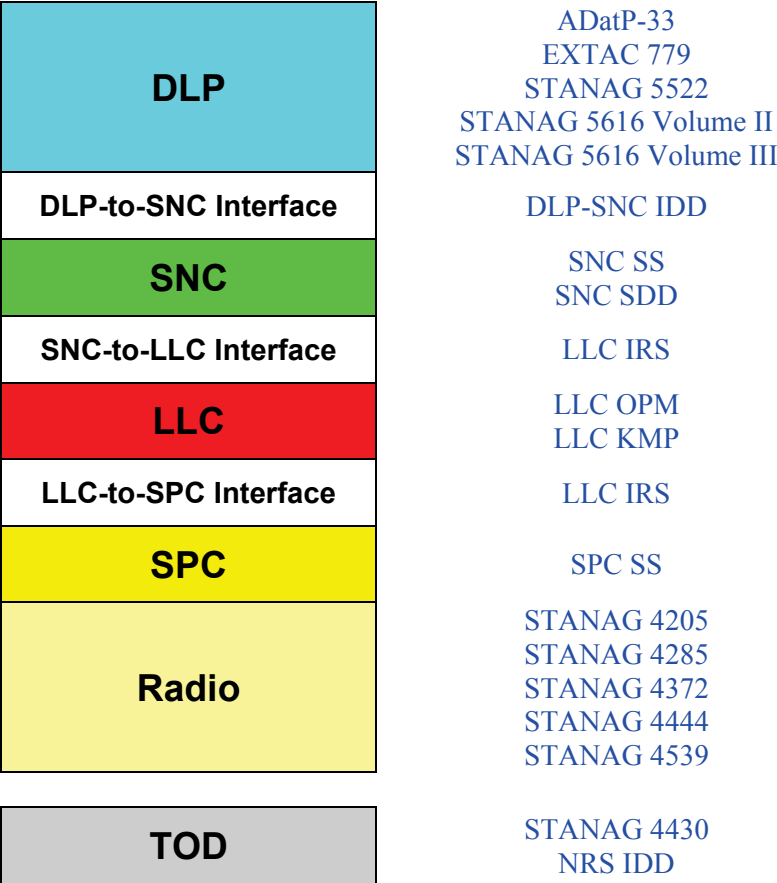


Figure G-1 Layered Architecture to Document Reference Mapping

The documents referenced within this guidebook are listed below, along with the version/edition of the document that was current at the time this version of the guidebook was produced.

ADatP-33	Multi-Link Standard Operating Procedures for Tactical Data Systems employing Link 11, Link 11B, Link 16, IJMS and Link 22 March 2008
DLP-SNC IDD	Interface Design Description for the Data Link Processing Segment and the System Network Controller for the NATO Improved Link Eleven (NILE) Program NG 278-A011-DLPIDD/B7
EXTAC 779	OPTASK LINK Message and SNC Initialization Data For LINK 22 - Working Paper for the NATO Improved Link Eleven Version 2.2.1
LLC IRS	Interface Requirement Specification (IRS) for the Link-Level COMSEC (LLC) Segment of the Link 22 (NILE) System NG 278-A011-LLCIRS/B7
LLC KCMP	Link 22 Modernized Link Level Communications Security (LLC-7M) Key and Certificate Management Plan, Version 1.5 N (NILE Version)
LLC OPM	Link Level Communication Security (LLC-7M) Installation, Configuration and Operation Instructions 007-500028-001, Rev. B
NRS IDD	Interface Design Description for the NILE Reference System for the NATO Improved Link Eleven (NILE) Program NG 278-A011-NRSIDD/B7
NRS STM	System Technical Manual for the NILE Reference System (NRS) and interfaced System Network Controller (SNC) NG 278-A011-NRSSTM/B7
SNC SDD	SNC Software Design Description for the NATO Improved Link Eleven (NILE) Program NG 278-A011-SNCSDDB7
SNC SS	Segment Specification for the System Network Controller (SNC) of the Link 22 (NILE) System NG-278-A011-SNCSS/B7
SPC SS	Segment Specification for the Signal Processing Controller (SPC) of the Link 22 (NILE) System NG 278-A011-SPCSS/B7
STANAG 4205	Technical standards for single channel UHF radio equipment Edition 3
STANAG 4285	Characteristics of 1200/2400/3600 bits per second single tone modulators / demodulators for HF radio links Edition 1
STANAG 4372	SATURN – A fast frequency hopping ECCM mode for UHF radio Edition 3

STANAG 4430	Precise Time and Frequency Interface and its Management for Military Electronic Systems Edition 1 Draft
STANAG 4444	Technical Standards for a Slow-Hop HF EPM Communications System Edition 2
STANAG 4539	Technical Standards for Non-Hopping HF Communications Waveforms Edition 1
STANAG 5522	Tactical Data Link – Link 22 Edition 4
STANAG 5616 Volume II	Standards For Data Forwarding Between Tactical Data Systems Employing Link 22 and Tactical Data Systems Employing Link 16 Edition 5
STANAG 5616 Volume III	Standards For Data Forwarding Between Tactical Data Systems Employing Link 22 and Tactical Data Systems Employing Link 11/11B Edition 5

This page is intentionally left blank.

Index

A

Access Delay

AD, 1-23, 1-25, 2-15, 2-24, 2-26, 2-27, 2-37,
2-41, 2-49, 2-51, 2-52, 2-70, 3-82, 3-89,
3-140, 3-145, 3-169, 3-180, 3-254, 3-256,
3-258, B-26, D-5
Tolerance, 2-26, 2-27, 2-37, 2-70, 3-82,
3-89, 3-140, 3-145, 3-256, D-5

Acknowledgement

ACK, 3-50, 3-169, 3-199, 3-203, 3-211, 3-213,
3-216, 3-344, 3-352

Active Join

AJ, 1-28, 3-153, 3-154, 3-155, 3-156, 3-171,
3-172, 3-174, 3-175, 3-177, 3-179, 3-180,
3-181, 3-352

Address, 2-104, 2-109, 2-110, 2-122, 3-25, 3-73,
3-78, 3-108, 3-109, 3-110, 3-113, 3-123, 3-125,
3-127, 3-150, 3-166, 3-169, 3-172, 3-180, 3-246,
3-249, 3-293, 3-294, 3-311, 3-312, 3-313, 3-314,
3-351, 3-352, 3-353, 3-354, 3-355, 3-357, 3-358,
B-2, B-5, B-21, B-22, B-24, B-26, B-28, D-7

Addressee, 2-176, 2-177, 3-200, 3-201, 3-202,
3-203, 3-208, 3-209, 3-210, 3-211, 3-212, 3-293,
3-294, 3-295, B-28

Addressing, 1-17, 1-18, 2-174, 2-175, 2-176, 3-92,
3-197, 3-234, 3-293, 3-294, B-28, 28

Dynamic List, 1-19, 2-175, 3-202, 3-234,
3-238, 3-239

Management, 2-104, 2-109, 2-110

MASN, 2-174, 2-175, 28

Neighborcast, 1-19, 2-175, 3-202, 3-234, 3-235,
3-236, 3-314

Totalcast, 1-19, 2-175, 3-121, 3-127, 3-202,
3-234, 3-241, 3-243, 3-270, 3-291, 3-293,
3-314

Adjacent Timeslot Hand-Off

ATH, 3-319, 3-320, 3-321, 3-324, 3-327, 3-328,
3-330, 3-331, 3-332

Advanced Unit Parameters, 2-40, 2-53

Air Specific Type

AST, 2-153

Air Task Order

ATO, v, 1-1, 2-179

Allied Data Publication

ADatP, 2-1, 2-30, 2-83, 2-159

Altitude/Time Indicator

ATI, 2-153

American National Standards Institute

ANSI, 3-6, 3-32

American Standard Code for Information

Interchange

ASCII, A-25

Amplification Data, 2-131

Anti-Air Warfare

AAW, 1-34, 1-36

Anti-Submarine Warfare

ASW, 2-123, 2-127, 2-128

Area of Probability

AOP, 2-127, 2-130, 2-170

Area of Responsibility

AOR, 1-34

Assignment Slot, 2-46, 2-47, 2-48, 3-260, 3-261

Automated Data Analysis Tool

ADAT, A-16, A-23, A-26

Automatic Comply Switch

ACS, 2-87, 2-88, 3-96, 3-97, 3-101, 3-103, D-8

Automatic Perform Function Switch

APFS, 2-87, 2-88, 3-96, 3-97, 3-101, 3-103,
D-8

B

Backward Compatibility, 3-343, 3-344, 3-349,
3-351, 3-358

Ballistic Missile Defense

BMD, 2-127, 2-170

Bandwidth, 1-35, 2-37, 2-42, 3-119

Calculation, 2-42

Requirement Set, 2-37

Baud Rate, 3-50, 3-229, 3-231, 3-232

Beyond Line-Of-Sight Communication

BLOS, 1-1, 1-6, 1-21, 1-36, 1-37, 2-18, 2-155,
2-158, 2-185

Bits Per Second

- BPS, 1-37
- Black Control CSCI
- BCC, B-29, B-33
- BLACK Data, 3-50
- Black Interface Processor
- BIP, B-29, B-33
- Broadcast, 2-159
- Built In Test
 - BIT, 2-147, 2-148, 3-23, 3-69, 3-70, 3-81, 3-185, 3-186, B-9, B-12, B-13, B-26, D-7
 - Failure, B-9, B-12, B-13
- Bypass Partition, 3-34, 3-35

C

- Cables and Equipment
 - Connecting, 1-39, 1-43
- Cancel Service Request
 - CSR, 3-11, 3-204, 3-207, 3-210, 3-211, 3-213, 3-215, 3-216, C-3
- Cannont Comply
 - CANTCO, 2-87, 2-89, 3-97, 3-102
- Capacity
 - Monitoring, 2-94
 - Reallocation
 - Types of, 3-318, 3-319
 - Adjacent Timeslot Hand-Off, 3-319, 3-320
 - Partial Timeslot Ownership Change, 3-319, 3-321
 - Swap Timeslots, 3-319
 - Timeslot Ownership Change, 3-319
- Capacity Need
 - CN, 1-21, 1-23, 1-25, 2-24, 2-25, 2-37, 2-41, 2-44, 2-45, 2-49, 2-52, 2-70, 2-93, 2-94, 3-59, 3-82, 3-89, 3-140, 3-145, 3-169, 3-180, 3-254, 3-256, 3-257, 3-330, B-26, D-5
- Channel Utilization, 2-79, 2-80, 3-15, 3-193, C-8
- Classified Number
 - CN, 1-21, 2-41, 2-44, 2-45, 3-59, 3-256, 3-257
- Command and Control
 - C², ¹⁻¹⁶, 2-134, 2-148, 2-155, 2-165, 2-169, 2-171, 2-173, 2-174
- Commercial off the Shelf
 - COTS, vii, 1-33, A-3, A-8
- Communication Service Message

- CSM, 3-295, 3-296, 3-297, 3-298, 3-299, 3-300, 3-305, 3-306, 3-310, 3-315, 3-316, 3-317
- Communications Security
 - COMSEC, vii, 1-2, 1-15, 3-63, A-4, B-11
- Communications Transport
 - CT, 1-22, 2-10, 2-80, 3-7, 3-18, 3-19, 3-20, 3-25, 3-91, 3-256, B-17
- Compatibility, vii, 3-71
- Complementary Link Reception Quality
 - CLRQ, 2-54, 2-55, 2-58, 3-266, 3-267, 3-268, 3-269, 3-270, 3-271, 3-277, 3-278, 3-279, 3-281
- Complimentary Quality of Link
 - CQOL, 2-112, 2-113
- Configuration/Initialization/Status
 - CIS, C-5, C-6, C-7, C-8, C-10
- Congestion, 1-9, 1-13, 1-31, 2-79, 2-80, 2-93, 2-94, 3-15, 3-18, 3-23, 3-193, 3-197, 3-280, 3-286, 3-287, 3-288, 3-289, 3-290, 3-291, 3-326, 3-329, 3-343, 3-351, 3-358, C-8
 - Alert, 3-15, 3-193, 3-290, C-8
 - Automated Management, 1-9
 - Calculation, 3-286
 - Congestion Value
 - CV, 2-80, 3-274, 3-286, 3-287, 3-288, 3-289, 3-290, 3-291, 3-329
 - Distribution, 3-286, 3-289
 - Management, 1-9, 1-13, 1-31
 - Technical message, 3-193, 3-290, 3-291, 3-343, 3-358
- Congestion Assessment Management
 - CAM, 3-18, 3-23, 28
- Connectivity, 2-40, 2-41, 2-79, 2-80, 2-85, 2-93, 2-112, 2-179, 2-186, 3-15, 3-85, 3-87, 3-89, 3-131, 3-193, 3-262, 3-263, 3-273, 3-295, C-8, C-10
 - CONN, C-6, C-10
 - Monitoring, 2-93
- Control and Status
 - C&S, 2-17, 2-23, 3-6, 3-7, 3-12, 3-14, 3-62, 3-64, 3-71, 3-105, 3-130, B-25, B-28, C-2, C-4, C-6, C-8, C-9
- Control and Status Interface, 2-17, 2-23, 3-6, 3-7, 3-12, 3-62, C-2, C-4, C-6, C-9, 28
- Correlation, 2-124, 2-132, 2-161, 2-163, 2-164, 2-168, 2-172, 2-173
- Course and Speed

- CAS, 2-43, 2-123, 2-124, 2-126, 2-128, 2-149, 2-151, 2-153, 2-169
- Crypto Variable Logical Label
 - CVLL, 2-18, 2-35, B-6
- Cryptographic
 - Data Set
 - Link 22, 2-35
 - Requirements, 2-179, B-2, B-6, D-8
- Cryptographic Unit
 - Crypto, 1-2, 1-15, 1-27, 1-35, 2-4, 2-6, 2-7, 2-16, 2-17, 2-18, 2-64, 2-65, 2-84, 2-86, 2-104, 2-106, 3-33, 3-34, 3-35, 3-37, 3-38, 3-45, 3-46, 3-47, 3-52, 3-53, 3-54, 3-157, 3-159, 3-233, 3-338, 3-341, B-1, B-6, B-7, B-15, B-48, D-7, D-8
- Cyclic Redundancy Check
 - CRC, B-53

D

- Data
 - Extrapolation, 2-174, 2-176
 - Filters, 2-164, 2-171, 2-172
 - Forwarding, 2-29, 2-30, 2-53, 2-56, 2-160, 2-161, 2-162, 2-163, 2-179, 3-254
 - Partition, 3-34, 3-36, 3-52
 - Registration, 2-164, 2-172, 2-173
 - Transfer Rate Comparison, 1-37
- Data Analysis
 - DA, A-3, A-11, A-14, A-23
- Data Communication Equipment
 - DCE, 3-51
- Data Element, 2-122, 2-145, C-12, C-16, C-17
- Data Extraction
 - DX, A-3, A-13, A-14, A-26
- Data Field Identifier, 2-121, 2-144, 3-347
 - DFI, 2-121, 2-144, 2-147, 2-148, 3-346, 3-347, 3-348, 3-349, 3-350, B-53
- Data Forwarding, 2-29, 2-30, 2-53, 2-56, 2-160, 2-161, 2-162, 2-163, 2-179, 3-254
- Data Link, 1-14, 1-34, 1-39, 2-2, 2-3, 2-171, 3-3, A-15, A-25
- Data Link Processor
 - DLP, 1-14, 1-39, 2-2, 2-3, 3-3, A-15, 28
 - DLP-SNC Minimum Implementation, C-1

- NU Performance Data, 3-13, 3-193, 3-195
- Optimization, 3-262, 3-283
- Recovery, B-19, B-20
- Request Management Info, 3-10, 3-13, 3-67, 3-130, 3-131, 3-132, 3-133, 3-134, 3-135, 3-136, C-5
- C&S Messages, 3-130, 3-136
- Congestion Indexes, 3-130, 3-135
- Connectivity Data, 3-130, 3-131
- Directory Update, 3-130, 3-133
- Link Participants, 3-130, 3-132
- List of Queued Messages, 3-130, 3-134
- Media Parameters, 3-130, 3-132
- Network Information, 3-130
- NU Capabilities, 3-130, 3-135
- TSR Management, 3-11, 3-197, 3-207
- MR Addressee, 3-207, 3-211, 3-212
- Non-MR Addressee Only, 3-207, 3-208
- SRID Management Function, 3-200, 3-207, 3-216
- Transmission Timeout, 3-207, 3-214, 3-216
- Expired TSR Resolution, 3-214, 3-215
- TSR Expiration, 3-214, 3-215
- TSR Lifetime, 3-214
- Data Link Reference Point
 - DLRP, 1-34
- Data Link Server, A-25
- Data Originator, 1-17, 1-18, 3-307, 3-313
- Data Reduction
 - DR, A-11, A-14, A-23, A-26
- Data Terminal Device
 - DTD, 1-40, 2-4, 3-46
- Data Termination Equipment
 - DTE, 3-51
- Data Unit
 - DU, 2-35, 3-221, 3-222, 3-223, 3-224, 3-244, 3-305, 3-306, 3-310, 3-311, B-6
- Data Unit Configuration Code
 - DUCC, 3-310, 3-311
- Data Update Request
 - DUR, 2-124, 2-132, 2-141, 2-150, 2-151, 2-177
- Data Use Identifier

DUI, 2-121, 2-144, 2-147, 2-148, 3-346, 3-347,
 3-348, 3-349, 3-350, B-53
 Day of Week
 DOW, 2-7, 2-17, 2-64, 2-66, 2-72, 2-86, 3-46,
 3-47, 3-48, 3-49, 3-69, 3-72, 3-74, 3-156,
 3-157, 3-159, 3-233, B-7, B-8, B-15, B-21,
 B-48, B-51, B-52, B-56, D-2, 28
 Decryption
 DECR, 3-48, 3-225, 3-232, 3-233
 Delay, 1-23, 2-26, 2-27, 2-37, 2-52, 3-259, 3-331
 Destination
 Dest, 3-92, 3-97, 3-113, 3-127
 Direct Link Reception Quality
 DLRQ, 3-262, 3-263, 3-264, 3-266
 Directory
 DIR, C-5, C-6, C-7, C-8, C-10
 Maintenance, 3-343, 3-344, 3-345, 3-351,
 3-355, 3-356, C-10
 Distributed Interactive Simulation
 DIS, A-24
 Distributed Protocols, 1-7
 DLP Interface
 DIF, 3-18, 3-19, 3-20, 3-21, 3-24, 3-30
 DLP Interface Reception
 DRX, 3-18, 3-30
 DLP Interface Transmission
 DTX, 3-18, 3-30
 DLP-SNC Interface, xiii, 3-2, 3-6, 3-7, 3-8, 3-69,
 3-70, 3-207, A-16
 Minimum Implementation, C-1
 Donor Processing, 3-318, 3-329
 Duplicate Detection, 3-20, 3-21, 3-197, 3-244,
 3-245, 3-246
 Dynamic List, 1-19, 2-175, 3-202, 3-234, 3-238,
 3-239
 Address, 3-238
 Dynamic TDMA
 DTDMA, 1-9, 1-22, 1-31, 2-6, 2-9, 2-16, 2-23,
 2-31, 2-33, 2-40, 2-48, 2-79, 2-81, 2-88,
 2-95, 2-97, 2-186, 3-13, 3-14, 3-15, 3-23,
 3-24, 3-79, 3-88, 3-93, 3-98, 3-104, 3-137,
 3-138, 3-139, 3-140, 3-144, 3-174, 3-193,
 3-197, 3-254, 3-257, 3-286, 3-287, 3-302,
 3-318, 3-319, 3-321, 3-323, 3-324, 3-325,
 3-326, 3-328, 3-329, 3-332, 3-334, 3-344,
 3-345, 3-351, 3-353, 3-354, B-14, B-26, C-4,
 C-5, C-7, C-8, C-10, D-5

Change, 3-13, 3-14, 3-98, 3-104, 3-137,
 3-138, C-5, C-7
 Changing the Network DTDMA flag,
 2-98
 Parameters, 3-318, 3-334
 Participation, 2-79, 2-81, 3-15, 3-193, C-8

E

Electronic Counter Measures
 ECM, 3-64
 Electronic Protective Measures
 EPM, 2-4, 2-5, 2-8, 2-15, 2-18, 2-19, 2-20, 2-27,
 2-36, 2-44, 2-45, 2-46, 2-47, 2-48, 2-66,
 2-97, 3-4, 3-56, 3-57, 3-59, 3-60, 3-64, 3-65,
 3-142, 3-157, 3-159, 3-160, 3-161, 3-162,
 3-254, 3-256, 3-260, 3-261, B-12, B-54,
 B-55, D-5, D-6
 Electronic Warfare
 EW, 2-124, 2-127, 2-129, 2-130, 2-164, 2-167,
 2-169, 2-170, 2-179, B-54, C-13, C-14
 Emission Control
 EMCON, 2-77
 Encryption
 ENCR, 2-35, 3-33, 3-46, 3-225, 3-232, 3-233,
 B-6
 External, 2-174, 2-176
 End of Text
 ETX, 3-34
 End To End Reference Number
 E2ERN, 3-246, 3-247, 3-248, 3-249, 3-297,
 3-299, 3-311
 Error Detection and Correction
 EDAC, 1-37, 3-57, 3-85, 3-159, 3-162, 3-348,
 B-17
 Error Rate, 2-79, 2-80, 3-15, 3-193, B-1, B-17,
 B-18, C-8
 Characteristics, 3-15, 3-193, B-1, B-17, B-18,
 C-8
 Explicit Source Identification
 ESI, 3-164, 3-165, 3-166, 3-176, 3-233, 3-302,
 3-325, 3-329, 3-332, 3-333, 3-334, 3-351,
 3-352, 3-353, 3-354, 3-355, 3-357, 3-358

F

Fault Management

FAM, 2-76, 2-79, 2-83, 3-18, 3-23, B-1, B-9, 28

Fixed Frequency

FF, 2-4, 2-8, 2-14, 2-15, 2-18, 2-19, 2-20, 2-22, 2-31, 2-32, 2-33, 2-44, 2-45, 2-47, 2-48, 2-49, 2-51, 2-64, 2-88, 3-4, 3-55, 3-56, 3-57, 3-59, 3-60, 3-65, 3-93, 3-98, 3-142, 3-157, 3-229, 3-254, 3-258, 3-260, 3-261, B-51, B-52, D-5, D-6

FJ-Series

Message, 2-141, C-15

Message Sequence, 2-135, 2-141

Flooding, 3-91, 3-274, 3-275

Flow Control/Metering protocol

FLOW, C-3, C-5, C-7, C-10

Forwarding Link 16 MIDS Unit

FJU, 2-160, 2-173, 2-183

Forwarding Link 16 MIDS Unit to Link 22

FJUN, C-15

Forwarding NILE Unit

FNU, 2-28, 2-160, 2-173, C-2

to/from TDL A (Link 11)

FNUA, 2-28

to/from TDL A and B

FNUAB, 2-28

to/from TDL B (Link 11B)

FNUB, 2-28

Forwarding Participating Unit

FPU, 2-160

Forwarding Reporting Unit

FRU, 2-160

Frequency Hop Set

FHS, D-5, D-6

Frequency Hopping, 1-21, 2-5

Friendly Platform Status, 2-164, 2-167

Friendly Weapon Danger Area

FWDA, 2-169

F-Series Messages, 1-16, 2-121, 2-122, 2-123,

2-124, 2-135, 2-136, 2-137, 2-141, 2-142, 2-143,

2-145, 2-177, C-15, C-16

Catalog, 2-122, 2-123

F Message Sequence, 2-135, 2-142

Unique F-Series Message Words, 2-136

Function Management Switches, 3-70, 3-92, 3-95, 3-96

Functional Interface, 3-6, 3-7, 3-33, 3-45, 3-52

G

Geodetic Positioning, 2-164, 2-167, 2-168

Global Data and Initialization

GDI, 3-18, 3-26, 3-28, 28

Global Positioning System

GPS, 1-42, 2-173, 2-174

Granularity of Measurement, 2-164, 2-167

Gridlock Reference Unit

GRU, 2-173

Guaranteed Delivery

GD, 1-18, 3-20, 3-201, 3-202, 3-211, 3-213,

3-215, 3-216, 3-234, 3-277, 3-292, 3-293,

3-294, 3-295, 3-296, 3-299, 3-300, 3-316,

3-317, 3-352, 3-353, 3-354, 3-355

Guard Time, 2-50, 3-348

H

Header, 3-9, 3-33, 3-34, 3-37, 3-53, 3-61, 3-228,

3-229, 3-230, 3-231, 3-234, 3-235, 3-236, 3-237,

3-301, 3-302, 3-305, 3-306, 3-307, 3-309, 3-310,

3-311, 3-312, 3-315, 3-340, 3-341

High Frequency

HF, 1-6, 1-21, 2-159, 3-56, 3-65, B-55

High Reliability

HR, 1-18, 3-201, 3-277, 3-278, 3-279, 3-292,

3-293, 3-295, 3-297, 3-352, 3-354, 3-356,

3-357, 3-358

High Update Rate

HUR, 2-26, 2-151, 2-174, 2-175

Host System, 1-14, 2-3

Human Machine Interface

HMI, 2-4, 3-3, 3-18, 3-23, 3-25, 3-55, 3-58,

A-25, B-21, 28

I

Identifier

- ID, 2-34, 2-35, 2-53, 2-124, 2-132, 3-34, 3-306, 3-335, 3-336, B-3, B-4
- IDENT, 2-34, 2-35, 2-53, 2-124, 2-132, 3-34, 3-306, 3-335, 3-336, B-3, B-4
- Identity
 - ID, 2-142, 2-143, 2-166
- Inactive Join
- IJ, 1-28, 3-153, 3-154, 3-155, 3-156, 3-162, 3-164, 3-165, 3-166, 3-167, 3-168, 3-169, 3-170, 3-171, 3-172, 3-173, 3-175, 3-176, 3-177, 3-178, 3-180, 3-181, 3-182, 3-233, 3-352
- Indicator
 - IND, 1-17, 1-18, 2-78, 2-123, 2-135, 2-136, 2-137, 2-138, 2-143, 2-147, 2-150, 2-153, 2-177, 3-41, 3-42, 3-121, 3-217, C-16
- Information Management, 2-132, C-13
- Information Set, 2-35
- Infrastructure
 - INF, 3-18, 3-19, 3-22, 3-26, 3-30
- Initialization, 3-354
- Initialization
 - INIT, xiii, 1-24, 1-25, 1-32, 2-6, 2-9, 2-16, 2-21, 2-32, 2-43, 2-63, 2-64, 2-67, 2-83, 2-89, 2-108, 3-13, 3-18, 3-23, 3-28, 3-59, 3-75, 3-77, 3-79, 3-80, 3-81, 3-97, 3-104, 3-147, 3-149, 3-153, 3-155, 3-181, 3-254, 3-335, 3-336, 3-337, 3-343, 3-344, 3-345, 3-351, 3-354
 - Hardware, 2-64, 2-65
 - Crypto Management, 2-65
 - SPC and Radio Management, 2-66
 - LNE and Configuration Management
 - ILM, 3-18, 3-23, 3-24
 - Network, 1-24, 1-25, 2-64, 2-67, 2-69, 2-72, 3-14, 3-67, 3-79, 3-80, 3-81, 3-83, 3-147, 3-149, 3-176, 3-177, 3-181
 - New Network, 2-84, 2-89, 2-90, 3-137, 3-147, 3-149
 - System, 2-64, 2-67
 - with Probing
 - IPROB, 1-25
- Initialization
 - INIT, 3-354
- Initialization, 3-354
- Initialization
 - INIT, 3-354
- Initialization
 - INIT, 3-354
- Initialization
 - INIT, B-23
- Initialization
 - INIT, B-47
- Initialization
 - INIT
 - Network, C-5
- Initialization
 - INIT
 - with Probing
 - IPROB, C-5
- Initialization
 - INIT
 - Network, C-5
- Initialization
 - INIT
 - with Probing
 - IPROB, C-5
- Initialization
 - INIT
 - with Probing
 - IPROB, C-5
- Initialization
 - INIT
 - Network, C-5
- Initialization
 - INIT, C-6
- Initialization
 - INIT
 - with Probing
 - IPROB, C-7
- Initialization
 - INIT
 - with Probing
 - IPROB, C-7
- Initialization
 - INIT
 - with Probing
 - IPROB, C-7
- Initialization
 - INIT

K

Key Management, 1-15, 2-17, 2-84, 2-86, 2-88,
2-104, 2-106, 3-37, 3-38, 3-46, 3-47, 3-94, 3-98,
3-335, 3-338, 3-357, B-6, B-7, D-8
Key Loading, 2-106, 2-107, 2-119
Key Rollover, 2-119, B-1, B-27, B-48
Key Zeroize, 2-86, 2-106, 2-107, 2-119

L

Land Points and Tracks, 2-164, 2-170
Late Network Entry
 LNE, 1-10, 1-25, 1-28, 2-53, 2-56, 2-67, 2-72,
 2-73, 2-74, 2-119, 3-67, 3-153, 3-344, 3-351,
 3-352, A-4, B-24, B-55
 Access Denied, 2-75
 Access Granted, 2-75, 3-172, 3-180
 Access Granted on Alternate Network,
 3-172, 3-180
 Add LNE unit to MASN, 2-110
 Add LNE unit to the Super Network,
 2-110
 Capacity Allocation, 3-175, 3-181
 Completion of, 3-176
 Failure, 2-74, 3-14, 3-159, 3-162, 3-172,
 3-177, 3-183, C-7
 Media Parameter Acquisition, 3-155,
 3-156, 3-157, 3-158, 3-159, 3-160, 3-161,
 3-162, 3-163, 3-165, 3-178, 3-183
 Network Information, 3-174
 ONCS Deduction, 3-164, 3-183
 Ordered, 2-110, 2-111
 Permission to Join from the SNMU,
 3-171
 Request Network Parameters, 2-74
 Slot, 2-56, 2-88, 2-100, 2-101, 3-13, 3-93,
 3-97, 3-98, 3-104, 3-155, 3-165, 3-166,
 3-167, 3-169, 3-183, 3-233, C-6
 Status, 2-74, 3-14, 3-162, 3-166, 3-172,
 3-173, 3-175, 3-177, 3-181, B-26, C-7
 Support, 2-92, 2-100, 2-104, 2-110
 Transmission Capacity Request,
 2-102, 3-14, 3-172, 3-176, C-7

Supporting Unit, 2-73, 3-124, 3-129, 3-153,
3-155, 3-167, 3-168, 3-183

Latitude/Longitude Scale

 LLS, 2-147, 2-150, 2-177

Least Significant Bit(s)

 LSB, 2-135, 2-145, 2-147, 3-36

Leg

 Acknowledged Delivery

 LAD, 3-295, 3-296, 3-297, 3-299

 Injection Packet, 3-20

 Message Packet Reference Number

 Leg MPRN, 3-296, 3-299, 3-313, 3-317

 Reliability, 3-278

Line Of Bearing

 LOB, 2-167, 2-170

Line-Of-Sight

 LOS, 1-1, 1-6, 1-36, 2-181, 2-184

Link 11, v, vii, viii, 1-2, 1-7, 1-26, 1-33, 1-34,
1-35, 1-37, 1-41, 2-4, 2-19, 2-28, 2-29, 2-33,
2-56, 2-121, 2-122, 2-125, 2-155, 2-156, 2-157,
2-159, 2-160, 2-161, 2-163, 2-164, 2-165, 2-166,
2-167, 2-168, 2-169, 2-170, 2-171, 2-172, 2-173,
2-174, 2-176, 2-177, 2-178, 2-180, 2-181, 2-182,
2-183, 2-184, 2-186, 3-65, A-15, B-54, B-55

 Comparison with, 1-34, 2-179, 2-183, 2-184

Link 11B, 2-28, 2-29, 2-125, 2-155, 2-157, 2-159,
2-160, 2-164, 2-165, 2-169, 2-172

Link 16, v, vii, viii, 1-2, 1-3, 1-15, 1-16, 1-26,
1-33, 1-34, 1-35, 1-36, 1-37, 2-11, 2-13, 2-19,
2-28, 2-29, 2-33, 2-35, 2-121, 2-122, 2-135,
2-141, 2-142, 2-155, 2-156, 2-157, 2-158, 2-159,
2-160, 2-161, 2-163, 2-164, 2-165, 2-166, 2-167,
2-168, 2-170, 2-171, 2-172, 2-173, 2-174, 2-176,
2-177, 2-178, 2-180, 2-181, 2-182, 2-183, 2-184,
2-185, 2-186, 2-187, 3-111, A-15, A-24, B-6,
B-53, B-54, B-55, B-56, C-15

 Comparison with, 1-36, 2-179, 2-180, 2-183,
 2-184

 Unique Features, 2-164, 2-173

 Air Control, 2-173, 2-174, 2-181, B-54

Link 22

 Address, 2-6, 2-11, 2-16, 2-27, 2-34, 2-36, 2-38,
 2-53, 2-64, 2-109, 3-25, 3-69, 3-76, 3-78,
 3-83, 3-89, 3-97, 3-108, 3-109, 3-110, 3-139,
 3-144, 3-146, 3-194, 3-313, B-2, B-3, B-25,
 B-27, D-2, D-3, D-5, D-7

- Comparison with, 1-36, 2-179, 2-180, 2-183, 2-184
- Interconnecting with Link 16, 2-179, 2-185
- Multilink Planning, 2-156, 2-178
- Super Network Information Set, 2-34
- Unique Features, 2-164, 2-174
 - Addressing, 2-174, 2-175
 - Data Extrapolation, 2-174, 2-176
 - Data Forwarding, 2-174, 2-175
 - External Encryption, 2-174, 2-176
 - High Update Rate (HUR), 2-26, 2-174
 - Machine Receipt, 2-174, 2-176, 2-177, 3-20, 3-201, 3-207, 3-234, 3-294, 3-295, 3-297, 3-311, 3-315
 - MASN, 2-174, 2-175
 - Slow Update Rate Protocol (SLURP), 2-174, 2-175
 - Transmission Assurance, 2-174, 2-177
- Link Connectivity Data
 - LCD, 2-80, 2-85, 3-15, 3-131, 3-193, 3-262, 3-271, 3-272, 3-273, 3-274, C-8
- Link Level COMSEC
 - LLC, 1-14, 1-39, 1-40, 2-2, 2-4, 28
 - Alarm, B-9, B-11
 - Configuration Failure, 3-15, B-9, B-10, B-15, B-24, C-9
 - Configuration Request, 3-37, 3-46, 3-50, 3-185, 3-335, 3-338
 - Crypto Time-of-Day, 3-47, B-48
 - Day of Week, 2-7, 2-17, 2-66, 2-72, 2-86, 3-47, 3-48, 3-49, 3-69, 3-72, 3-74, 3-156, 3-157, B-7, B-8, B-15, B-21, B-48, B-51, B-52, B-56, 28
 - Disabled, 3-15, B-9, B-15, B-24, C-9
 - Errors, B-9, B-11
 - Information Flow, 3-45
 - LLC Simulator, A-3, A-4, A-16
 - Recovery, B-9, B-10, B-11, B-12, B-15, B-16, B-18
 - Status Request, 3-13, 3-37, 3-189, 3-335, 3-337, B-10, C-6
 - Time of Week, 3-47, 3-48, 3-49, B-51, B-52, B-56
- Link Quality, 2-119, 3-13, 3-87, 3-121, 3-283, 3-284, 3-285, B-26, C-6
- Link Reception Quality

- LRQ, 2-54, 2-55, 2-58, 2-80, 2-85, 3-15, 3-86, 3-131, 3-193, 3-262, 3-263, 3-264, 3-265, 3-266, 3-267, 3-268, 3-269, 3-270, 3-271, 3-272, 3-273, 3-274, 3-285, 3-327, 3-344, 3-353, C-8
 - Computation, 3-266
 - Quality, 3-266, 3-269
 - Status, 2-119, 3-13, 3-121, 3-283, 3-284, 3-285, C-6
 - Technical Message Quality, 3-266, 3-268
- Live Link, A-17, A-19
- LLC Simulator, A-3, A-4, A-16
- Local Area Network
 - LAN, 3-6, 3-8, 3-13, 3-32, 3-34, 3-149, 3-155, 3-156, 3-336, A-5, B-23, B-24, C-5
- Low Battery
 - LO BATT, 3-40
- Lowest Allocatable NILE Address
 - LANA, 3-109, 3-110, D-2
- Low-Volume Terminal
 - LVT, 2-158

M

- Machine Receipt
 - Address Group, 3-294
 - MR, 2-174, 2-176, 2-177, 3-20, 3-201, 3-202, 3-203, 3-207, 3-208, 3-211, 3-212, 3-213, 3-214, 3-215, 3-216, 3-234, 3-235, 3-236, 3-237, 3-248, 3-293, 3-294, 3-295, 3-296, 3-297, 3-298, 3-299, 3-307, 3-311, 3-314, 3-315
- Major Version Number, 3-71
- Management Function
 - MF, 3-7, 3-18, 3-19, 3-20, 3-21, 3-22, 3-23, D-8
- Maximum Perishability, 3-246
- Media
 - Fragmentation Rate, 1-21, 2-6, 2-8, 2-16, 2-20, 2-46, 2-48, 2-50, 2-72, 2-85, 2-97, 3-60, 3-79, 3-81, 3-84, 3-137, 3-142, 3-155, 3-157, 3-159, 3-160, 3-183, 3-254, B-26, D-5
 - Frequency, vii, 1-21, 1-41, 2-4, 2-5, 2-6, 2-8, 2-15, 2-16, 2-18, 2-19, 2-20, 2-69, 2-85, 2-97, 2-123, 2-128, 2-178, 2-180, 2-181, 3-56, 3-62, 3-64, 3-65, 3-79, 3-80, 3-81,

- 3-85, 3-137, 3-142, 3-144, 3-146, 3-157,
3-159, 3-162, B-4, B-26, B-49, D-5
- HF EPM SPC, 3-63
- HF FF SPC, 3-63
- Interface Congestion, 3-15, B-9, B-12, C-9
- Media Setting Number
 - MSN, 2-6, 2-8, 2-16, 2-18, 2-19, 2-69, 2-72,
2-85, 2-97, 2-99, 3-79, 3-81, 3-83, 3-137,
3-155, 3-157, 3-159, 3-160, 3-254, B-26,
B-56, D-5
- Media Simulator
 - MS, A-3, A-4, A-5, A-6, A-7, A-9, A-10,
A-16, A-19, A-20
- Parameter
 - Change on Network, 2-99
- Parameter Settings Set, 2-36
- UHF EPM SPC, 3-64
- UHF FF SPC, 3-55, 3-63
- Media Coding Frame
 - MCF, 1-21, 3-48, 3-57, 3-58, 3-59, 3-60, 3-81,
3-159, 3-162, 3-232, 3-233, B-51, B-52
- Media Control and Management
 - MCM, 3-18, 3-30
- Media Interface
 - MIF, 3-15, 3-18, 3-19, 3-20, 3-23, 3-24, 3-30,
B-9, B-12, C-9
- Media Parameter Acquisition
 - MPA, 3-155, 3-156, 3-157, 3-158, 3-159, 3-160,
3-161, 3-162, 3-163, 3-165, 3-178, 3-183
- Media Reception
 - MRX, 3-18, 3-30
- Media Setting Number
 - MSN, 2-6, 2-8, 2-16, 2-18, 2-19, 2-21, 2-44,
2-45, 2-46, 2-47, 2-48, 2-69, 2-72, 2-85,
2-97, 2-99, 3-60, 3-79, 3-80, 3-81, 3-83,
3-84, 3-85, 3-86, 3-87, 3-137, 3-142, 3-144,
3-146, 3-155, 3-157, 3-159, 3-160, 3-183,
3-254, 3-256, 3-260, 3-261, 3-348, B-26,
B-56, D-5, D-6
- Media Simulator
 - MS, A-3, A-4, A-5, A-6, A-7, A-8, A-9, A-10,
A-16, A-17, A-19, A-20
- Media Transmission
 - MTX, 3-18, 3-30
- Memorandum of Understanding
 - MOU, vi, 1-2

- Message
 - Definition, 3-6, 3-8, 3-33, 3-53
 - Delivery, 3-19, 3-197, 3-234, 3-292, 3-293,
3-294, 3-295, 3-307, 3-310
 - Message Packet, 3-18, 3-20, 3-21, 3-24, 3-220,
3-244, 3-245, 3-246, 3-249, 3-250, 3-251,
3-252, 3-278, 3-301, 3-303, 3-305, 3-306,
3-312, B-27
 - Preparation Request, 3-11, 3-199, 3-202,
3-207, 3-208, 3-211, 3-227, C-3
 - MPR, 3-11, 3-199, 3-202, 3-207, 3-208,
3-211, 3-227, C-3
 - Preparation Time
 - MPT, 3-13, 3-69, 3-70, 3-71, 3-72, 3-74,
3-95, 3-203, 3-206, 3-227, 3-228, B-12,
B-24, B-26, C-2, C-5, D-7
 - Relay, 3-262, 3-282
 - Reliability, 3-197, 3-234, 3-292
 - Guaranteed Delivery, 1-18, 3-20, 3-201,
3-202, 3-234, 3-277, 3-292, 3-293, 3-295,
3-296, 3-299, 3-316, 3-317
 - High Reliability, 3-293
 - Standard Reliability, 3-293
 - Source, 3-20, 3-329
 - Time of Validity
 - MTV, 2-81, 2-82, 3-198, 3-202, 3-203,
3-221, 3-224, 3-226, 3-228, 3-244, 3-246,
3-247, 3-249, 3-297, 3-311, 3-312, B-25
- Message Packet
 - MP, 3-18, 3-20, 3-21, 3-24, 3-220, 3-221, 3-222,
3-223, 3-224, 3-244, 3-245, 3-246, 3-247,
3-248, 3-249, 3-250, 3-251, 3-252, 3-253,
3-278, 3-279, 3-281, 3-301, 3-302, 3-303,
3-304, 3-305, 3-306, 3-307, 3-310, 3-312,
3-313, 3-315, 3-316, 3-317, B-27, 28
 - Expansion
 - MPE, 3-18, 3-20, 3-21, 28
 - Reference Number
 - MPRN, 3-296, 3-313, 3-317
 - Store, 3-21, 3-244, 3-245
 - to Network Packet ratio
 - MP/NP, 3-278, 3-279, 3-281
- Military Standard
 - MIL-STD, 2-158
- Minimum Implementation

- MIN IMP, ix, 2-17, 2-23, C-1, C-3, C-5, C-6, C-9, C-11, C-12, C-13, C-14, C-15, C-16, C-17, 28
- Minislot, 2-45, 2-46, 2-50
- Ministry of Defense
 - MOD, 3-124
- Minor Version Number, 3-71
- Mission Area Subnetwork
 - MASN
 - Add LNE Unit, 2-110
 - Create, 2-105, 2-106, 3-13, 3-76, 3-78, 3-104, 3-112, 3-113, C-5, D-3
 - Delete, 2-105, 2-106, 3-13, 3-104, 3-112, C-5
 - Management, 2-104, 2-105
 - MASN Set, 2-57
 - Modify, 2-105, 2-106, 3-13, 3-104, 3-112, C-5
- Mission Requirements, 2-40, 2-53
- MLSD, A-23, A-24
- MLST3 Single, A-18, A-22
- Modulation and Demodulation
 - MODEM, 3-57
- Monitor Statistics, 2-76, 2-79
- Most Significant Bit(s)
 - MSB, 2-177
- MS Standalone, A-10
- Multifunctional Information Distribution
 - Systems
 - MIDS, 2-155, 2-158, 2-163, 2-173, 2-174, 2-176, 2-177, 2-181
- Multi-Link Data Analysis
 - MLDA, A-25
- Multilink Environment, 2-156, 2-157
 - Considerations, 2-156, 2-164
 - Data Reduction
 - MLDR, A-23
 - Multilink Terms, 2-157, 2-160
- Scenario Developer
 - MLSD, A-23, A-24
- Scenario Generator
 - MLSG, A-25
- Multiple Link System Test & Training Tool
 - MLST3, vii, viii, 1-11, A-1, A-2, A-4, A-5, A-15, A-16, A-17, A-18, A-19, A-20, A-21, A-22, A-23, A-24, A-25, A-26, B-53

- Components, A-15, A-16
- Configuration, A-15, A-17
- MLST3 Programs, A-15, A-23
 - Single, A-18, A-22
- Multiple Link Test System
 - MLTS, A-23, A-25
- Multiple Units, A-4, A-6, A-7, A-17, A-18, A-19
- Multiple Units Under Test, A-4, A-6, A-7
 - MUUT, A-4, A-6, A-7, A-8

N

- National Security Agency
 - NSA, 1-2
- NATO Improved Link Eleven
 - NILE, v, 1-2
- NATO Link 1, 2-157, 2-159
- NCE Simulation, A-17, A-21
- NCS Changes
 - NCSC, C-7, C-10
- NCS Handler
 - NCH, 3-18, 3-23, 3-24, 28
- Negative Acknowledgement
 - NACK, 3-50
- Neighborcast, 1-19, 2-175, 3-202, 3-234, 3-235, 3-236, 3-314
- Net Control Station
 - NCS, 1-34, 1-35, 2-159
- Network
 - Closedown, 3-184, 3-186, 3-189
 - Connectivity, 1-36, 2-41, 3-83, 3-271, 3-273
 - Cryptographic Resource Description Set, 2-38
 - Join, 1-13, 1-28
 - Monitoring Management
 - NMM, 3-18, 3-23, 3-24, 28
 - Termination, 2-116, 2-117, 2-119
- Network Cycle, 1-13, 1-22, 2-6, 2-10, 2-16, 2-23, 2-51, 2-72, 2-80, 2-81, 3-23, 3-25, 3-59, 3-82, 3-91, 3-137, 3-165, 3-197, 3-225, 3-254, 3-281, B-17
 - Access Delay, 1-23, 1-25, 2-15, 2-24, 2-26, 2-27, 2-37, 2-41, 2-49, 2-51, 2-52, 2-70, 3-82, 3-89, 3-140, 3-145, 3-169, 3-180, 3-254, 3-256, 3-258, B-26, D-5

- Access Delay Tolerance, 2-26, 2-27, 2-37, 2-70, 3-82, 3-89, 3-140, 3-145, 3-256, D-5
- Capacity Need, 1-23, 1-25, 2-24, 2-25, 2-37, 2-41, 2-49, 2-52, 2-70, 2-93, 2-94, 3-82, 3-89, 3-140, 3-145, 3-169, 3-180, 3-254, 3-330, B-26, D-5
- DTDMA, 1-9, 1-22, 1-31, 2-23, 2-33, 3-197, 3-318, 3-344, 3-351, 3-353, B-26, D-5
- Planner Defined NCS, 2-23, 2-70, 2-98
- SNC Defined NCS, 2-23, 2-24, 2-69, 2-70, 2-98
- Structure
 - NCS, 1-13, 1-22, 2-6, 2-10, 2-16, 2-23, 3-23, 3-25, 3-59, 3-82, 3-137, 3-197, 3-225, 3-254, 28
 - Computation, 3-254, 3-255, B-27
 - Exit Criteria, 3-259
 - First Net Cycle Time, 3-256
 - Metrics, 3-259
 - Priority Injection, 3-258
 - Timeslot, 3-256
 - Timeslot Placement, 3-258
 - Constraints, 3-254, 3-260
 - Handling, 3-82, 3-197, 3-225, 3-254
- Time
 - NCT, 1-22, 2-10, 2-51, 2-72, 2-80, 2-81, 3-91, 3-165, 3-281, B-17
- Network Initialization, 1-24, 1-25, 2-64, 2-67, 2-69, 2-72, 3-14, 3-67, 3-79, 3-80, 3-81, 3-83, 3-147, 3-149, 3-176, 3-177, 3-181, C-5, C-7, C-8, D-1, D-4, D-6
- Network Initialization with Channel
 - Probing, 2-69, 3-81, 3-83, 3-147
- Short Network Initialization, 1-25, 2-69, 2-108, 3-82, B-24
- Network Management, 1-7, 1-13, 1-26, 1-36, 2-9, 2-22, 2-76, 2-91, 2-92, 2-182, 3-3, 3-7, 3-18, 3-23, 3-24, 3-92, 3-97, 3-114, 3-195, 3-343, 3-345, 3-351, 3-357, 3-358, B-54, C-1, C-10, D-8
- Changing the Network DTDMA flag, 2-98
- Changing the Network ONCS flag, 2-98
- Monitoring, 2-82, 2-92, 2-97, 2-178, 2-186, 3-10, 3-15, 3-67, 3-193, 3-194
- Capacity, 2-94
- Connectivity, 2-93
- Network Parameters Management, 2-92, 2-97
- Network Parameters
 - Changing Media Parameters, 2-99
- Role Management
 - NMU, 2-92, 2-95, 2-105
- Network Management and Control
 - NMC, 3-18, 3-23, 3-24, C-6, C-8, C-10, 28
- Network Management Function
 - NMF, D-8
- Network Management Unit
 - NMU, 1-26, 2-9, 2-22, 3-114, C-1
 - Management, 2-92, 2-95, 2-105
- Network Membership Determination, 2-40, 2-44
- Network Packet
 - NP, 1-21, 2-8, 2-50, 2-80, 3-8, 3-18, 3-19, 3-20, 3-37, 3-38, 3-46, 3-47, 3-53, 3-54, 3-56, 3-57, 3-58, 3-59, 3-60, 3-61, 3-84, 3-159, 3-162, 3-165, 3-225, 3-228, 3-229, 3-230, 3-232, 3-277, 3-278, 3-280, 3-301, 3-302, 3-328, 3-329, 3-340, 3-342, B-17
 - Continuation Data, 3-303, 3-304
 - Data, 3-302
 - Header, 3-302
 - Optional Data, 3-304
 - Padding, 3-305
- Network Packet Header, 3-302
- Network Packet Production
 - NPP, 3-18, 3-20, 28
- Network Packet Reception
 - NPR, 3-18, 3-20, 3-21, 28
- Network Participation Group
 - NPG, 2-157, 2-170, 2-174, 2-176, 3-111
- Network Start Time
 - NST, 2-17, 2-31, 2-33, 2-37, 2-85, 3-79, 3-87, 3-90, 3-95, 3-139, 3-140, 3-141, 3-143, 3-145, 3-147
- New Network
 - Creation, 2-104, 2-108, 2-119
 - Initialization, 2-84, 2-89, 2-90, 3-137, 3-147, 3-149
 - Assignment of roles, 3-147, 3-149
 - Creation of MASN, 3-147, 3-148
 - Distribution of the New Network Order, 3-147, 3-148
 - Initialization of the New Network, 3-147, 3-149

NILE Address, 2-11, 2-34, 2-39, 3-13, 3-14, 3-24, 3-84, 3-108, 3-109, 3-110, 3-111, 3-153, 3-166, 3-169, 3-171, 3-172, 3-175, 3-180, 3-232, 3-233, 3-244, 3-246, 3-249, 3-257, 3-296, 3-302, 3-312, 3-313, C-5, C-7

NILE Communications Equipment, 1-14
NCE, 1-14, 1-16, 3-6, A-17, A-21

NILE Network

NN, 1-4, 1-6, 1-9, 1-19, 1-22, 1-24, 1-25, 1-26, 1-27, 1-28, 1-29, 2-6, 2-7, 2-8, 2-9, 2-10, 2-15, 2-16, 2-18, 2-32, 2-38, 2-85, 2-88, 2-101, 2-108, 2-116, 2-175, 3-23, 3-24, 3-25, 3-46, 3-93, 3-98, 3-132, 3-188, 3-233, 3-254, B-3, B-4, C-1, D-3

Parameters, 2-6, 2-7, 2-16, 2-18, 3-254
DTDMA Enabled/Disabled, 2-6, 2-9, 2-16, 2-23, 2-97

Dynamic TDMA, 2-85

Fragmentation Rate, 1-21, 2-6, 2-8, 2-16, 2-20, 2-46, 2-48, 2-50, 2-72, 2-85, 2-97, 3-60, 3-79, 3-81, 3-84, 3-137, 3-142, 3-155, 3-157, 3-159, 3-160, 3-183, 3-254, B-26, D-5

Frequency, vii, 1-21, 1-41, 2-4, 2-5, 2-6, 2-8, 2-15, 2-16, 2-18, 2-19, 2-20, 2-69, 2-85, 2-97, 2-123, 2-128, 2-178, 2-180, 2-181, 3-56, 3-62, 3-64, 3-65, 3-79, 3-80, 3-81, 3-85, 3-137, 3-142, 3-144, 3-146, 3-157, 3-159, 3-162, B-4, B-26, B-49, D-5

Initialization Type, 2-6, 2-9, 2-16, 2-21, 3-80

LLC Integrity, 2-6, 2-8, 2-16, 2-20, 2-31, 2-72, 2-85, 2-97, 3-46, 3-60, 3-79, 3-88, 3-137, 3-142, 3-144, 3-155, 3-157, 3-159, 3-160, 3-162, 3-233, B-17, B-26, B-52, B-56, D-4, D-5

Media Setting Number, 2-6, 2-8, 2-16, 2-18, 2-19, 2-69, 2-72, 2-85, 2-97, 2-99, 3-79, 3-81, 3-83, 3-137, 3-155, 3-157, 3-159, 3-160, 3-254, B-26, B-56, D-5

Media Type, 1-21, 2-6, 2-8, 2-16, 2-18, 2-19, 2-20, 2-45, 2-69, 2-85, 2-97, 2-99, 3-79, 3-81, 3-137, 3-142, 3-144, 3-146, 3-157, 3-254, B-4, B-26, B-51, B-52, D-4

NILE Network Parameters

Network Cycle Structure, 1-13, 1-22, 2-6, 2-10, 2-16, 2-23, 3-23, 3-25, 3-59, 3-82, 3-137, 3-197, 3-225, 3-254, 28

Network Members, 2-6, 2-9, 2-16, 2-22, 2-40, 2-44, 2-60, 2-105, 2-187, 3-112, 3-121, 3-187, 3-191, 3-240, B-2, B-3, D-3, D-4

Network Start Date, 2-6, 2-8, 2-16, 2-21, 2-36

Network Start Time, 2-17, 2-37, 2-85, 3-79, 3-87, 3-90, 3-95, 3-139, 3-140, 3-141, 3-143, 3-145, 3-147

Roles, 2-6, 2-9, 2-16, 2-22

NILE Network Structure Set

NNCS, 2-33, 2-38, D-5

NILE Reference System

NRS, vii, viii, 1-11, 3-5, A-1, A-2, A-3, A-4, A-5, A-6, A-7, A-8, A-9, A-10, A-11, A-13, A-15, A-16, A-23

Components, A-3

Configurations, A-3, A-6, A-13

NILE Super Network, C-1

NILE Unit

NU, 1-24, 1-27, 2-6, 2-10, 2-11, 2-16, 2-27, 2-28, 2-34, 2-39, 2-54, 2-80, 2-85, 2-155, 2-165, 3-23, 3-25, 3-109, 3-194, 3-222, 3-258, B-20, D-2, D-3, D-5, D-6

Loss of, 3-184, 3-191

NU Closedown, 3-184, 3-188, 3-190

NU Data, 3-15, 3-117, 3-118, 3-193, 3-194, C-8, D-1, D-7, D-8

NU Link Reception Quality

NU LRQ, 2-53, 2-54

NU Management, 2-76, 2-84, 2-108, 3-107

NU Performance Data, 2-41, 2-92, 2-93, 2-94, 3-14, 3-117, 3-193, 3-195, 3-291, C-6, C-8

NU Reception, 2-79, 2-81, 2-93

NU Relay Setting, 3-108

NU Status, 2-53, 2-54, 2-56, 2-111, 2-112, 2-114, 2-119, 3-13, 3-14, 3-76, 3-78, 3-108, 3-109, 3-116, 3-117, 3-119, 3-121, 3-173, 3-187, 3-189, 3-191, 3-192, B-20, C-6, C-7, D-3

NU Termination, 2-116

Parameters, 2-6, 2-11, 2-16, 2-27, 2-165, 3-109

Link 22 Address, 2-6, 2-11, 2-16, 2-27, 2-34, 2-36, 2-38, 2-53, 2-64, 2-109,

- 3-25, 3-69, 3-76, 3-78, 3-83, 3-89,
3-97, 3-108, 3-109, 3-110, 3-139,
3-144, 3-146, 3-194, 3-313, B-2, B-3,
B-25, B-27, D-2, D-3, D-5, D-7
- Role Takeover, 1-30, 2-6, 2-11, 2-16,
2-27, 2-30, 2-84, 2-91, 2-119, 3-13,
3-115, B-13, C-6
- Track Number Blocks, 2-6, 2-11, 2-16,
2-27, 2-29, 2-58
- Unit Identification, 2-6, 2-11, 2-16,
2-27
- NMU Role Management, 2-92, 2-95, 2-105
- Non Command and Control
 - NonC2, 2-155
- Non Machine Receipt
 - Non-MR, 3-201, 3-202, 3-207, 3-208, 3-209,
3-210, 3-214, 3-216, 3-234, 3-293, 3-294,
3-295, 3-312
 - Address Group, 3-294
- North Atlantic Treaty Organization
 - NATO, v, 1-1, 1-2, 1-14, 1-33, 2-33, 2-157,
2-159, 2-171

O

- Officer in Tactical Command
 - OTC, 2-118, 3-184
- Operation Order
 - OPORD, 2-171
- Operational Network Cycle Structure
 - ONCS, 2-10, 2-97, 3-225, 3-318
 - Changing the Network ONCS flag, 2-98
- Operational Start Time
 - OST, 2-67, 2-68, 2-70, 2-97, 3-169, D-3, D-5
- Operational Tasking (order)
 - OPTASK, 1-20, 2-13, 2-30, 2-33, 2-34, 2-64,
2-171, 2-179, 2-180, 2-181, 3-68, 3-75,
3-147, 3-155, C-4, D-1
- Operator Actions
 - Amplification Data, 2-131
 - Electronic Warfare (EW), 2-127, 2-130, 2-169,
C-13
 - Information Management, 2-132, C-13
 - Participant Location & Identification (PLI),
2-125
 - Summary, 2-63, 2-119

- Surveillance, 2-25, 2-43, 2-127, 2-128, 2-129,
2-170, 3-200, C-13, C-14
- Threat Warning, 2-124, 2-131, 2-164, 2-171
- Weapons Coordination and Management,
2-133, C-13
- Operator Interface System
 - TDS/DLP, 1-39, 2-65, 2-68, 2-70, 2-87, 2-101,
2-108, 2-117, 2-158, 2-177, B-49
- OPTASK Link Managemet
 - OLM
 - Advanced Production, 2-40, 2-57
- OPTASK Link Message
 - OLM, 1-20, 2-13, 2-30, 2-33, 2-34, 2-64, 2-171,
2-179, 2-180, 2-181, 3-68, 3-75, 3-147,
3-155, C-4, D-1
 - Network Data, D-1, D-4
 - Super Network Data, 3-76, D-1, D-2
- Orders, 3-92
 - Automation, 2-84, 2-87, 2-119
 - Function Management Switches, 3-70, 3-92,
3-95, 3-96
 - Overview, 3-92
 - Protocol, 3-92, 3-97, 3-99, 3-100, 3-101
 - Queue Processing, 3-103, 3-105
 - Queuing Commands, 3-103, 3-104

P

- Packed Message Indicator
 - PMI, 2-135
- Partial Timeslot Ownership Change
 - PTOC, 3-319, 3-321, 3-324, 3-327, 3-328,
3-330, 3-331, 3-332
- Participant Location & Identification
 - PLI, 2-25, 2-43, 2-78, 2-123, 2-125, 2-126,
2-145, 2-158, 2-177, 3-121, C-13, C-14,
C-15
- Participants Set, 2-36
- Participating Unit
 - PU, 1-34, 2-28, 2-29, 2-155, 2-159, 2-160,
2-172, 2-173, 2-176
- Perishability, 1-17, 1-18, 3-292, 3-307, 3-312
- Perishable Message, 3-200, 3-201
- Physical Interface, 3-6, 3-32, 3-50
- Point to Point

P2P, 1-19, 2-175, 3-127, 3-202, 3-234, 3-236,
 3-237, 3-238, 3-293, 3-352, 3-353, 3-355,
 3-356, 3-357, B-55
 Position
 POS, 2-43, 2-123, 2-126, 2-128, 2-142, 2-149,
 2-151, 2-167, 2-173, 2-174, 2-177, 3-165,
 B-6, B-55, D-7
 Post-Test, A-11, A-14, A-23, A-25, A-26
 Potential Relay NILE Unit
 PRNU, 3-270, 3-271, 3-272, 3-274, 3-282,
 3-283, 3-284
 Power Management, 2-103, 3-137, 3-143, 3-145,
 3-147, 3-150
 Preamble, 2-50, 3-38, 3-54, 3-183, 3-342
 Precise Participant Location and Identification
 PPLI, 2-143, 2-158
 Preparation Request Response
 PRR, 3-11, 3-199, 3-203, 3-207, 3-210, 3-213,
 C-2, C-3
 Pre-Test, A-11, A-12, A-23, A-24
 Priority Injection
 PI, 1-8, 1-17, 1-18, 1-22, 1-34, 2-38, 2-46, 2-47,
 2-48, 2-51, 3-83, 3-89, 3-139, 3-144, 3-165,
 3-200, 3-201, 3-210, 3-213, 3-217, 3-223,
 3-258, 3-260, 3-261
 Priority Injection Indicator
 PII, 1-17, 1-18, 3-200, 3-201, 3-210, 3-213,
 3-217, 3-223
 Probability of Correct Reception, 3-262, 3-277,
 3-293
 Probing, 2-8, 2-9, 2-21, 2-37, 2-69, 2-71, 2-74,
 2-88, 2-99, 2-108, 3-13, 3-14, 3-79, 3-80, 3-83,
 3-84, 3-86, 3-87, 3-88, 3-89, 3-90, 3-91, 3-93,
 3-94, 3-98, 3-102, 3-104, 3-138, 3-146, 3-148,
 3-149, 3-345, 3-354, C-5, C-7, D-4, D-5, D-6
 Probing Network Initialization, 2-69, 2-71, 2-99
 Probing Reception Quality
 PRQ, 2-69, 3-84, 3-85
 Processing Algorithm, 3-244, 3-246
 Compare to the MP Data Store, 3-247, 3-250,
 3-251
 E2ERN Received Flag, 3-247, 3-248
 Index Maintenance, 3-247
 MP Index, 3-247, 3-249
 Store a Non Duplicate, 3-247, 3-249, 3-250,
 3-251, 3-252
 Time Index Value, 3-246, 3-247

Program Management Warfare
 PMW, vi
 Project Management Office
 PMO, 2, ii, vi, x, xi, 2-33
 Pulses Per Second
 PPS, 3-57
 Push-to-talk
 PTT, 3-63

Q

Quality of Service
 QoS, 1-3, 1-13, 1-16, ¹⁻¹⁷, 3-234, 3-262
 Addressing, 1-17, 1-18, 2-174, 2-175,
 2-176, 3-92, 3-197, 3-234, 3-293, 3-294,
 B-28
 Data Originator Identification, 1-17, 1-18
 Indicator Flags, 1-17, 1-18
 Perishability, 1-18
 Priority, 1-17
 Reliability, 1-18, 3-281

R

Radio Frequency
 RF, 1-19, 2-158, 3-56, 3-264
 Radio Power
 Change, 2-76, 2-77, 2-103
 Management, 2-92, 2-103, 3-14, C-8
 Cannot Control Radio Power, 3-152
 Request to Adjust another NU's Radio
 Power, 3-151
 Radio Silence
 RS, 1-18, 1-27, 2-54, 2-77, 2-78, 2-79, 2-88,
 2-103, 2-112, 2-114, 2-115, 2-118, 2-119,
 3-93, 3-98, 3-104, 3-109, 3-116, 3-117,
 3-118, 3-119, 3-120, 3-121, 3-194, 3-200,
 3-201, 3-285, 3-293, 3-357, B-26, B-50, C-5
 Change, 2-76, 2-77, 2-78
 Network, 2-92, 2-103, 2-104, 2-119
 Status, 1-27, 3-120
 Radio System, 1-39, 1-41, 2-158
 Real Time, 2-25, 2-26, 2-43, A-25, A-26

- Reallocation, 2-155, 3-14, 3-175, 3-177, 3-319, 3-320, 3-321, 3-322, 3-323, 3-324, 3-325, 3-328, 3-329, 3-330, 3-331, 3-332, 3-333, 3-334, C-7
- Total capacity Amount
 - RTA, 3-330, 3-331
- Receipt Compliance
 - R/C, 2-123, 2-181
- Receive Data
 - RxD, 3-51
- Received Message Delay, 2-81, 2-82
- Received Tactical Errors, 2-81, 2-82
- Reception
 - Explicit Flow Control Protocol, 3-206
 - Optimized Receive Protocol, 3-69, 3-206, C-2, D-7
 - Problems, B-51, B-52
- Reception Probability
 - RxP, 3-263, 3-264, 3-265, 3-269, 3-270
- Recipient Processing, 3-318, 3-325
- Re-Configuration
 - RECONF, 1-31, 2-88, 2-95, 2-119, 3-13, 3-14, 3-93, 3-94, 3-98, 3-102, 3-104, 3-106, 3-118, 3-137, 3-138, 3-139, 3-140, 3-141, 3-195, 3-354, C-5, C-6, C-7, C-10
- Red Control CSCI
 - RCC, 3-49, B-33, B-51
- Red Interface Processor
 - RIP, B-12, B-29, B-33
- Reed Solomon
 - RS, vii, viii, 1-11, 1-43, 3-50, 3-57, 3-60
- Reference
 - Ref, 2-124, 2-128, 2-135, 2-142, 2-143, 2-149, 2-150, 2-170, 2-177, 3-246, 3-297, 3-311, 3-323, B-55
- Re-Initialization
 - Media Parameter Change, 3-141, 3-142, 3-143
 - REINIT, 1-32, 2-20, 3-118, 3-137, 3-141, 3-195, 3-354, C-5, C-7, C-10
 - Re-initialization with Probing, 3-141, 3-146, 3-147
 - Short Re-Initialization, 3-141, 3-144
- Relay
 - and Routing Management
 - RRM, 3-18, 3-20, 3-23, 3-24, 3-287, 28
 - Flow Control Decisions, 2-84, 2-91, 2-119
 - Setting, 2-53, 2-55

- Automatic, 1-5
- Management, 2-104, 2-113
- Setting
 - Change, 3-13, 3-78, 3-104, 3-283, C-5
 - Unit, 3-262, 3-270
- Reporting Potential Relay NILE Unit
 - RPRNU, 3-270, 3-271, 3-272, 3-273, 3-274, 3-276, 3-283, 3-284
- Reporting Responsibility
 - R2, 2-151, 2-171
- Reporting Unit
 - RU, 2-28, 2-155, 2-160, 2-172, 2-173
- Request Management Information, 2-84, 2-119
- Resilience, 1-13, 1-29
- Role
 - Loss Timeout, 3-115, D-2
 - Maintenance, 3-123, 3-129
 - NMU, 1-26, 2-9, 2-22, 3-114, C-1
 - SNMU, 1-26, 2-7, 3-114, C-1
 - Standby NMU, 3-114
 - Takeover Control, 2-84, 2-91, 2-119, 3-13, 3-115, C-6
- Roll Call, 1-34, 2-159
- Routing, 3-20, 3-91, 3-121, 3-131, 3-141, 3-146, 3-197, 3-221, 3-240, 3-241, 3-262, 3-274, 3-275, 3-276, 3-280, 3-281, 3-282, 3-291, 3-297, 3-343, 3-344, 3-351, 3-353
- Control Value
 - RCV, 3-274, 3-275, 3-281, 3-282, 3-283
- Path Determination, 3-262, 3-273
- Selection, 3-262, 3-280
 - Prediction, 3-280, 3-287
 - Production, 3-280, 3-287, 3-289
 - Random Selection, 3-280, 3-281
 - Selection Criteria, 3-280
 - Coverage, 3-280, 3-281
 - Delay, 3-280, 3-281, 3-331
 - Reception, 3-280, 3-281
 - User Throughput, 3-280, 3-281

S

- Scenario Developer
 - SD, A-11, A-12
- Scenario Generator

- SG, A-3, A-10, A-11, A-12, A-13, A-14, A-16, A-25
 - Programs, A-12, A-13, A-14
- Scenario Generator Extractor
 - SGEX, A-11, A-16
- Scenario Generator Server
 - SGSV, A-11
- Scenario Generator Workstation
 - SGWS, A-11
- Scheduler
 - SCH, 3-18, 3-26, 3-27, 3-29
- Secure Communication, 1-13, 1-15
- Secure Data Unit
 - SDU, 2-35, B-6
- Segment Specification
 - SS, vii, 3-57, 3-63, 3-277, 3-293, 3-301, 3-307, 3-346, 3-347
- Sequence Identifier
 - SID, 3-35, 3-335, 3-336, 3-339
- Series
 - SER, 1-3, 1-16, 1-35, 1-36, 2-121, 2-122, 2-135, 2-136, 2-137, 2-138, 2-139, 2-141, 2-142, 2-143, 2-147, 2-151, 2-157, 2-159, 2-164, 2-166, 2-177, 3-193, C-16
- Service Header, 3-111, 3-234, 3-235, 3-236, 3-237, 3-238, 3-239, 3-281, 3-305, 3-306, 3-307, 3-308, 3-309, 3-310, 3-311, 3-312, 3-313, 3-315
 - Structures, 3-307
- Service Request, 3-199, 3-200, 3-205
 - Identifier
 - SRID, 3-199, 3-200, 3-202, 3-203, 3-204, 3-207, 3-216, 3-219, 3-220, 3-221, 3-222, 3-224, B-25
- Short Network Initialization, 1-25, 2-69, 2-108, 3-82, B-24
- Signal Processing Controller
 - SPC, vii, 1-14, 1-39, 1-41, 2-2, 2-4
 - Alarms, B-9, B-11, B-47
 - Configuration Failure, 3-15, B-9, B-10, B-11, B-47, C-8
 - Configuration Request, 3-37, 3-53, 3-57, 3-152, 3-185, 3-186, 3-339, 3-340
 - Data Entities, 3-58
 - Media Coding Frame (MCF), 3-58, 3-59
 - Network Packet (NP), 3-56, 3-58, 3-59, 3-60, 3-225

- Desirable features, 3-64
 - Disabled, 3-15, B-9, B-10, B-47, C-8
- HMI Interface, 3-58
- Radio Equipment, 2-2, 2-4, 3-2, 3-65
- Radio Interface
 - Mandatory radio control, 3-64
 - Mandatory radio report handling, 3-64
- Recovery, B-9, B-10, B-11, B-12, B-15, B-16, B-18
- SNC/LLC Interface, 3-57
- SPC System Capabilities, 3-61
- Status Request, 3-37, 3-53, 3-189, 3-339
- TOD Interface, 3-57
- Silent Join
 - SJ, 1-28, 2-72, 2-73, 2-74, 3-129, 3-153, 3-154, 3-155, 3-156, 3-162, 3-164, 3-165, 3-176, 3-177
- Simulation
 - SIM, 2-143, 2-147, A-9, A-20, A-21
- Slow Update Rate Protocol
 - SLURP, 2-26, 2-174, 2-175
- SNC Diamond
 - SNCd, A-3, A-4, A-16
- SNC Initialization, 1-25, 2-67, 3-13, 3-24, 3-67, 3-68, 3-69, 3-71, 3-76, 3-78, 3-79, 3-109, 3-113, 3-148, 3-155, B-20, B-23, B-24, C-5, C-6, D-1, D-2, D-4
 - DLP-SNC Interface, 3-70
 - LLC Configuration, 3-15, 3-37, 3-38, 3-46, 3-48, 3-50, 3-68, 3-72, 3-74, 3-156, 3-185, 3-335, 3-338, B-9, B-10, B-15, B-23, B-24, C-9
 - Connect to LLC, 3-72, 3-73
 - Start, 3-68, 3-69, B-23
 - Super Network Directory Configuration, 3-68, 3-75, 3-108, 3-112, B-21, B-23
- SNC TSR Queue, 3-21, 3-197, 3-214, 3-217, 3-218, 3-219, 3-228
 - External TSR Queue, 3-217
 - Internal TSR Queue Structure, 3-217, 3-219
 - TSR Queue Operations, 3-217, 3-222
 - Cancel, 3-216
 - Change Priority, 3-222, 3-223
 - MP Creation, 3-222
 - TSR Creation, 3-208, 3-211, 3-222
 - Update Data, 3-222, 3-224

- SNC Verification, A-6
- Software Units, 3-18, 3-19
- Software User's Manuals
 - SUMs, A-23, A-25
- Space and Naval Warfare Systems Command
 - SPAWAR, 2, ii, vi, x
- STANAG Repetition Rate Variance, 2-81, 2-82
- Standard
 - STD, 1-18, 2-30, 2-174, 3-8, 3-34, 3-201, 3-268, 3-273, 3-277, 3-278, 3-279, 3-292, 3-293, 3-294, 3-295, 3-297, 3-352, 3-353, 3-354, 3-355, 3-356, 3-357, 3-358
- Standard Reliability
 - SR, 1-16, 1-18, 3-199, 3-201, 3-277, 3-280, 3-287, 3-292, 3-293, C-2
- Standard Update Rate
 - SUR, 2-25, 2-43, 2-123, 2-124, 2-149, 2-151, 2-174
- Standardization Agreement
 - STANAG, 2-81, 2-82, 2-144, 2-145, 2-146, 2-147, 2-148, 2-149, 2-150, 2-151, 2-157, 2-159, B-54
- Status Management, 2-104, 2-111
- Subject Matter Expert
 - SME, xi
- Sub-surface
 - SUB, 2-25, 2-43, 2-123, 2-124
- Super High Frequency
 - SHF, 2-158
- Super Network
 - SN, 1-4, 1-10, 1-20, 1-24, 1-26, 1-27, 1-28, 1-30, 1-34, 2-6, 2-7, 2-8, 2-10, 2-11, 2-15, 2-16, 2-17, 2-18, 2-21, 2-31, 2-32, 2-34, 2-35, 2-39, 2-40, 2-41, 2-42, 2-44, 2-54, 2-55, 2-56, 2-72, 2-74, 2-76, 2-77, 2-78, 2-79, 2-80, 2-81, 2-85, 2-88, 2-92, 2-93, 2-101, 2-104, 2-105, 2-106, 2-109, 2-110, 2-111, 2-112, 2-114, 2-115, 2-116, 2-118, 2-119, 2-181, 2-182, 2-187, 3-13, 3-23, 3-25, 3-68, 3-75, 3-76, 3-77, 3-78, 3-79, 3-91, 3-92, 3-93, 3-97, 3-98, 3-108, 3-109, 3-110, 3-112, 3-113, 3-114, 3-116, 3-117, 3-118, 3-119, 3-121, 3-129, 3-132, 3-141, 3-146, 3-153, 3-164, 3-167, 3-171, 3-173, 3-184, 3-188, 3-189, 3-191, 3-192, 3-193, 3-194, 3-195, 3-202, 3-241, 3-271, 3-273, 3-283, 3-314, 3-349, B-7, B-13, B-20, B-21, B-23, B-24, B-25, B-27, B-56, C-1, C-2, C-4, C-5, D-1, D-2, D-3
- Closedown, 3-184, 3-189
- Directory
 - SN Dir, 1-27, 2-114, 3-23, 3-25, 3-68, 3-75, 3-76, 3-77, 3-108, 3-112, B-21, B-23, 28
 - Components, 3-108, 3-109
 - Maintenance, 3-67, 3-77, 3-108, 3-123, 3-133, 3-148, 3-149, 3-171, 3-187, 3-189, 3-240, B-21
- Management, 1-26, 2-7, 2-76, 2-104, 3-114, C-1
 - MASN Management, 2-104, 2-105
 - Create MASN, 2-105, 2-106, 3-13, 3-76, 3-78, 3-104, 3-112, 3-113, C-5, D-3
 - Delete MASN, 2-105, 2-106, 3-13, 3-104, 3-112, C-5
 - Modify MASN, 2-105, 2-106, 3-13, 3-104, 3-112, C-5
 - SNMU Role Management, 2-104
- Management Unit
 - SNMU, 1-26, 2-7, 3-114, C-1
 - Management, 2-104
- Parameters, 2-6, 2-7, 2-16, 2-17
 - Crypto, 2-7
 - Distribution, 2-104, 2-114
 - Roles, 1-26, 2-7, 3-114, C-1
 - Start Date, 2-6, 2-7, 2-15, 2-16, 2-17, 2-21, B-7
 - Start Time, 2-17, 2-37, 2-69, 3-92, 3-95, 3-105, 3-144, 3-146, 3-330, 3-331, B-28, D-5
- Radio Silence, 2-104, 2-115, 2-119
- Role
 - Management, 2-104
 - Termination, 2-116, 2-118, 2-119
- Supporting Unit
 - SU, 2-73, 3-124, 3-129, 3-153, 3-155, 3-167, 3-168, 3-169, 3-170, 3-171, 3-172, 3-173, 3-175, 3-180, 3-181, 3-183, 3-352
- Surface
 - SUR, 2-25, 2-26, 2-43, 2-123, 2-124, 2-125, 2-126, 2-127, 2-128, 2-133, 2-134, 2-145, 2-149, 2-151, 2-174, 3-292, C-13, C-15

Swap Timeslots
 SWAP, 3-319, 3-324, 3-327, 3-328, 3-329,
 3-330, 3-331, 3-332, 3-333
 System Architecture, 1-13
 Data Link Processor
 DLP, 1-14, 1-39, 2-2, 2-3, 3-3, A-15, 28
 Link-Level COMSEC
 LLC, 1-14, 1-39, 1-40, 2-2, 2-4
 Radio Equipment, 2-2, 2-4, 3-2, 3-65
 Signal Processing Controllers
 SPC, 1-14
 System Network Controller
 SNC, vii, 1-5, 1-11, 1-14, 2-2, 2-3, 3-3,
 3-16, A-3, A-15, 28
 Time of Day Distribution, 2-2, 2-5
 System Network Controller
 SNC, vii, 1-5, 1-11, 1-14, 2-2, 2-3, 3-3, 3-16,
 A-3, A-15
 Bad Status, B-23, B-24
 Communications Transport, 3-7, 3-19,
 3-20
 Duplicate Message Packet Store, 3-20,
 3-21, 3-245
 Message Packet Expansion
 MPE, 3-18, 3-20, 3-21, 28
 Network Packet Production
 NPP, 3-18, 3-20, 28
 Network Packet Reception
 NPR, 3-18, 3-20, 3-21, 28
 Transmission Request Handler
 TRH, 3-18, 3-20, 3-21, 28
 Transmission Service Request
 TSR Queue, 3-20, 3-21, 3-207,
 3-210, 3-213, 3-214, 3-215, 3-217,
 3-219, 3-221, 3-222, 3-223, 3-224
 Failure, B-23, B-24
 Infrastructure
 Global Data and Initialization, 3-18,
 3-26, 3-28
 Initialization Errors, B-23
 Management Function, 3-7, 3-19, 3-20,
 3-22, 3-23
 Congestion Assessment Management
 CAM, 3-18, 3-23, 28
 Fault Management
 FAM, 2-76, 2-79, 2-83, 3-18, 3-23,
 B-1, B-9
 Human Machine Interface
 HMI, 2-4, 3-3, 3-18, 3-23, 3-25, 3-55,
 3-58, A-25, B-21
 Initialization, LNE and Configuration
 Management
 ILM, 3-18, 3-23, 3-24, 28
 NCS Handler
 NCH, 3-18, 3-23, 3-24
 Network and Monitoring
 Management
 NMM, 3-18, 3-23, 3-24
 Network Cycle Structure
 NCS, 1-13, 1-22, 2-6, 2-10, 2-16,
 2-23, 3-23, 3-25, 3-59, 3-82,
 3-137, 3-197, 3-225, 3-254, 28
 Network Management and Control
 NMC, 3-18, 3-23, 3-24, C-6, C-8,
 C-10, 28
 Relay and Routing Management
 RRM, 3-18, 3-20, 3-23, 3-24, 3-287
 Super Network Directory
 SN Dir, 1-27, 2-114, 3-23, 3-25,
 3-68, 3-75, 3-76, 3-77, 3-108,
 3-112, B-21, B-23, 28
 Packing, 3-197, 3-228, 3-234, 3-301
 Processor Hardware, 1-39, 1-40
 Rejected Messages, B-23, B-25
 Status, 3-14, 3-69, 3-70, 3-116, B-9, B-13,
 B-22, C-7
 System Network Controller Diamond
 SNCd, A-5
 System Simulation, A-6, A-9, A-17, A-20, A-21

T

Tactical
 Loads, 2-40
 Tactical Data
 Minimum Exchange, C-1, C-11
 Tactical Data Link
 TDL, 2-28, 2-153, 2-155, 2-158, 2-163, 2-171,
 2-172, 2-176, 2-177, 2-178, 2-180, 2-182,
 2-186, 2-187, A-16
 Tactical Data System
 TDS, 1-14, 1-16, 1-20, 1-39, 1-42, 2-3, 2-65,
 2-67, 2-68, 2-69, 2-70, 2-76, 2-87, 2-101,

2-108, 2-116, 2-117, 2-158, 2-177, 3-3, B-49, 28

Tactical Data Words
TDW, C-2

Tactical Interface
TACT, 3-6, 3-7, 3-10, 3-11, C-2, C-3, C-10

Tactical Messages, xiii, 1-3, 1-13, 1-15, 1-16, 2-24, 2-25, 2-42, 2-121, 2-122, 2-124, 2-125, 2-126, 2-129, 2-130, 2-131, 2-132, 2-133, 2-134, 2-135, 2-141, 3-3, 3-7, 3-11, 3-20, 3-21, 3-69, 3-197, 3-199, **3-200**, 3-204, 3-206, 3-244, 3-310, 3-311, 3-323, 3-327, B-25, C-2, C-3

Construction, 2-122, 2-135

Design Goals, 2-122

F-Series Catalog, 2-122, 2-123

Tactical Message Hierarchy, 2-122, 2-125

Transmission, 1-13, 1-16

Statistics, 2-79, 2-81

Words
TMW, 1-16, 2-24, 2-25, 2-37, 2-42, 2-43, 2-44, 2-45, 2-122, 2-135, 2-141, 2-153, 3-69, **3-200**, 3-244, 3-310, 3-311, 3-323, 3-327

Takeover, 2-11, 2-84, 2-91, 3-115, B-13, D-2, 28

Technical Messages, 3-20, 3-21, 3-23, 3-24, 3-102, 3-124, 3-125, 3-197, 3-268, 3-271, 3-273, 3-290, 3-301, 3-318, 3-321, 3-322, 3-323, 3-324, 3-343, 3-345, 3-346, 3-347, 3-349, 3-350, 3-351, 3-352, 3-353, 3-354, 3-355, 3-357, 3-358

Exchange, 3-318, 3-321, 3-322

Message List, 3-343

Message Structure, 3-9, 3-33, 3-53, 3-343, 3-346

Termination
Network, 2-116, 2-117, 2-119

NILE Unit, 2-116

Super Network, 2-116, 2-118, 2-119

Test Controller User Interface
TCUI, A-25

Test Execution, A-11, A-12, A-13, A-14

Test Facilities, 1-11

Threat Warning, 2-124, 2-131, 2-164, 2-171

Time Division Multiple Access
TDMA, 1-8, 1-9, 1-22, 1-29, 1-34, 2-9, 2-10, 2-23, 2-157, 3-63, 3-64, 3-197, 3-225, 3-318, B-11, B-47, B-54

Time Figure of Merit
TFOM, 3-4, 3-5, 3-58, B-49

Time Index, 3-246, 3-247, 3-248, 3-249, 3-253

Time of Day
TOD, 1-40, 1-42, 2-2, 2-3, 2-4, 2-5, 2-65, 3-2, 3-3, 3-4, 3-5, 3-18, 3-19, 3-31, 3-47, 3-49, 3-55, 3-57, 3-58, 3-112, 3-116, 3-121, 3-194, 3-323, 3-324, 3-325, 3-328, 3-331, 3-332, 3-340, B-1, B-9, B-13, B-14, B-21, B-23, B-48, B-49, B-50, B-56

Time Of Day
TOD
Crypto, 3-47, B-48
Day of Week, 2-7, 2-17, 2-66, 2-72, 2-86, 3-47, 3-48, 3-49, 3-69, 3-72, 3-74, 3-156, 3-157, B-7, B-8, B-15, B-21, B-48, B-51, B-52, B-56
Time of Week, 3-47, 3-48, 3-49, B-51, B-52, B-56
Degradation, B-9, B-13
Failure, B-9, B-13
Source Hardware, 1-39, 1-42

Time Of Weekday
TOW, 3-47, 3-48, 3-49, B-51, B-52, B-56

Timeslot, 2-44, 2-47, 2-48, 2-50, 3-15, 3-64, 3-83, 3-84, 3-85, 3-89, 3-139, 3-144, 3-165, 3-230, 3-233, 3-256, 3-257, 3-258, 3-260, 3-261, 3-265, 3-296, 3-319, B-9, B-14, C-8, D-5
Violation, 3-15, B-9, B-14, C-8

Timeslot Duty Factor
TSDF, 2-178, 2-181, 2-186

Timeslot Number
TSN, 3-46, 3-47, 3-48, 3-49, B-51, B-52

Timeslot Ownership Change
TOC, 3-319, 3-321, 3-324, 3-327, 3-328, 3-330, 3-331, 3-332, 3-333

Timing Event Generator
TEG, 3-18, 3-31

TMW Construction, 2-122, 2-135

Totalcast
TC, 1-19, 2-175, 3-121, 3-127, 3-202, 3-234, 3-241, 3-243, 3-270, 3-291, 3-293, 3-314

Track
Identification, 2-164, 2-166
Number

- TN, 2-6, 2-11, 2-16, 2-27, 2-29, 2-30, 2-58, 2-135, 2-142, 2-143, 2-145, 2-149, 2-150, 2-151, 2-164, 2-165, 2-175, 2-176, 2-177, **3-200**
- Block, 2-6, 2-11, 2-16, 2-27, 2-29, 2-58, 28
- Quality
- TQ, 2-143, 2-164, 2-165
- Transmission
- TX
 - Assurance, 2-174, 2-177
 - Completed
 - TXC, 3-11, 3-199, 3-203, 3-207, 3-208, 3-210, 3-211, 3-213, 3-216, C-3
 - Needs, 2-40
 - Priority Management, 3-197, 3-205
 - Rules, 2-144, 2-149, 3-4, 3-291
 - Success Rate, 2-81, 2-82
- Transmission Completed
 - TXC, 3-11, 3-199, 3-203, 3-207, 3-208, 3-210, 3-211, 3-213, 3-216, C-3
- Transmission Control Protocol
 - TCP, 1-43, 2-4, 2-159, 3-6, 3-8, 3-28, 3-30, 3-32, 3-33, 3-69, 3-73, 3-206, 3-227, 3-228, 3-231, 3-232, 3-336, B-13, B-24
- Transmission Request Handler
 - TRH, 3-18, 3-20, 3-21
- Transmission Security
 - TRANSEC, 2-18, 2-66, 3-63, B-55
- Transmission Service Request
 - TSR, 1-16, 3-11, 3-20, 3-21, 3-198, 3-199, 3-204, 3-205, 3-207, 3-280, 3-287, C-2, C-3
 - Addressee Information, 3-200, 3-201
 - Perishable Message Indicator, 3-200, 3-201
 - Priority, 3-216
 - Priority Injection Indicator, 1-17, 1-18, 3-200, 3-201, 3-210, 3-213, 3-217
 - Radio Silence Override Indicator, 1-18, 3-200, 3-201
 - Reliability, 1-17, 1-18, 1-29, 3-200, **3-201**, 3-277, 3-278, 3-279, 3-292, 3-293, 3-295
 - Service Request Identifier
 - SRID, 3-199, 3-200
 - Source Track Number, 3-199, **3-200**

- Tactical Message Size, 3-199, **3-200**
- with Data, 3-198, 3-199
- without Data, 3-198

- Transmit Data
 - TxD, 3-51

U

- Ultra High Frequency
 - UHF, 1-6, 1-21, 2-159, 3-56, 3-65, B-55
- Unit Addresses, 2-164, 2-165
- Unit Data Set, 2-39, 2-57
- Unit Reception Quality Set, 2-57, 2-58
- Unit Under Test
 - UUT, A-3, A-4, A-5, A-6, A-7, A-17, A-18, A-21
- United Kingdom
 - UK, vi, xi, 1-2
- United States
 - US, vi, 1-2, 2-30, 2-158, 2-171, 2-182
- Universal Time Coordinated
 - UTC, 1-42, 3-4, 3-5, 3-57, B-49, B-50
- Update Rate, 2-26, 2-143, 2-186
- User Datagram Protocol
 - UDP, 2-159
- Utilities
 - UTL, 3-18, 3-26, 3-28

V

- Versa Module Eurocard
 - VME, 1-40, 1-41, 3-55
- Version Numbers, 3-123, 3-169, 3-180

W

- Weapons Coordination, 2-133, C-13
- Weapons Management, 2-133, C-13
- Will Comply
 - WILCO, 2-87, 2-89, 3-97, 3-99, 3-100, 3-101, 3-102, 3-114, 3-149, D-8
- Worldwide Geodetic System
 - GWS, 1-34, 1-36
 - WGS, 1-34, 1-36, 2-168, 2-173



NILE Project Management Office
Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, CA 92110-3127, USA
Website: <https://www.link22.org>



Northrop Grumman Systems Corporation
9326 Spectrum Center Boulevard, San Diego, CA 92123, USA
Voice: 858-514-9047, Facsimile 858-499-0208
E-Mail: cis.productsupport@ngc.com
Website: www.tacticalnetworks-ngc.com

NORTHROP GRUMMAN

