CHAPTER 28

RF Network Management

See Distribution Statement A

LIST OF FIGURES

LIST OF TABLES

Distribution Statement A

Approved for public release: distribution unlimited.

28. CHAPTER 28

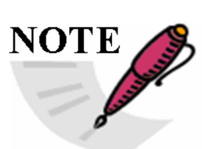
28.1 Introduction

This chapter defines the mechanisms and processes for managing RF links with the RF Network. The RF Network implements an Open Systems Interconnect (OSI) model approach (Figure 28-1) to data transmission, where data moves through the OSI stack from the application layer to the physical layer, from physical layer to physical layer through some transmission medium, then back up the stack to another application on the receiving side. For the most part, the RF Network operates just like any other TCP/IP network, where a message is created using a standard data management protocol, such as SNMP, is encapsulated at the transport layer to TCP or UDP, and then is further encapsulated into a IP packet that contains the logical addressing and path routing determination. Where the RF Network differs from the standard OSI model is in the data link and physical layers, where Media Access Controls (MAC) have been modified to support transmission over RF links.

OSI Model					
Layer		Data Unit	Function	Examples	
Host Layers	7. Application	Data	High Level APIs, including resource sharing, remote file access, directory services and virtual terminals	HTTP, FTP, SNMP, SSH, TELNET	
	6. Presentation		Translation of data between a networking service and an application, including character encoding, data compression and encryption/decryption	HTML, CSS, GIF	
	5. Session		Managing communications sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, PAP, SSL, SQL	
	4. Transport	Segments/Datagram	Managing communications sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	TCP, UDP, NETBEUI	
Media Layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control	IPv4 IPv6, IPSec, Apple Talk, ICMP	
	2. Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer	PPP, IEE 802.2 L2TP, MAC, LLDP	**Covered by this chapter**
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	Ethernet physical layer, DSL USB, ISDN, DOCSIS	**IRIG 106 Chapter 27**

Figure 28-1 – OSI Model as related to the TmNS RF Network

The RF Network manages communications at the data link and physical layers of the OSI model. This chapter focuses on the RF Network with respect to managing the data link layer of the OSI model. The RF Network is a multi-node network with a network layer control and data plane. The control plane for managing the RF link layer multiple access is described in this document. For information on the physical layer of the RF Network, refer to Chapter 27. The RF Network's control plane uses the existing ground network and adds RF connectivity to allow changes to RF transmission and capacity allocation in transceivers during missions. Radios need not establish direct bidirectional links with other transceivers in order to be part of the RF Network. Rather, they are part of the network based on the principles and standards associated with normal IP routing protocols and need only support one or more paths to and from the overall RF Network.



This note is expected to be deleted after initial review.

Early versions of this chapter defined transceiver protocols that required pairs of direct links between communicating RF Network transceivers. Since the actual implementation of RF propagation in a epoch structure based network supports broader concepts, this limitation was removed and as such concepts allowing for RF multicast and multiple RF receiver source selection are now possible.

RF Network media access utilizes an epoch structure transmission scheme. Management of the epoch schedule is coordinated through the interfaces defined in this document.

In order to support dynamic updates to the epoch structure, transceivers update their currently active policies based on RF Network Messages. These messages define when the transceiver has been given authority to transmit. This chapter covers the setting of transmit opportunities (TxOps) and the associated supporting RF Network Messages. The RF Network Messages are defined in Chapter 24, Message Formats. The end product of the link layer control plane messaging is the coordinated definition of the start and stop times associated with transmit opportunities in the RF Network. An overview of the RF Network's link layer concepts are given in section 28.2 of this document.

When coordinating the transmission of multiple transmitting entities, it is the responsibility of RF link management to sequence the sending of TxOp messages and check for feedback of assigned transmission opportunities from the transmitting entities in order to avoid multiple concurrent use of the channel by multiple transmitters as required by range policy. TxOps are assigned with either a finite or an infinite timeout value. An example of an epoch structure of an RF Network is given in section 28.3 of this document.

A specific RF link manager implementation performing the RF link management function and the transceivers being managed are all RF Network components and should provide the interfaces covered in IRIG 106 Chapters 22 through 25.

The bit numbering, bit ordering, and byte ordering conventions used in this chapter are described in Appendix 21B.

28.2 RF Network Management Concepts and Definitions

28.2.1 Data Link Layer Framing

The RF Network provides a standards-based IP network (IETF RFC 791 and RFC 2474). Layers supporting this IP layer are unique to the TmNS RF Network. Figure 28-2 shows an overview of the protocol layers associated with sending an IP packet over the data link layer and RF physical interface. The IP packets are referred to as MAC Service Data Units (MSDUs) and are comprised of complete IP packets containing user data. The MSDUs are placed into payload blocks with aggregation and fragmentation performed to meet the maximum transmission unit (MTU) of the RF channel. AES-CCMP encryption may be used to provide added security on the RF link by encrypting the payload blocks. The length-limited payload blocks are separated into RF MAC frames and link layer header information is added. Forward error correction is added to the RF MAC frames to create LDPC blocks suitable for transmission over the RF interface. Details of the lower levels of this protocol are covered in Chapter 27.

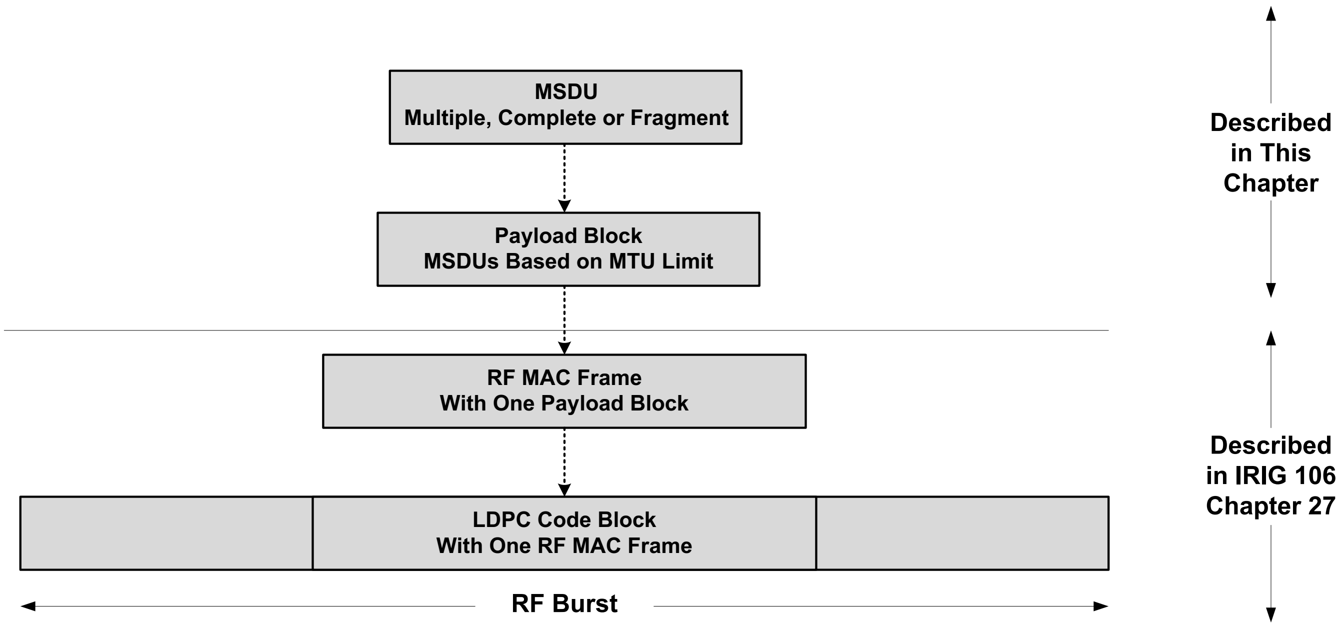


Figure 28-2 - Data Link Layer Framing Overview

28.2.2 RF Link Management

RF link management is responsible for scheduling RF spectrum access for TmNS transceivers. Time synchronization is required as defined in IRIG 106 Chapter 22. The format of the time in RF Network Messages is defined in Chapter 24. RF link Management also performs route selection for packets transiting from the wired networks to the RF networks.

There is at least one RF link management source associated with a ground station. The RF link management on the range may be controlling one or more transmitting entities on the ground. RF link management also controls transmitting entities which are networked through the ground network such as those contained on test articles.

RF link management provides a set of control protocols for managing a transmitting entity's RF spectrum access. These protocols include:

- Transmission scheduling
- RF transmission capacity management
- Handoff management
- Power management - TBD
- Link and RF Traffic Loading Status

28.2.3 Epoch Structure

The RF Network implements an epoch structure to provide an efficient utilization over a shared bandwidth. Link management messages support dynamic adjustment of the epoch structure being utilized by components comprising a RF Network.

28.2.4 Epoch Length

An epoch is a period of time over which transmission opportunities are assigned to a transmitting entity. An epoch shall be defined of one of the following lengths: 1000 ms (maximum epoch size), 500 ms, 250 ms, 100 ms (default epoch size), 50 ms, 40 ms, 25 ms, 20 ms, 10 ms (minimum epoch size).

Epochs shall be aligned with time synchronized seconds as defined in Chapter 22 corresponding with a transition between two adjacent epochs.

28.2.5 Transmission Opportunities (TxOps)

A transmission opportunity (TxOp) is a time allocated opportunity for a transmitting entity to transmit data. A TxOp is a window in time over which a transmitting entity may transmit over its associated RF interface. The TxOp contains a start time and stop time that is relative to a repeating time boundary which is referred to as an epoch. The epoch is settable to a number of discrete times during initialization.

28.2.6 Guard Time

Guard Time is the time utilized by an overall RF Network epoch schedule to assure clock jitter and RF propagation delays do not create undesired RF collisions. There are no RF Network Messages associated that specify guard time. Rather, the TxOps that are allocated to components within a RF Network should be set up in a fashion in order to support the desired guard time. IRIG 106 Chapter 23, Metadata Configuration, specifies an interface for communicating guard time to an RF link manager component. Default guard time is recommended to be 1 millisecond.

28.2.7 TE Queues

RF Network components that are intended to behave as IETF IP routers and provide Quality of Service (QoS) handling of traffic which is delivered to the RF interface. The QoS interface is implemented in the form of Traffic Engineering (TE) queues. As such, the behavior concerning the ingress and subsequent egress (or in overload situations, drop) of messages shall comply with the details specified in IRIG Chapter 22, Network-Based Protocol Suite (Section 22.5.3, Quality of Service (QoS)).

28.2.8 Handoff

Handoff is a process by which the RF path is changed to use a different RF Network interface. In this way, the route (path) of RF propagation that is experiencing undesired receive RF quality can be directed to a different path. This updated path (post handoff) will be through a different RF Network interface that may be in the current RF Network or it may include switching to another RF Network. This chapter does not provide a particular mechanism for performing handoff operations but rather a sequence of use of RF management interfaces can accomplish a variety of handoff operations.

NOTE	It is expected that handoff will be performed when a test article transceiver begins to move out of range of a ground antenna, moves from one RF Network to another, or moves from one range to another. This chapter does not specify a policy for when a handoff is to be performed. It can be automatically or manually directed.

28.2.9 Heartbeat

The Heartbeat mechanism defines a relative time to automatically cease transmissions and clear all TxOps from the transmission schedule for a transmitting entity. The initial heartbeat value shall be loaded from an MDL configuration file, and the value shall be updated upon reception of a RF Network Message containing a Heartbeat TLV. Reception of a RF Network Message containing a Heartbeat TLV from RF link management which is directed to any RF Network interface on the receiving transmitting entity will refresh the heartbeat counter for all RF Network interfaces (e.g. links) on which the transmitting entity is processing TxOps. Links are defined in Section 28.2.10.

28.2.10 RF MAC Header Addressing

A link is comprised of a RF MAC address source/destination pair that defines the endpoints of an RF transmission. Throughout this chapter, this pair is referred to as a "link". Links are individually managed, including scheduled, by the RF Link Management.

The RF MAC Address shall be a 16-bit value subdivided into a Vendor ID field (most significant 4 bits) and an RF Interface field (least significant 12 bits), whereby the Vendor ID field uniquely identifies the manufacturer and the RF Interface field further uniquely identifies a RF component produced by that manufacturer. One of the Vendor ID fields is reserved for RF multicast group addresses.

Table 28-1 – RF MAC Header Vendor IDs

Vendor IDs	Description
4'b0000	Reserved
4'b0001–4'b1101	Vendors
4'b1110	Experimental
4'b1111	Multicast

The assignment of a unique Vendor ID value to each manufacturer is outside the scope of this chapter. Manufacturers are responsible for ensuring the uniqueness of the RF MAC Address space of the components they produce.

28.2.11 Timing

The RF link management and all entities under its control shall have their clocks synchronized. Methods of time synchronization is defined in IRIG 106 Chapter 22. The format of the time in RF Network Messages is defined in Chapter 24.

28.2.12 Virtual TxOps

When a transmitting entity does not have any TxOps allocated for the current or any future epochs, a Virtual TxOp time slot shall be available for responding to link layer control plane TCP connection over the RF interface. The Virtual TxOp shall be a single burst in size and shall be located at the beginning of each GPS second. This allows the RF link management to receive return messages from a transmitting entity in the exchange of TCP control messaging after which time a TxOp Assignment TLV can be sent to the transmitting entity in order to maintain long term communications.

NOTE The RF link management uses a TCP connection which requires a bidirectional handshake to occur before TxOp Assignment TLVs can be received. The use of the Virtual TxOp transmission allows standard TCP methods to establish the link layer control path without using unprotected messaging.

28.2.13 Independent Operation

A RF network shall be capable of operating independent of RF link management control. In this mode of operation, TxOp allocations are the result of configuring with an MDL file that contains the transmission schedule. A heartbeat value of infinite allows TxOp assignments to remain in effect indefinitely, assuming the TxOp timeout value remains greater than zero, or until RF link management changes the value by sending a non-infinite heartbeat value in a Heartbeat TLV. The transmitting entity operating independent of RF link management as described shall allow RF link management control to take over independent operations. An

See Distribution Statement A

independent transmitting entity allows externally received Heartbeat TLVs and TxOp Assignment TLVs to overwrite MDL-provided values.

28.3 RF Media Access Control Layer

The RF MAC layer is responsible for providing access to the physical media (i.e. the wireless RF network). On the transmission side it is responsible for framing IP packets for physical transmission (adding in the layer 2 hardware addresses for the source/destination pair of the link). On the receive side it is responsible for validating the checksum sent with each packet (known as the Frame Check Sequence) and de-framing the received packet.

28.3.1 Epoch

This physical structure of the RF channel will be supported by an epoch structure, to separate transmission signals. It emulates full-duplex communication over a half-duplex link and is utilized by the TmNS RF Network. The transmitting entity shall synchronize the epoch start time with a commonly referenced external time synchronization mechanism which is common to the RF Network.

28.3.1.1 Epoch Structure

An epoch structure shall contain an integer multiple of transmission opportunity assignments (TxOps). The number of TxOps and their durations are assigned according to the need and policy which has been put in place by RF link management. Figure 28-3 depicts an example of a schedule with four transmitting entities in a network with TxOps to access the RF network.

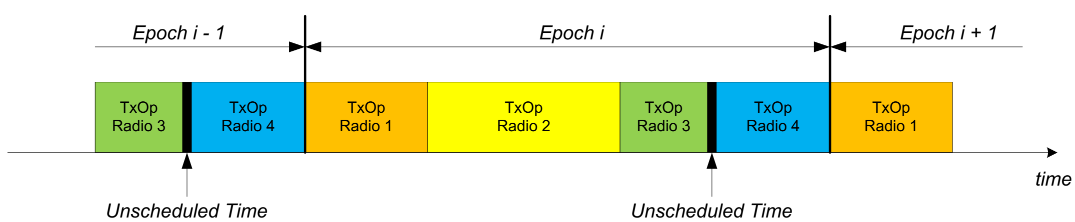


Figure 28-3 - Typical Epoch Structure

Transmitting entities in the network are only aware of the start and stop times of a transmission opportunity, and it is the responsibility of RF link management to provide unscheduled time in order to provide sufficient guard times when scheduling TxOps. For times other than the assigned TxOp periods in an epoch, a transceiver shall transition to receive mode, i.e., capable of receiving transmissions destined for it. When there are no packets ready to be transmitted when a scheduled TxOp period occurs, the transmitting entity shall not transmit. A detailed description of the TmNS RF burst sequence requirements for the transmitting entity can be found in Chapter 27.

28.3.1.2 Epoch Timing

The duration of the epoch frame period shall be constrained to the following allowable values: 1000 ms (maximum epoch size), 500 ms, 250 ms, 125 ms, 100 ms (default epoch size), 50 ms, 40 ms, 25 ms, 20 ms, 10 ms (minimum epoch size). Epoch size for a transmitting entity shall only be set during configuration through the MDL configuration file. It is not required that RF link management update the allocated capacity at the same rate as the epoch period used in the RF network.

NOTE	While this chapter allows for different components within a RF Network to be configured with different epochs, it is expected that all epochs will be the same.

28.3.1.3 Guard Times

Between TxOp allocations, a period of no transmissions referred to as a guard time may be provided by RF link management or independent MDL configuration to allocate time between transmissions. Guard times also can be used to account for RF propagation delays across the range. It is the responsibility of the RF link management to provide guard times between the TxOps that it allocates. Guard times are intentional gaps in the epoch structure in which no transmitting entity has a TxOp.

28.3.1.4 Transmission Opportunity

The use of transmission opportunities provide a mechanism of provisioning coordinated channel capacity across multiple transmitting entities on a RF Network based on the policies in place for the range. To access the RF media, one or more transmission opportunities are assigned to a transmitting entity. A single transmission opportunity is the authority of the transmitting entity to transmit to its RF interface between two time periods referred to as start and stop times. The start and stop times of a transmission opportunity are defined relative to a reoccurring epoch start time. The epoch start time of a transmitting entity should be synchronized with GPS seconds or external time synchronization as defined in IRIG 106 Chapter 22.

Each transmit opportunity has a defined destination RF MAC address (e.g. link) which is set to the RF MAC address of an individual transceiver or an RF multicast group address. Transceivers can be set to listen on one or more multicast addresses in addition to their RF MAC address. Multiple transmission opportunities can be assigned to a transmitting entity which are for the same, different, or a combination of RF MAC addressed destinations.

If a Transmitting entity does not have sufficient data to generate burst sequences that completely fill a transmission opportunity, then it may cease transmission after all needed burst sequences have been transmitted, i.e., a transmitting entity is not required to pad to fill a transmission opportunity.

If a transmitting entity has ceased transmission in a TxOp and more data becomes available to be transmitted while there is sufficient time remaining in the TxOp both to allow the minimum time between transmissions and to transmit one or more complete burst sequences, then the transmitting entity shall resume transmission, transmitting one or more contiguous burst sequences.

NOTE	The timeout value in the TxOp TLVs allows epochs of transmissions to be scheduled and not each transmission. This relaxes the requirement of RF link management processing and supporting network speed. Prior to the addition of the timeout functionality, the RF link management was required to generate the complete network complement of RF Network Messages containing TxOp TLVs and transfer them to the transmitting entities, meeting tight setup times, each epoch for proper RF data plane management. Section 28.3.1.4 discusses the TxOp capability.

28.3.2 Media Access Control Frame Structure

The media access control frame structure determines what RF transmissions are received. The RF MAC filters received traffic, accepting only those RF transmissions that the receiving entity is interested in receiving.

28.3.2.1 Header Format

Frame headers for RF MAC control frames contain the destination, source, and a length. The destination address is either an RF MAC address of the destination transceiver or an RF multicast address which specifies the RF multicast group that receiving entities can listen to. The source address is always the RF MAC address of the transmitting entity. A length is included which indicates the length of the MAC payload in the MAC frame. Additional information about the RF MAC Frame Format can be found in Chapter 27.

28.3.2.2 Unprotected Payload

All link layer control frames are contained in secure TCP payload streams with only the RF MAC layer header including the source and destination sent unprotected. The FCS is also sent unprotected to allow for PHY layer verification of a correctly received frame.

28.3.2.3 Protected Payload

The link layer control frames are contained in TCP secure IP packets. These frames contain RF Network Messages to control transmissions on the RF network. If AES encryption is used, then the secure TCP packets will have an additional level of encryption.

28.3.3 RF MAC Payloads

MSDUs are received from upper protocol layers by the RF Link Layer and are aggregated, fragmented or directly placed into payload blocks. The payload blocks have a FPSH header added to preserve the original MSDU shape when reconstruction is performed at the link layer on the receiving end. The combined payload block and FPSH header is then encapsulated either encrypted or unencrypted into the RF MAC frame described in Chapter 27. This is shown in Figure 28-4.

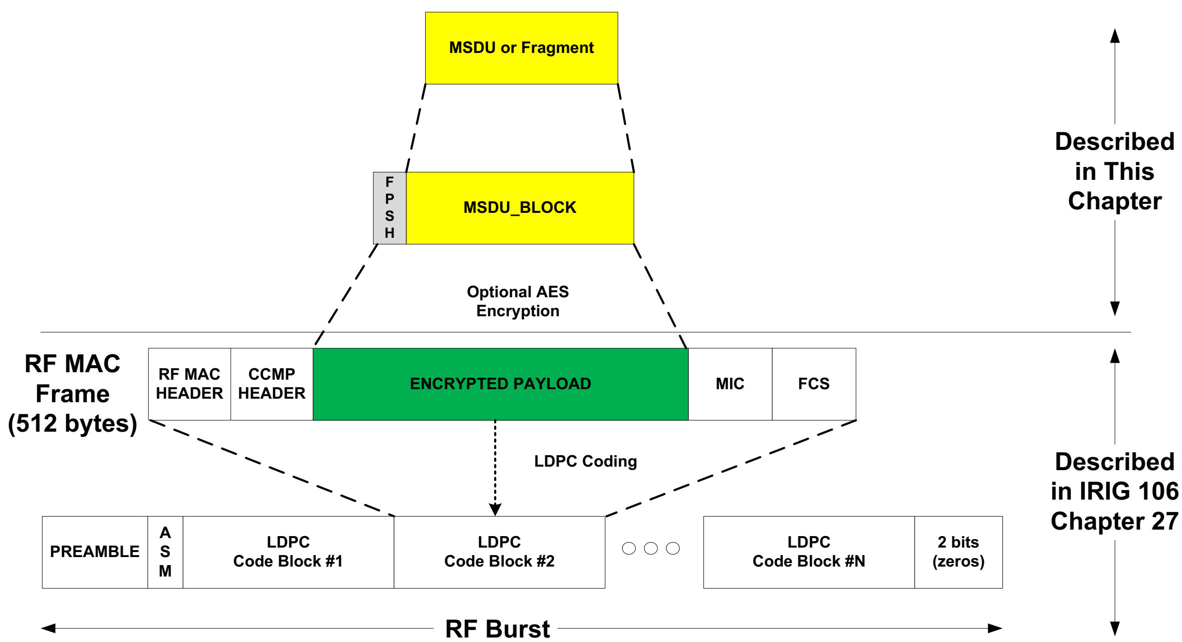


Figure 28-4 - MSDU Insertion into RF MAC Frame

28.3.3.1 RF MAC Service Data Units

Portions of messages to be transmitted across the RF link in the RF MAC payload are called RF MAC Service Data Units (MSDUs). These originate as IP packets.

28.3.3.2 RF MAC Frame Fragmentation

If an IP packet is too long to fit into a RF MAC frame, then it is fragmented. Fragmentation is the process by which a RF MAC SDU is divided into one or more MSDU_Blocks. An MSDU_Block contains a full MSDU or a fragment of an MSDU. MSDU_Blocks can also be called ARQ blocks if ARQ is being used (see Section 28.3.5). The fragmentation process is undertaken to allow efficient use of available payload in an RF MAC PDU. Capabilities of fragmentation and reassembly are required. Fragments are tagged with their position in their parent SDU in accordance with the values defined for the Fragmentation Control field shown in Table 28-2.

Multiple short RF MAC SDUs and/or fragments of RF MAC SDUs can be packed in the same RF MAC frame. Capabilities of packing and unpacking are required. When an RF MAC SDU is not fragmented, the Fragmentation Control field in the FPSH shall be set to 00 “No Fragmentation”.

A fragmentation/packing sub-header (FPSH) precedes each fragment or packed entity. Each fragment or packed message is itself an MSDU_Block. An MSDU_Block can be variable length, with a maximum length of 494 bytes. The FPSH structure is depicted in Figure 28-5.

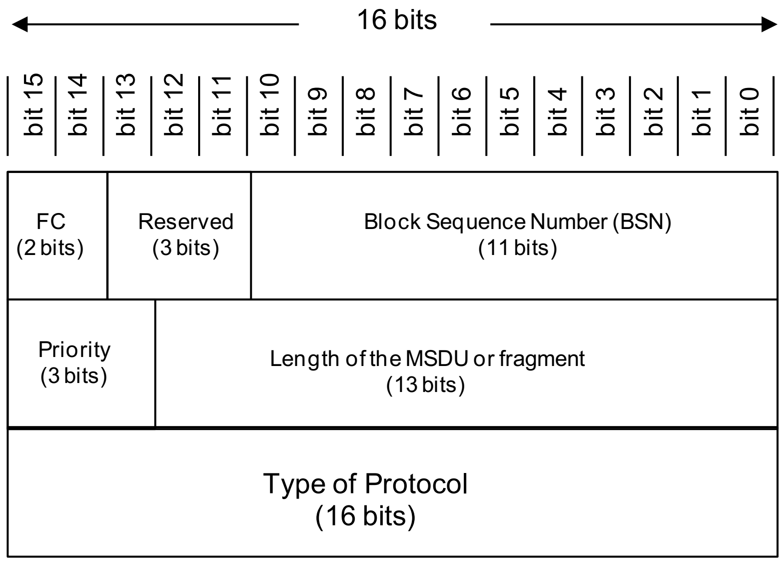


Figure 28-5 - Fragmentation/Packing Sub-Header (FPSH)

Table 28-2 - Definition of Fields in Fragmentation/Packing Sub-Header (FPSH)

Field	Width (Bits)	Description
FC	2	Fragmentation Control (FC) Indicates the fragmentation state of the payload MSDU: 00 = no fragmentation 01 = last fragment 10 = first fragment 11 = continuing (middle) fragment
Reserved	3	Reserved

BSN	11	Block sequence number (BSN) for this MSDU_Block [0 … 2047] modulo 2048
Priority	3	Priority ranking for this MSDU_Block
Length	13	Length (in bytes) of this MSDU_Block, including this six-byte FPSH [7 … 500]
Protocol	16	Type of Protocol Use standard Ethernet values
TOTAL	48	

The MSDU_Block size shall be variable with a maximum of 494 bytes in an unprotected RF MAC frame and 478 bytes in an RF MAC frame protected with AES CCMP encryption.

The link layer control messages described in this document are sent within standard IP packets which are marked as IP type in the Protocol field.

If a RF MAC frame has a payload field, the payload shall comprise one or more MSDU_Blocks each with its associated FPSH. See the notional diagram in Figure 28-6.

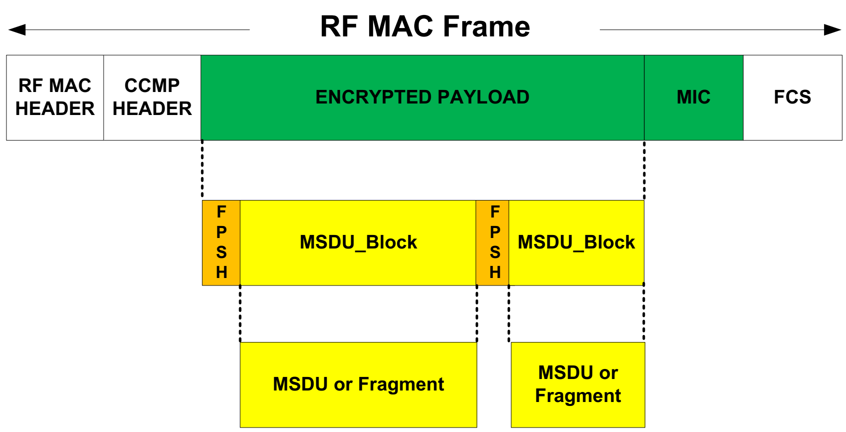


Figure 28-6 - Notional Diagram of RF MAC Frame Containing Two MSDU_Blocks

Whenever possible, the payload of a RF MAC frame shall be completely filled. This may necessitate fragmenting the next MSDU that is to be transmitted.

If there are 6 bytes or fewer remaining in a payload, the remaining bytes shall be padded with zeroes. The length field in each FPSH tells the size of the following MSDU_Block.

If an MSDU is fragmented into multiple MSDU_Blocks, the multiple MSDU_Blocks shall be transmitted in the same order in which they occurred in the MSDU and shall have BSNs which are consecutive integers, modulo the BSN modulus.

If an MSDU is fragmented into multiple MSDU_Blocks and all the MSDU_Blocks are not transmitted in a single TxOp, then the remaining MSDU_Blocks should be the first new MSDU_Blocks sent at this priority level. When MSDU_Blocks are available for more than one priority level, MSDU_Blocks marked with the higher numeric priority values shall be chosen over lower numeric priority values.

See Distribution Statement A

NOTE	ARQ needs to follow the same policy that the transceiver has been assigned by system management and not a priority of its own. As a result, just implementing a priority based ARQ is a conceptually broken solution. Priority is the metric that the policy implements. The epoch based link layer does not support resending quickly upon failure, so ARQ packets are queued and without policy based processing, the ARQ packets inherently violate the policy that the transceiver has received. To have a separate set of TE queues that are managed with a policy in coordination with the TE queues that are not a part of ARQ is a high degree of complexity to be required of the vendor's design.

28.3.4 Frame Check Sequence

The FCS contained at the end of an RF MAC frame shall serve as a link layer error checking mechanism. The FCS generation and verification is covered in Chapter 27. Additionally, the higher-layer protocols (e.g, IP checksums) perform their own error checking.

28.3.5 ARQ Processing

TBD.

28.4 Logical Link Control Layer

The logical link control (LLC) layer of the RF Network provides media access control and transfer of data frames. The LLC layer provides the control mechanisms for dynamically managing transmission bandwidth.

Epoch-based RF link management is accomplished by sending RF Network Messages to the transmitting entities to modify the current transmission schedules. The RF Network Messages are defined in IRIG 106 Chapter 24. All RF link management messages are sent using a secure TCP connection with the transmitting entity. The details of the security provided for RF link management is defined in the Information Assurance document (Ref TBD).

RF Network Messages are sent with IP Precedence as defined in IRIG 106 Chapter 22 – Network-Based Protocol Suite (Section 22.5.3.2, DiffServ Code Point (DSCP) Assignments).

A RF Network Message may contain multiple types of TLVs. When an RF Network Message contains multiple TLVs, each message shall be processed in the order in which they are packed.

28.4.1 TxOp Processing

The external loading of a schedule of TxOps from external MDL shall be equivalent to receiving a sequence of RF Network Messages with TxOp Assignment TLVs. An export of a transmitting entity's configuration in MDL shall include all the currently scheduled TxOps regardless of whether they originate from TxOp Assignment TLVs in RF Network Messages, an MDL configuration file, or a combination of both input sources. The transmitting entity shall allow TxOp Assignment TLVs received in RF Network messages to modify existing scheduled TxOps, including those initially set during configuration with an MDL file.

A TxOp assignment for a transmitting entity may be different in each epoch, and multiple TxOp Assignment TLVs for use in a single epoch may be sent in the same RF Network Message from RF link

See Distribution Statement A

management. Received TxOps shall take effect within two complete epoch start times after reception. For each allocated TxOp in a transmitting entity's schedule, the transmitting entity shall send a status RF Network Message containing TLVs with both information on all Quality of Service (QoS) transmit queue levels and receiver link quality to RF link management.

A RF Network Message containing one or more TxOp Assignment TLVs can be sent by RF link management and likewise be received at any time during the epoch by a transceiver. TxOp Assignment TLVs adjustments are state based, that is they adjust the epoch schedule based on top of all prior adjustments that were accomplished. A TxOp Assignment TLV can add, remove, or modify an existing TxOp window for transmissions. A modification of a currently active TxOp Assignment TLV occurs when a new TxOp Assignment TLV completely subsumes an existing TxOp. The start time of the new subsuming TxOp should be equal to or earlier than the existing TxOp and the stop time should be equal to or greater than the existing TxOp.

The TxOp Assignment TLV also contains a timeout value that specifies the lifetime of the TxOp as measured in epochs. The timeout value can be zero which will result in the removal of one or more TxOps which are completely subsumed by the TxOp Assignment TLV received regardless of their former timeout values. If the timeout value is infinity, which is defined as the value 255, the TxOp defined by the received TLV is put in place with no epoch-based timeout, and it shall replace all TxOps which are subsumed by the start and stop times of the TxOp TLV.

TxOp Assignment TLVs are associated with a particular RF link. The RF link is a source and destination pair of RF MAC addresses that identifies the source, e.g. the radio that is to use the particular TxOp, and the destination RF MAC address to which it is to transmit to. Any transmitting entity that transmits to multiple destination groups shall have separate TxOp Assignment TLVs sent to it in order to differentiate which RF interface is being allocated for transmission. The associated link is contained in the RF Network Message header.

Each time the transmission schedule of a transmitting entity is updated, it shall report to RF link management with an RF Network Message containing a TxOp ID Acknowledgement Report TLV. The report shall be generated after the new schedule has been applied. The report may be generated in the epoch prior to the first use of the associated TxOp if the relative start time and stop time have already occurred within the current epoch if the new TxOp will be first utilized during the next epoch. TxOps with TxOp ID values of zero (16'h0000) shall not be acknowledged by transmission entities. TxOp ID Acknowledgement Report TLVs are not specific to the particular source and destination RF MAC Addresses contained in the message header of the RF Network Message containing the TLV. If the RF Network Message only contains the TxOp ID Acknowledgement Report TLV, then the RF Network Message header should use its own RF MAC Address as the source address and a valid RF MAC Address for the destination address, such as the address pair associated with the RF Network Messages that contain the TxOp Assignment TLV messages from RF link management.

A transmitting entity may only transmit over a particular RF interface at the frequency and for the epoch-based periodic time slot that has been specified in a valid TxOp Assignment TLV. Any time a TxOp is executed, the frequency of the transceiver is set according to the associated frequency value that was specified in the corresponding TxOp Assignment TLV, and transmission is allowed for the duration of the TxOp. If a TxOp Assignment TLV's start time is equal to its stop time (i.e., time duration is zero), it shall be considered a valid TxOp Assignment TLV.

NOTE	A zero-duration TxOp may be used to support handoff scenarios that involve a frequency change. That is, they provide a mechanism that supports commanding a transceiver to change its receiving frequency but does not give authority to transmit over the new frequency. Rather, a TxOp received on the new frequency from a different RF network management entity that would then give authority to transmit.

Each TxOp is given a lifetime in terms of the number of epochs that it is valid for. The lifetime may be updated before it expires on its own if a new TxOp Assignment TLV arrives with a start and stop time that completely subsumes an existing scheduled TxOp.

Multiple TxOp Assignment TLVs may be packed into a single RF Network Message if the associated TxOps are destined for the same source over the same RF interface (link).

Because start and stop times are relative to the size of the epoch, a time window equal to the size of the epoch is used to define when the start time and stop time in a TxOp Assignment TLV are considered to be valid. TxOp Assignment TLVs that define transmission opportunities falling outside this window shall be discarded.

Because the start and stop times of TxOps are quantized values (limited to integers that represent microseconds within an epoch), the start time shall correspond to times greater than or equal to the time represented by the value of the start time field. The stop time shall correspond to the exact instance of the greatest value that is less than the stop time field plus 1. Thus, the valid transmission time associated with a TxOp shall be according to the following equation:

$$t_{start} \leq valid\ transmission\ range < t_{stop} + 1$$

If the start time of one TxOp is equal to the stop time + 1 of the previous TxOp, the TxOps can be called back-to-back TxOps. From a transmitter's perspective, back-to-back TxOps allow continual transmission without a requirement to turn off the transmitter power prior to the conclusion of the first TxOp.

From a transmitting entity's perspective of the system, each time an epoch is processed, all scheduled TxOps that contain a non-zero TxOp timeout value will be executed. After execution, the timeout value associated with that TxOp will be decremented by one unless it is an infinite TxOp with a timeout value of 255. Once the timeout value of a TxOp reaches the value of zero, it is removed from any future processing. For infinite TxOps, the timeout does not decrement after execution.

28.4.1.1 TxOp Processing After Power Interruption

In the event of power interruption, the transceiver shall configure itself to receive using the relevant parameters of the last processed TxOp or the configuration data from the last loaded MDL configuration file, whichever occurred more recently. If no valid TxOps exist, it shall be assumed that no transmission slots are allocated to it for the next epoch. The transceiver shall continue to perform its receiver functionality.

NOTE	In the event of a power interruption, the transceiver should store its current TxOps and associated timeout values. After booting back up, the transceiver shall resume transmissions if the TxOps have not timed out and the transceiver's heartbeat timeout is not zero. This can be determined by calculating the number of epochs that have passed since the reboot event. The transceiver should still obtain time synchronization prior to executing any TxOps.

28.4.1.2 TxOp Processing When Heartbeat Times Out

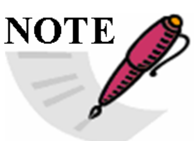
If the timeout value for the last received heartbeat from RF link management expires before the receipt of the next heartbeat, the transceiver shall flush all scheduled TxOps with a remaining non-zero timeout value that was received.

Any new TxOp Assignment TLVs that are received whose current heartbeat timeout value is zero shall be discarded. A non-zero heartbeat timeout is required in order to process new TxOp Assignment TLVs.

See section 28.4.4 for more information regarding Heartbeat TLVs.

28.4.2 Queue Management Processing

To provide the state of traffic loading in the Traffic Engineering (TE) queue interface to the RF channel as defined in this IRIG 106 chapter (Chapter 28) as well as Chapter 22, 23, and 27, a MAC Queue Status Report TLV in a RF Network Message shall be generated. MAC Queue Status Report TLVs shall contain traffic loading for each DiffServ Code Point (DSCP) type contained in the transmitting entity. The traffic loading shall include all storage in traffic bearers contained within the transmitting entity. This RF Network Message is generated once per TxOp and occurs at the start of each burst. These chapters specify that there are eight TE queues, each of which corresponds to a specific IETF Precedence Class as summarized by the table contained in IRIG 106 Chapter 22. IRIG 106 Chapter 23, Metadata Configuration, defines the TE queue to IETF class mapping and also includes details of the Metadata Description Language (MDL) grammar that provides a method to define user-specific per hop behaviors for a mission and how they apply to each of the TE queues (Precedence Classes). Transmitting entities shall comply with the QoS concepts defined in IRIG 106 Chapters 22, 23, 27, and 28 by selecting MSDUs to send when a TxOp occurs based on the overall policy that has been specified through MDL. This selection process is therefore the overall configured policy for the mission and specifies the behavior choice process that is to be used across the TE queues. As long as time within the TxOp remains, further messages shall be sent based on the TE queue policies until the TxOp is over.

	It is expected that typical RF link management uses a combination of instantaneous historical queue status TLVs to determine potential adjustment to link layer TxOp allocations.

28.4.3 Link Metric Processing

The Link Metric TLV is used to inform RF link management of the quality of the received data signal in the transceiver. The TLV(s) are sent at a minimum time of once every epoch when a TxOp is performed.

28.4.4 Heartbeat Processing

The initial heartbeat value is obtained through configuration via an MDL configuration file. A RF Network Message containing a Heartbeat TLV shall be used to overwrite the current value of its heartbeat value.

The Heartbeat TLV, which is described in more detail in Chapter 24, provides a numeric timeout value that represents the number of epochs in the future that the transmitting entity is authorized to execute TxOps. These TLVs are generated by the RF link management and sent to the transmitting entities. The timeout value of a newly received Heartbeat TLV shall replace the existing heartbeat timeout value. It is the responsibility of the RF link management to issue new Heartbeat TLVs before the heartbeat timeout expires. A transmitting entity whose heartbeat value has reached zero, all active TxOps are removed, and the transmitting entity shall not transmit further until it receives a non-zero heartbeat value, either from a RF Network Message with a Heartbeat TLV or through reconfiguration with an MDL configuration file.

While the heartbeat timeout value of a transmitting entity is zero, any newly received TxOp Assignment TLVs shall be discarded. A Heartbeat TLV may be sent in the same RF Network Message alongside TxOp Assignment TLVs. Because TLVs within a RF Network Message are processed in order, the Heartbeat TLV should be first before any TxOp Assignment TLV.

A heartbeat value is a global configuration parameter that affects all RF interfaces on the entity. Reception of a RF Network Message containing a heartbeat TLV from RF link management which is directed to any RF Network interface on the receiving entity will refresh the heartbeat counter for all RF Network interfaces (e.g. links).

Heartbeat values that are set to the value representing an infinite lifetime shall never expire. However, these values may be overwritten through RF Network messaging as described above.

The current heartbeat value shall be provided in the MDL file produced by a transceiver during an MDL export operation.

NOTE	In the event of a power interruption, the transceiver should store its current heartbeat timeout value. The heartbeat value should be used after the transceiver boots back up, but only after the proper number of decrements to the timeout are made. The number of epochs missed due to the transceiver being rebooted or powered off should be used to determine the proper number of decrements.

28.5 Tunnel Management

Network tunnels provide a mechanism to ease the complexity of transporting TmNS data and TmNS command and control network packets across pre-existing networks. For example, routing, QoS, multicast delivery, and handoff can be supported by the tunnel, thereby not requiring customized range IT solutions. These tunnels can be created, removed, and adapted through management functions.

Tunnel management provides support for multiple receiving entities of a single transmission in a seamless manner (message-selection-from-many). Doing this allows the network to appear as a packet funnel; that is, it makes the multiple packet receptions appear as a single packet reception. Likewise, tunnel management supports the selection of a particular transmitting entity from a set of possible transmitting entities (transmitter-selection) such that it can appear as a single continuous transmission stream, even in dynamic switching scenarios. Receiving entity message-selection-from-many is a process of allowing multiple receivers to receive the same RF transmissions from a single source. The selection portion chooses the first received packet and forwards it on to its destination while all duplicate packets received are discarded. The transmitter-selection portion of tunnel management allows for the dynamic switching of transmitting entities.

NOTE	Message-selection-from-many and transmitter-selection capabilities of tunnel management can be utilized on a range to support handoff. The message-selection-from-many choice can support a kind of packet-based source selection for the air-to-ground transmissions. The transmitter-selection involves the selection of the transmitting entity for delivering packets to the target network.

Tunnel management shall be implemented by using virtual network interfaces. Virtual interfaces appear just like any real network interface to the host operating system, but they can also be accessed by application programs. These virtual interfaces are commonly called "taps" and are first-class interfaces in linux (https://kernel.org/doc/Documentation/networking/tuntap.txt). Implementations for Windows (www.varsanofiev.com/inside/using_tuntap_under_windows.htm) and OS X (http://tuntaposx.sourceforge.net) are also prevalent.

The overall process of using the virtual interfaces and tunnel selection process is a functionality referred to as TmNS Source Selector (TSS) capability. TmNS transceivers shall provide taps that can be connected through TCP tunnels by RF link management. These taps are referred to as TSS interfaces. TSS tunnels between TSS interfaces shall be implemented using SSL over TCP. See Chapter 22, Section 22.4.3 for more information on SSL. See Chapter 22, Section 22.4.1 for more information on TCP.

28.5.1 Tunnel Connection

RF link management initiates a TCP connection to the TSS listening port on transceiver in order to establish the connection to be used as the tunnel. The default port for listening to incoming TSS connections shall be 55000.

28.5.2 TSS Interface Initialization

Each time a TCP connection is established between RF link management and a target transceiver, the TSS initialization sequence shall occur. Each tunnel end point shall follow their own initialization sequence.

28.5.2.1 Initialization of Transceiver TSS Interface

The transceiver shall create its virtual interface, apply interface properties to it, and then bring up the interface. Once the interface is up and active on the transceiver, it shall send its virtual interface properties through the tunnel to the RF link management. The interface properties shall be carried through TSS Initialization Messages. The TSS Initialization Messages, including the order in which they shall be sent, are described in Chapter 24. The TSS Initialization Messages shall be the first messages sent through the tunnel. After these six messages are sent, any post-initialization operations, such as routing table updates, may be made.

TSS interface parameter values for transceivers may be initialized during configuration through MDL. Default values shall be used if not explicitly described in MDL during component configuration. Default values for a transceiver's TSS interface is shown in Table 28-3.

Table 28-3 – Default Interface Values for TSS Interface of Transceivers

Value	Description
192.168.1.255	Broadcast address to associate with the TSS remote interface
192.168.1.1	IP address to assign to this TSS remote interface
55000	Port to listen on for incoming TCP connection
tap0	Name to give the TSS remote interface
255.255.255.0	Netmask of the TSS remote interface

28.5.2.2 Initialization of RF Link Management TSS Interface

For each transceiver that the RF link management establishes a TSS tunnel with, RF link management shall create a separate virtual interface. The virtual interface shall have its interface properties applied, and then the interface shall be brought up. Once it is up, it shall listen for the six TSS Initialization Messages being sent from the TSS interface of the connected transceiver. Once the six messages are received, the TSS interface has been initialized. If the interface is to be immediately available for routing, a post-initialization routing rule should be added to the RF link management's routing table.

28.5.3 Tunnel Operation

From the RF link management perspective, transmitter-selection IP routing shall be performed by writing to only one of the tunnels associated with the destination IP address. Message-selection-from-many shall use the CRC field of the TSS Data Message in order to identify duplicated received packets. For message-selection-from-many, the first instance of a received IP packet shall be forwarded towards its destination. All subsequent duplicate packets shall be discarded.

With the exception of TSS Initialization Messages, all packets that traverse the tunnels are TSS Data Messages, and they shall conform to the structure described in Chapter 24.

28.5.4 Tunnel Selection

When there are multiple potential RF links (e.g., routes) to a single receiving entity, the RF link management shall route all IP traffic to the target network through the appropriate tunnel. The appropriate tunnel is defined as the tunnel whose endpoint is associated with the transmitting entity that is actively being scheduled with TxOps for the target network.

NOTE	During handoff scenarios, it is expected that RF link management will manage the tunnel selection in conjunction with the TxOp scheduling of the transmitting entities.

See Distribution Statement A