218-20

Range Commanders Council

TELECOMMUNICATIONS AND TIMING GROUP

TELEMETRY OVER INTERNET PROTOCOL (TMoIP) STANDARD

ABERDEEN TEST CENTER
DUGWAY PROVING GROUND
ELECTRONIC PROVING GROUND
REAGAN TEST SITE
REDSTONE TEST CENTER
WHITE SANDS TEST CENTER
YUMA PROVING GROUND

NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION PATUXENT RIVER
NAVAL AIR WARFARE CENTER WEAPONS DIVISION CHINA LAKE
NAVAL AIR WARFARE CENTER WEAPONS DIVISION POINT MUGU
NAVAL SURFACE WARFARE CENTER DAHLGREN DIVISION
NAVAL UNDERSEA WARFARE CENTER DIVISION KEYPORT
NAVAL UNDERSEA WARFARE CENTER DIVISION NEWPORT
PACIFIC MISSILE RANGE FACILITY

30TH SPACE WING
45TH SPACE WING
96TH TEST WING
412TH TEST WING
ARNOLD ENGINEERING DEVELOPMENT COMPLEX

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

**DISTRIBUTION A: APPROVED FOR PUBLIC RELEASE,
DISTRIBUTION IS UNLIMITED**

This page intentionally left blank.

DOCUMENT 218-20

TELEMETRY OVER INTERNET PROTOCOL (TMoIP) STANDARD

February 2020

Prepared by

TELECOMMUNICATIONS AND TIMING GROUP

Published by

Secretariat
Range Commanders Council
U.S. Army White Sands Missile Range,
New Mexico 88002-5110

This page intentionally left blank.

Table of Contents

Changes in this Edition vii

Preface ix

Acronyms xi

Chapter 1. Introduction and Overview of the Telemetry over Internet Protocol 1-1

Chapter 2. Telemetry Transport Techniques 2-1

2.1 Telemetry System Overview 2-1

2.1.1 Airborne Instrumentation System 2-2
2.1.2 Common Telemetry RF Link 2-2
2.1.3 TM Ground Station 2-2
2.1.4 Ground Network 2-3
2.1.5 Telemetry over IP 2-3

2.2 Motivation for TMoIP 2-5
2.3 Challenges for TMoIP 2-6

2.3.1 Downlink Data Requirements 2-6
2.3.2 Uplink Command Requirements 2-8
2.3.3 System Management 2-8

Chapter 3. TMoIP Payload Construction 3-1

3.1 Overview/Management Elements 3-1

3.1.1 TMoIP payload 3-1
3.1.2 TMoIP solution 3-1

3.2 High-Level Requirements (Concept of Operations) 3-1
3.3 OSI Layered Approach 3-2
3.4 OSI Protocol Layer Implementation: TM Terminal 3-4

3.4.1 Layer 1 3-4
3.4.2 Layers 2 – 7 3-4

3.5 OSI Protocol Layer Implementation: Network Processor 3-4

3.5.1 Layer 7 – Application 3-4
3.5.2 Layer 6 – Presentation 3-4
3.5.3 Layer 5 (Null) 3-11
3.5.4 Layer 4 - Transport 3-11
3.5.5 Layer 3 3-13
3.5.6 Layer 2 3-15
3.5.7 Layer 1 3-18

3.6 TMoIP Packet Design Summary and Discussion 3-18

Chapter 4. TMoIP Management 4-1

4.1 Management Mechanisms 4-1
4.2 QoS 4-2

4.2.1 Layer 2 Mechanisms 4-2
4.2.2 Layer 3 Mechanisms 4-3

4.3 Network Performance 4-3

4.3.1 Packet Delay Variation 4-3
4.3.2 Delay 4-3
4.3.3 Network Errors 4-3

4.4 IPv4 to IPv6 Migration 4-4
4.5 Multicast Support 4-5

Appendix A. Recommendations for TM Terminal Layer 1 .... A-1

Appendix B. Considerations for Legacy Asynchronous Transfer Mode Interworking B-1

Appendix C. Summary of Managed Objects C-1

Appendix D. Application Notes D-1

Appendix E. Citations E-1

Appendix F. References F-1

List of Figures

Figure 2-1. Generic TM System 2-1
Figure 2-2. Ground Network Functional Blocks 2-3
Figure 3-1. OSI Layers for TM Terminal and Network Processor 3-3
Figure 3-2. TMoIP Layer 6 implementation 3-5
Figure 3-3. TMoIP 218-10 Control Word 3-6
Figure 3-4. TMoIP 218-P Control Word 3-7
Figure 3-5. TMoIP 218-20 Control Word 3-8
Figure 3-6. TMoIP 218-20 Control Word (12-Byte Detail) 3-9
Figure 3-7. TMoIP Layer 4 - Layer 6 implementation 3-11
Figure 3-8. TMoIP Layer 3 - Layer 6 Implementation 3-13
Figure 3-9. TMoIP Layer 2 - Layer 6 Implementation 3-16
Figure 3-10. TMoIP Packet Layout 3-19

List of Tables

Table 3-1. High-Level Requirements 3-2
Table 3-2. TMoIP OSI Protocol Layer Implementation 3-3
Table 3-3. TMoIP 218-10 Control Word 3-7
Table 3-4. TMoIP 218-P Control Word 3-7
Table 3-5. TMoIP 218-20 Control Word 3-8
Table 3-6. Packet Size Tradeoffs 3-9
Table 3-7. Clock Recovery 3-10
Table 3-8. UDP Header Field Descriptions 3-11
Table 3-9. UDP Header Field Requirements 3-12

Table 3-10. IP Header Field Descriptions 3-13
Table 3-11. IPv4 Header Field Requirements 3-14
Table 3-12. Ethernet Overhead Fields 3-16
Table 3-13. Ethernet Overhead Field Requirements 3-17
Table 3-14. TMoIP Layer 1 Requirements 3-18
Table 3-15. TMoIP Packet Summary 3-19
Table 3-16. Sample Payload Calculations 3-20
Table 4-1. Management Mechanisms 4-1
Table 4-2. Layer 2 QoS Mechanisms 4-2
Table 4-3. Layer 3 QoS Mechanisms 4-3
Table 4-4. Network Performance - Dropped Packets 4-4
Table 4-5. IPv4/IPv6 Requirements 4-4
Table 4-6. Multicast Packets 4-6
Table A-1. Recommendations and Guidelines for the Layer 1 (Physical Layer) Implementation of the TM Terminal A-1
Table B-1. Request for Comments (RFC) 2684 Optimal Payloads B-1
Table C-1. Alarms C-1
Table C-2. Configuration Parameters C-1
Table C-3. TM Statistics C-2
Table C-4. Ethernet Statistics C-2

This page intentionally left blank.

Changes in this Edition

This document is an updated version of and replaces Range Commanders Council (RCC) Document 218-10. The RCC Timing and Telecommunications Group (TTG) made an extensive effort to produce a well-coordinated and useful document. The following is a summary of the changes made in this version, 218-20.

a. TMoIP control word additions

   (1) 64-bit timestamp with nanosecond resolution

   (2) Time source reference flag for Universal Coordinated Time or International Atomic Time

   (3) Payload shaping for minor frames and data quality

   (4) Frame sync status for payload shaped frames

   (5) Fragmentation indication for managing shaped payloads and maximum transmission unit

b. TMoIP control word subtractions

   (1) Identify failures in local TM interface

   (2) Fault signaling capability across the network

   (3) LEN field

c. Reserved a control word version to preserve proprietary variants.

d. Bit rates and changes in bit rates shall be calculated using packet timestamps and algorithms. For compliance, no proprietary packets or bits shall be used.

e. Removal of real-time protocol from timing as an option for clock recovery.

f. Removed many references to range use of ATM.

This page intentionally left blank.

Preface

The Telecommunications and Timing Group (TTG) of the Range Commanders Council (RCC) prepared this Standard. This Standard replaces RCC Standard 218-10, Telemetry over Internet Protocol (TMoIP) Standard. This Standard provides the ranges with a standards-based solution for the ground transport of serial streaming telemetry from multiple vendors and an improvement in cost competitiveness.

Chapter 4 contains recommendations for implementing the ground network. Two appendixes provide information for TMoIP implementation. Appendix F provides additional insight into the management aspects of TMoIP. Appendix G, while not in the scope of the TMoIP requirements, provides information to the user to enable the deployment of a network infrastructure that supports the TMoIP implementation.

Any range that uses telemetry will benefit from this Standard. The purpose of the TTG effort is the identification of the needs of the Major Range and Test Facility Base (MRTFB) community for telemetry (TM) transmission and development of a standard to ensure future interoperability of commercial solutions. This document presents a common standard for use by industry to ensure interoperability and a more cost effective solution for the ranges. Use of this document will also eliminate the need to rely on a single source for critical equipment in the support of range missions within the MRTFB.

Please direct any questions to:

Secretariat, Range Commanders Council
ATTN: TEWS-RCC
1510 Headquarters Avenue
White Sands Missile Range, New Mexico 88002-5110
Phone: DSN 258-1107 COM (575) 678-1107
E-mail usarmy.wsmr.atec.list.rcc@mail.mil

This page intentionally left blank.

Acronyms

AIS	airborne instrumentation system
ATM	asynchronous transfer mode
CDH	communications distribution hub
CFI	Canonical Format Indicator
CLI	command line interface
COTS	commercial off-the-shelf
DQE	data quality encapsulation
DiffServ	differentiated services
DS3	Digital Signal 3
DSCP	differentiated services code point
FIPS	Federal Information Processing Standards
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LC	Lucent connector; local connector
MAC	media access control
MTU	maximum transmission unit
OSI	Open Standard Interconnect
PE	provider edge
PTP	Precision Time Protocol
QoS	Quality of Service
RF	radio frequency
RFC	Request for Comments
SAP	Session Announcement Protocol
SC	subscriber connector; square connector; standard connector
SDP	Session Description Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SSH	Secure Shell
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TDM	time-division multiplexing
TM	telemetry
TMoIP	Telemetry over Internet Protocol
ToS	Type of Service
UDP	User Datagram Protocol
VID	VLAN identifier
VLAN	virtual local area network

This page intentionally left blank.

CHAPTER 1

Introduction and Overview of the Telemetry over Internet Protocol

This document provides specifications and guidance for the ground network segments, which includes the telemetry (TM) terminal, network processor, and the ground network subsystems of a TM range network. This document is for use by equipment vendors in designing products that enable the transport of TM data over Internet Protocol (IP) networks. The “Transmission over Internet Protocol (TMoIP) solution”, discussed in Chapter 2, addresses the ground network elements listed below. The ground network functional blocks, first identified in Chapter 2, are discussed in detail in subsequent chapters. The requirements and recommendations for the TM terminal and network processor elements are located in Chapter 3. In addition, Chapter 4 addresses the ground network implementation via a set of recommendations regarding implementation elements that will enhance the robustness of the TMoIP solution.

a. TM Terminal. The TM terminal interface provides connectivity to the TM stream. The TM stream interface is described by a set of electrical characteristics (such as waveform amplitude and frequency) and mechanical characteristics (such as connector type). This document defines the range of TM stream types to be supported, including the characteristics associated with Layer 1 (Physical Layer) of the Open Standard Interconnect (OSI) model (see Section 3.3).

b. Network Processor. The network processor furnishes the bulk of the TMoIP solution, and consists of the TM stream interface, the TM stream processing, and the ground network interface. The scope of this document is to define the requirements for the network processor associated with OSI Layer 7 through OSI Layer 1.

NOTE	While this document refers to TMoIP, the requirements for the network processor at OSI Layer 1 and OSI Layer 2 are also within the scope of the TMoIP implementation.

c. Ground Network Link. This link provides IP network connectivity and transport of the TMoIP traffic. The ground network includes the network end equipment, typically an IP switch or router, and the interconnecting network. In some cases, the interconnecting network may not be an IP network, but may be a Synchronous Optical Networking (SONET) or asynchronous transfer mode (ATM) implementation. In these cases, the network end equipment may include functionality to perform the required adaptation from the IP switch/router to the native network format.

This page intentionally left blank.

CHAPTER 2

Telemetry Transport Techniques

This chapter provides an overview description of TM systems. Included are the major functions of a TM system and current methods for distribution of TM streams via range communications infrastructures. This chapter also presents the motivations and technical challenges for implementing TM system transport over IP networks. Subsequent chapters address the detailed specifications that define the TMoIP implementation.

2.1 Telemetry System Overview

The RCC's *Telemetry Standards*[1] defines TM as the method of getting data from vehicles during operational launches, test missions, and a variety of other applications. In this section, the different segments that constitute a TM system are discussed. The segments of a generic TM system are shown in Figure 2-1.

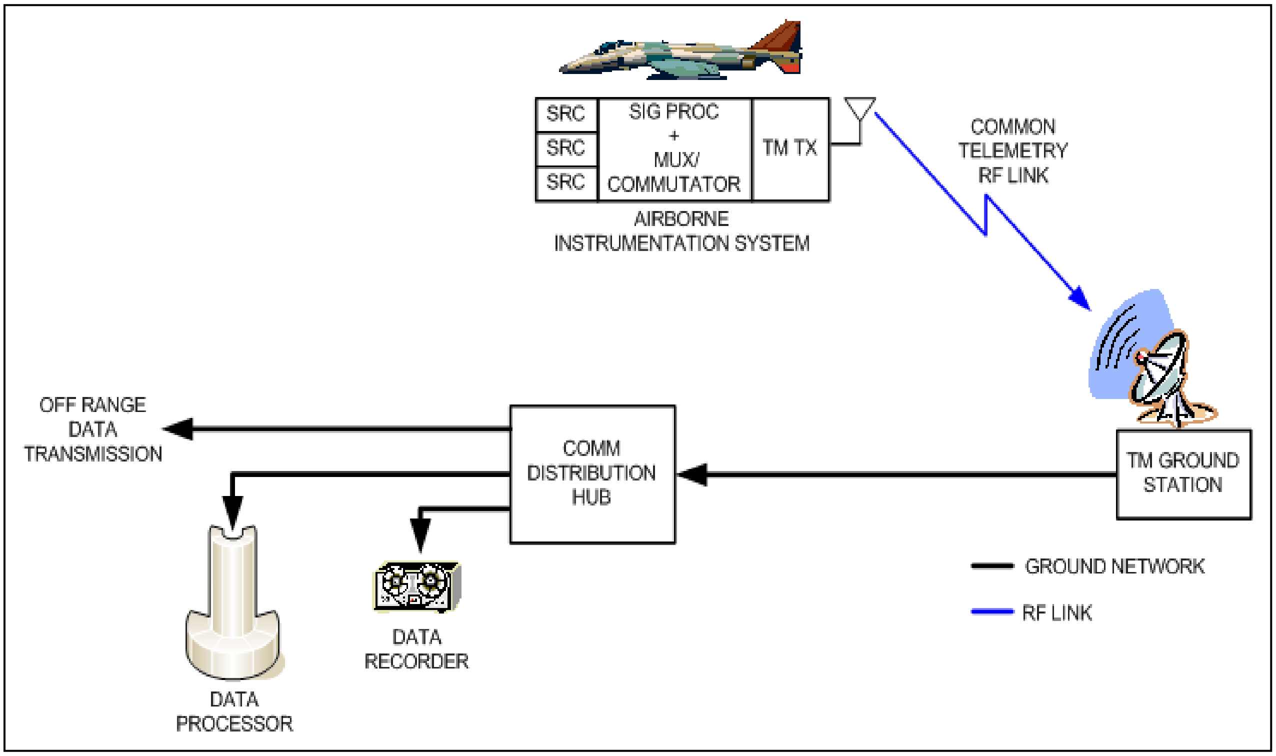

Figure 2-1. Generic TM System

The segments of a TM system are as follows.

a. Airborne instrumentation system (AIS)

b. Common TM radio frequency (RF) link

[1] Range Commanders Council. *Telemetry Standards*. RCC 106-19. July 2019. May be superseded by update. Retrieved 22 July 2019. Available at https://www.wsmr.army.mil/RCCsite/Pages/Publications.aspx.

c. TM ground station

d. Ground network

    (1) Communications distribution hub (CDH)

    (2) Data processor

    (3) Off-range data transmission

    (4) Data recorder

The overall TM goal is to get information that characterizes the operation of the vehicle to the engineers and end users who need it. If any one of the above segments does not function correctly, the data will not be available when needed.

2.1.1 Airborne Instrumentation System

The AIS consists of the TM source (SRC), the Signal Processing and Multiplexer/ Commutator function (SIG PROC + MUX/COMMUTATOR), and the TM transmitter (TM TX).

a. Telemetry Source (SRC). The TM source is a transducer or other information source that produces data (such as temperature or mechanical strain) to be measured or monitored.

b. Signal Processor (SIG PROC). The SIG PROC controls the relevant characteristics of the TM source (such as amplitude, offset, and frequency) to allow interface compatibility with downstream circuitry and to enhance signal integrity and quality.

c. Multiplexer/Commutator (Mux/Commutator). The MUX/COMMUTATOR function allows multiple TM sources to be combined for transmission. The output is the combined information generated by one or more individual information source(s) that have been appropriately processed for optimal fidelity. The resulting composite TM source signal is fed to the TM transmitter for transmission as an RF signal to the TM ground station.

d. Telemetry Transmitter (TM-TX). The TM-TX provides the functions required for RF transmission and includes components such as the RF modulator, amplifier, and antenna. The output of the TM-TX is an RF signal that conveys the composite TM source information to the ground for reception, demodulation, and transport to the required end points.

2.1.2 Common Telemetry RF Link

The common telemetry RF link provides the connectivity from the AIS to the TM ground station.

2.1.3 TM Ground Station

The functional blocks at the TM ground station include receiving antenna(s), TM receiver(s), and demodulator(s) as required to regenerate the source TM streams. The source TM streams, once they have been recovered from the RF link, are available for transport to the various end stations as required over the ground network.

2.1.4 Ground Network

The ground network provides distribution of the TM streams from the TM ground station to destinations that require the TM stream for analysis, storage, and monitoring.

a. CDH. The TM ground station is connected to the CDH. The function of the CDH is to forward the TM streams to the required end stations. The end stations can provide: recording capability (data recorder); analysis; post-processing (data processor); or transmission to off-range locations.

b. Data Processor. The data processor supports processing of the telemetry data and includes functions such as bit or frame synchronization, decryption/encryption, error correction algorithms, coding, and timing functions along with data reduction algorithms.

c. Data Recorder. The data recorder provides the capability to record telemetry data in support of store and forward or playback mission requirements.

d. Off-Range Data Transmission. The off-range data transmission facility allows the telemetry data to be transported to remote locations for monitoring or additional processing.

The number of destination points that exist on the ground network, and the potential requirement to forward the TM stream simultaneously to more than one destination point, reveals the requirement to support multicast transmission of the TM streams over the ground network. The ability to natively support multicast traffic is one feature that makes IP transport of TM streams very desirable.

2.1.5 Telemetry over IP

The TMoIP involves the transport of the TM streams in the ground network over a packet-switched network. Examples include TM stream transport from the TM ground station to off-range transmission, CDH to data recorder, etc. Use of the IP protocol as the packet network of choice facilitates using commercial switches and routers that are based on the IP protocol in the ground network.

Figure 2-2 shows a model for the transport of TMoIP in the ground network.

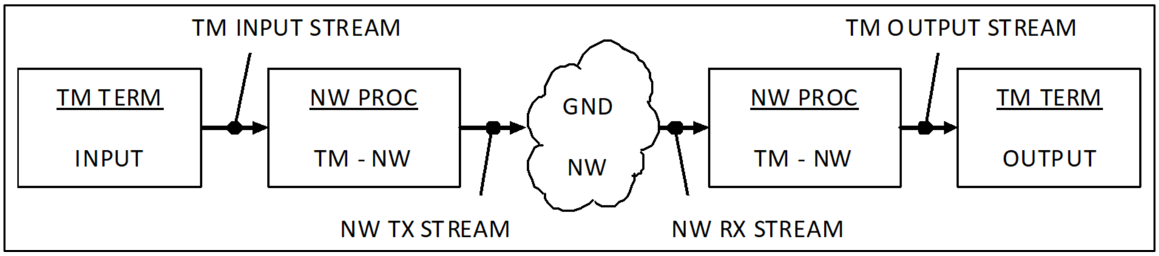

Figure 2-2. Ground Network Functional Blocks

There are three basic functional blocks associated with the ground network that participate in TM stream transport: the TM terminal, the network processor, and the ground network link.

a. TM Terminal (TM TERM). The TM TERM functional block provides connectivity to the native TM stream. At the ground network ingress, the TM terminal block provides the

TM input stream to the network processor. At the ground network egress, the network processor receives the network RX stream, generates the TM output stream, and sends it to the TM terminal.

b. Network Processor (NW PROC). The network processor provides the TMoIP functions to the ground network.

At the ingress to the ground network, the network processor receives the TM input stream and provides the required TMoIP formatting and adaptation to enable transport over the ground network. The end product of the network processor is the network transmit (NW TX) stream.

At the ground network egress, the network processor receives the TMoIP network receive (NW RX) stream and performs the inverse formatting process to recover the TM stream. An additional important function of the network processor at the ground network egress is to recover the TM clock information such that the TM output stream has timing characteristics identical to the TM input stream.

c. Ground Network Link (GND NW LINK). The ground network link provides the actual transport that carries the network stream between locations over a packet switched network.

The goal of the network processor and ground network is to provide seamless transport for the TM stream. Ideally, the TM input stream should be identical to the TM output stream except for the delay introduced by the transport process.

The following sections describe a number of implementations for ground network transport of native TM streams. This subsystem has evolved from dedicated point-to-point (fiber or microwave), proprietary solutions requiring a dedicated Digital Signal 3 (DS3) link (45 Mbps) to ATM-based solutions, and finally to the IP-based solutions that are currently implemented.

(1) Time-division multiplexing (TDM). The TDM transport formats the TM traffic as one or more bit streams. The TDM structure typically supports a number of simultaneous transmission channels, where the transmission link is divided into a fixed number of channels and each channel has a constant bandwidth. The timeslot for each individual channel is recurring and pre-allocated to that channel. Although TDM provides basic transport capability, current implementations are proprietary and do not lend themselves to multicast support. Further, the fixed bandwidth of TDM connections can result in inefficient bandwidth usage and stranded bandwidth if the traffic does not conform to the TDM link capacity.

(2) ATM. The ATM protocol formats data traffic into fixed-length (48 data bytes + 5 bytes of header) packets for transmission through the network. The ATM technology is connection-oriented, where a connection must be established between two endpoints before actual data transfer can begin. Support for multicast traffic is not an inherent part of the ATM protocol, and is dependent upon vendor implementation. The ATM protocol lends itself well to the transport of TM streams due to the following properties.

- Through the Circuit Emulation mechanism, ATM supports transport of TDM streams.

- The small fixed packet size produces minimal cell jitter.
- The ATM mechanism supports built-in Quality of Service (QoS) mechanisms to ensure timely packet delivery.

Additionally, ATM is well-suited for legacy range networks, such as Plesiochronous Digital Hierarchy or SONET. It also provides a straightforward migration for use in many existing range networks.

The ATM structure supports packet switching and QoS mechanism that ensure packet delivery. It is a connection-oriented protocol that requires connections to be configured prior to transmission.

(3) IP. This protocol is one where data traffic is formatted into variable-length packets, referred to as datagrams; however, in contrast to the ATM protocol, the packet size can vary from 64 to 1536 bytes.

NOTE	The IP documents use the term datagrams for the unit of exchange. In an effort to remain consistent with existing proposals for the transport of serial streams over IP networks (Pseudo Wire) and for the transport of TM streams over IP networks (Packet TM), the term packet will be used in this document to refer to the unit of exchange of TM traffic over IP networks.

The TM streams place strict requirements on delivery because they are real-time traffic streams; if a packet does not arrive to its endpoint in a known and dependable fashion, the data is lost. The support of the transport of real-time streams such as TM traffic over IP networks requires QoS mechanisms for IP networks and the support for these mechanisms in the end equipment. Recent developments in protocol extensions to IP to support QoS have produced a number of QoS mechanisms to support reliable delivery of TM traffic.

2.2 Motivation for TMoIP

There is a number of reasons and motivations for providing the capability to transport TM streams over IP networks. The IP technology is the packet technology of choice for a variety of networking uses, ranging from traditional data applications to real-time applications such as voice and video transport. With the maturation of the technologies that have enabled the transport of voice and video streams over IP networks, this same technology is envisioned to be applied to the transport of TM streams over IP networks.

Due to the proliferation of IP networking products and the associated economies of scale, performance has increased while equipment costs have decreased. Therefore, implementations of IP benefit from increased capabilities and lower costs.

Another benefit of TMoIP comes in the form of operational support. Since IP is very widespread, the skill set of the operators becomes less specialized to support one more capability over the ubiquitous IP network. An IP technology technician can be cross-trained on TM (as a new service) and support the TM mission in a relatively short amount of time. This approach addresses perhaps the single biggest issue facing range managers today: the turnover of qualified people supporting the mission.

In terms of mission management, transport technology has evolved from TDM solutions to ATM solutions. Although ATM has generated cost savings and also increased capability, ATM methods are perceived as complex. One reason for this is that ATM is a connection-oriented technology that requires that ATM connections be provisioned for each TM stream. In contrast, IP is a connectionless technology, meaning that no equipment configuration is required prior to transmission. Coupling the connectionless nature of IP with improved management tools that will become available as the commercial world advances will enable solutions like TMoIP to simplify the operational requirements of the networks and make them easier to deploy.

Applying the IP capability in the range and TM world is fairly uncomplicated. The support requirement is to link the receiving station to the end terminating station over a packet network. The operators still have the task to identify which resources to link together, but today this becomes an exercise in network management, for which there are tools becoming available that should make the effort straightforward.

Another motivation for migration to TMoIP is the native support of multicast traffic provided by the IP protocol. Multicast techniques support reception by multiple users without replicating the traffic to each user. Additionally, by using multicast techniques, a bandwidth-efficient scheme can be implemented to perform TMoIP transport. This scheme works as follows.

a. The NW TX stream is constructed to be a multicast IP stream. This construction essentially results in the generation of an IP stream with an address in a specific range, indicating that it is a multicast stream.

b. The TM terminals needing to receive the multicast stream notify their local IP switch or router that they want to receive the stream. Notification is made using an IP protocol called Internet Group Management Protocol[2] (IGMP), which provides mechanisms to support efficient transport of multicast traffic in IP networks (see Chapter 4).

c. When a switch or router receives a request from a TM terminal, it will forward the network RX packets that carry the TM stream to the TM terminal.

d. If a switch or router receives a multicast packet and there are no local or downstream TM terminals that want to receive it, the packet will not be forwarded. In this fashion, network bandwidth is only consumed when a TM terminal requires it; therefore, the need to build connections for every link is eliminated and the configuration is simplified.

2.3 Challenges for TMoIP

A number of technical requirements and challenges must be addressed in the TMoIP implementation before the advantages of IP network integration can be obtained.

2.3.1 Downlink Data Requirements

Downlink data may originate from a variety of sources, such as a launch vehicle, payload, aircraft, ship, and/or weapon platform. Downlink data requirements are fairly common

[2] Internet Engineering Task Force. "Internet Group Management Protocol, Version 3." RFC 3376. Updated by RFC 4604. October 2002. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc3376/.

across Department of Defense Services because the mission requirements have typically sent data in a serial stream; additionally, the timing source normally uses an on-board oscillator.

Downlink data is handled in several ways. Many operations require the recording of data at the first receiving site to preserve the data and to ensure all data is available. Other operations record at the data processing equipment location. Many missions support on-board recording for post-flight and only use the ground-based recording in case the on-board copy is corrupted. During a real-time test, there is typically no time or available bandwidth for re-transmission of errors.

Difficulties arise when transmitting downlink data across a network having different timing characteristics than those of the source TM stream. This problem has been the challenge with TM since the beginning of real-time mission support. The isochronous nature of the TM stream using the on-board oscillator can be exacerbated by a number of causes that can affect timing, including Doppler and multi-path effects. Given the critical nature of the timing information contained in the source TM stream, it is important that the TMoIP solution address the requirement to accurately and reliably transport and regenerate the source TM timing across the network.

The requirement for delay is very subjective. Most users will say “as fast as possible” without being able to quantify. Typically, the most stringent requirement on delay is either voice or range safety. Typical range safety requirements state that no more than one second shall pass between an event on the vehicle and the time the vehicle receives the flight termination signal, not counting three seconds allotted for human processing. This requirement often translates into a requirements allocation of 100 milliseconds for the transmission of data from the receiving station to the data processing building. In the case of voice, audio embedded in the TM stream is often used to communicate with the test personnel as a hot-microphone. If the TM transmission is delayed, an uncomfortable pause is noticed in the conversation and an echo is added that must be removed when the ultra-high frequency/very high frequency radio is used on the ground. Because echo cancellers can be used for the delay, the uncomfortable pause is the driving factor for a delay requirement that does not exceed 100 ms. Traditionally, the delay introduced by the transport process was mainly caused by stream processing and end-to-end transit time. As the IP protocol is packet-based, the conversion of the source TM streams to packets introduces an additional delay component that must be included in the total system delay. This packetization delay can be a significant component of the total system delay, especially at low TM rates.

Path-delay control mechanisms provide alignment of TM streams in the following scenarios.

a. A single TM stream enters the network at different points and is received at a single site. Due to the differential path delays, the multiple receive streams must be re-aligned.

b. A number of TM streams enter the network at different points and are received at a single site. Again, due to the different path delays, these streams must be aligned so that the data corresponds in time.

c. A number of TM streams of diverse rates enter the network and are received at a single site. Due to the differential delays introduced by packetizing each stream, the streams must be aligned to enable the data points to correspond in time.

Potentially the biggest issue with providing a successful TMoIP solution is that IP is a best-effort service without guaranteed service delivery. The lack of guaranteed delivery of TM packets can result in negative effects to clock regeneration and recovery. Those effects include packet jitter and network congestion, which cause out-of-order packets and packet loss. To enhance the network QoS for TMoIP, QoS mechanisms available in commercial off-the-shelf (COTS) network equipment are used. Providing guidance for the provision of effective QoS is an important part of the TMoIP solution. The subject of QoS support is addressed in detail in Chapter 4.

2.3.2 Uplink Command Requirements

Uplink commands are different from downlink commands because the data rate is typically much lower and the entire message must be received without a single bit error. The uplink data used for platform or payload reconfiguration is, in many cases, a pre-determined event that can be pre-loaded from the mission control computers to the RF uplink station. Therefore, the transport mechanism for uplink streams must support message validation and re-transmission. The implementation for message validation is reserved for the application layer.

2.3.3 System Management

System management in today's environment means selection of one of a number of options, including manual patch panels, DS3 cross-connect, and ATM connections. The use of TMoIP provides opportunities to simplify the provisioning control plane of the network by self-routing protocols available in every IP network today.

Local management operations provide the mechanism to provision and manage local end equipment. Remote management methods are employed in order to support management operations for equipment located at distant locations. In-band or out-of-band and management methods can be used with TMoIP to support provisioning, statistics, and fault management. Protocols such as Hypertext Transfer Protocol (HTTP)[3] and Simple Network Management Protocol (SNMP)[4] are available to provide the remote management capability.

[3] Internet Engineering Task Force. "Hypertext Transfer Protocol – HTTP/1.1." RFC 2616. June 1999. Obsoleted by RFC 7230, RFC 7231, RFC 7232, RFC 7233, RFC 7234, and RFC 7235. Retrieved 27 January 2020. Available at https://tools.ietf.org/html/rfc2616.

[4] Internet Engineering Task Force. "Simple Network Management Protocol (SNMP). RFC 1157. May 1990. May be superseded by update. Retrieved 2 January 2020. Available at https://datatracker.ietf.org/doc/rfc1157/.

CHAPTER 3

TMoIP Payload Construction

3.1 Overview/Management Elements

The preceding chapters discussed existing TM transport techniques and challenges for migration to using IP networks as a transport medium. In this and following chapters, the requirements for the implementation of a TMoIP solution are developed.

This chapter describes the TMoIP payload details. Chapter 4 defines management elements to enable status reporting, configuration, and integration with the end equipment that, with the TM terminal, comprises the ground network.

3.1.1 TMoIP payload

A payload structure is designed to provide sufficient flexibility to allow the user to optimize for payload efficiency and different network topologies, yet provide inter-working capability between different vendors.

3.1.2 TMoIP solution

The TMoIP solution includes management activities such as the following.

a. Addressing the requirement to accurately and reliably regenerate the source TM timing at the network receiver by including objective specifications for the performance of the clock regeneration function.

b. Recommending mechanisms to control path delay, as well as the capability to provide the alignment of TM streams.

c. Identifying and supporting a number of methods by which network equipment provides support for QoS, while allowing the user to provision the optimal QoS solution.

d. Including provisions for maintenance and management support. Both in-band and out-of-band methods will be defined. In-band methods support the requirement for status information to be transported concurrently with the TM traffic, and out-of-band methods provide the capability to provide extended management features.

In addition to the above management elements, Chapter 4 will address TMoIP implementation issues relating to network performance, reliability, and multicast traffic considerations.

3.2 High-Level Requirements (Concept of Operations)

Table 3-1 describes the major user operational requirements for a TMoIP system. These high-level requirements drive each of the detailed specification requirements discussed later in this document.

Table 3-1. High-Level Requirements

Req/Opt[1]	Requirement description
Req	Accurately and reliably transport and regenerate the source TM data and timing across the network.
Req	Support an Encode/Decode latency of less than 100 milliseconds for the TM input stream to the TM output stream for the following TM rates: 100 Kbps < TM Stream Rate < 35 Mbps
Req	Enable the use of QoS mechanisms that are available in COTS network equipment.
Req	The transport mechanism for uplink streams must support message validation and re-transmission.
Req	Support local and remote management mechanisms to provision and monitor the TMoIP equipment.

[1] Req = Required, Opt = Optional, Note = notes

NOTE In this standard, a series of requirements, options, and notes will indicate the elements that make up the TMoIP implementation. Note that "Req" indicates a required element for TMoIP, "Opt" indicates an optional element, and "Note" indicates notes, recommendations, and informational items.

3.3 OSI Layered Approach

The OSI protocols are a family of information exchange standards. The OSI model describes seven layers of interconnection: the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer.

For purposes of defining the TMoIP payload, this standard will identify the interface requirements as they relate to the OSI protocol layers for the TM TERM and NW PROC functional blocks that were defined within the ground network in Figure 2-2.

Figure 3-1 shows the OSI layer structure for the TM terminal and network processor functions for the TMoIP data plane. A red line traces the path of a source TM stream (TM input stream) from Layer 1 of the TM terminal to the network processor where ultimately the network TX stream is produced for transport via the IP network. Conversely, the green line is the path of the IP traffic (NW RX Stream) through the network processor to the TM terminal, where it finally appears as the TM output stream.

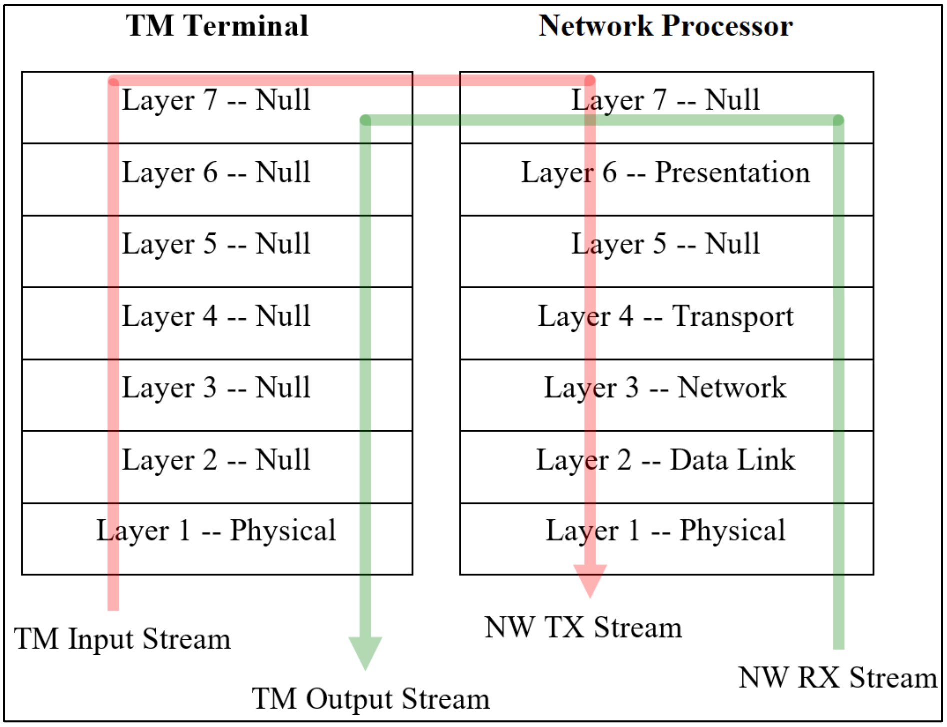

Figure 3-1. OSI Layers for TM Terminal and Network Processor

The TM terminal implements a single layer (Layer 1) in the OSI model, with Layer 2 through Layer 7 being null layers. The network processor implements Layer 6 and Layer 4 through Layer 1 of the OSI model, with Layer 5 and Layer 7 being null layers.

NOTE	This document cites a family of standards maintained by the Institute of Electrical and Electronics Engineers (IEEE). Each standard in the family, IEEE802, is available here.

Table 3-2 gives a brief description of each OSI protocol layer and the specific requirements for the TMoIP implementation as each relates to each of the OSI layers.

Table 3-2. TMoIP OSI Protocol Layer Implementation

Layer ID and Description	TM Terminal	Network Processor
Layer 7 - Application Provide user interface to network	Null layer	Null layer
Layer 6 - Presentation Data transformation such as encoding and encryption to provide standard application layer interface	Null layer	Stream-to-packet convergence
Layer 5 - Session Establish, manage, and terminate connections	Null layer	Null layer
Layer 4 - Transport	Null layer	UDP TCP

Provide link reliability, flow control, and error control		
Layer 3 - Network Data transport at network level, functions include routing	Null layer	IP IGMP
Layer 2 - Data Link Data transfer between network entities, detect and correct errors in Physical layer	Null layer	802.3 802.1.p 802.1Q
Layer 1 - Physical Defines physical interconnections and the electrical specification of the signals	TM stream physical interface TM stream electrical interface TM stream coding	10BASE-T, per 802.3i 10BASE-F, per 802.3j 100BASE-TX, per 802.3u 100BASE-FX, per 802.3u 1000BASE-X, per 802.3z 1000BASE-T, per 802.3ab

3.4 OSI Protocol Layer Implementation: TM Terminal

3.4.1 Layer 1

Layer 1, the physical layer, provides the electrical and mechanical interface for the TM input stream and the TM output stream from the TM terminal to the network processor.

The Layer 1 properties include physical, electrical, and signal encoding interfaces. The range and scope of these properties preclude their inclusion in the body of the TMoIP protocol document. Appendix A provides a set of guidelines to promote interoperability and to provide a baseline interface definition.

3.4.2 Layers 2 – 7

The remaining TM terminal layers are null layers, meaning that no processing is performed and no overhead is added. The application layer (Layer 7) will provide connectivity of the TM stream to the OSI protocol stack for the network processor.

3.5 OSI Protocol Layer Implementation: Network Processor

3.5.1 Layer 7 – Application

The application layer in the network processor is a null layer and provides the TM stream interface to the TM terminal.

3.5.2 Layer 6 – Presentation

Layer 6 provides data transformation and conversion functionality. In the TMoIP solution, this layer provides the payload convergence function that enables the TM stream to be carried over packet networks.

a. Payload Convergence. The payload convergence function converts the serial TM stream into a format compatible with transport over packet-switched networks. As the implementation described is similar to the scheme used in Pseudo Wire emulation techniques for the emulation of serial services over packet switched networks, the nomenclature used in the description of Pseudo Wire implementations will be used (Pseudo Wire_1[5], Pseudo Wire_2[6], and Pseudo Wire_3[7]).

The payload convergence sub-layer provides the following functions.

(1) TM stream format conversion from a serial stream into a packet format. The resulting packet will be referred to as the raw packet payload.

(2) Appending of TMoIP control word to the raw packet payload.

The resulting structure will be referred to as the TMoIP payload. Figure 3-2 shows the format for a TMoIP payload.

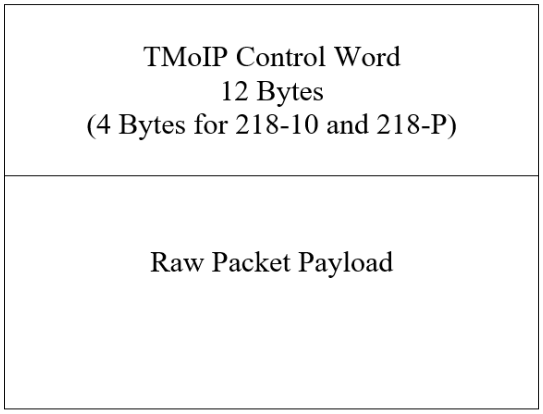

Figure 3-2. TMoIP Layer 6 implementation

b. TMoIP Control Word Format. The TMoIP control word is pre-pended to the raw packet payload and supports the following functions.

(1) Detection of packet loss or packets out of order

(2) Identify TMoIP version

i. Legacy version 218-10

1. Ability to identify failures in local TM interface

2. Fault signaling capability across the network

ii. Proprietary 218-P, vendor variants of 218-10 (including proprietary use bits)

iii. Current version 218-20

1. Payload shaping with frame sync status and fragmentation

2. Timestamp and time source reference

[5] Internet Engineering Task Force. "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture." RFC 3985. Updated by RFC 5462. March 2005. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc3985/.

[6] Internet Engineering Task Force. "Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)." RFC 3916. September 2004. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc3916/.

[7] Internet Engineering Task Force. "Structure Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)." RFC 4553. June 2006. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc4553/.

NOTE	The 64-bit timestamp increases the TMoIP control word to 12 bytes from 4 bytes in legacy versions 218-10 and 218-P.

The intents of this update are to eliminate unused flag bits from previous versions, provide options for payload shaping, and timestamp the first bit of the TM data in the raw packet payload. Through interaction with ranges and vendors, it was determined that the alarm bits and length field identified in 218-10 were unused and unnecessary, so they were removed.

Payload shaping was added to provide the ability to fill the raw packet payload with an intact TM minor frame (see IRIG 106 Chapter 4[8]) or a data quality (DQE) frame (see IRIG 106 Chapter 2 Appendix G[9]). In the case of payload shaping for a TM minor frame, flag bits are available to pass minor and major frame sync status. Packets with maximum transmission unit (MTU) larger than any hop on the network risk being dropped rather than fragmented. The IP header provides flag bits to identify fragmented packets and should be checked by the receiving system. Network devices may be configured to drop large packets rather than fragment them; therefore, the MTU should be configured to stay under the network's smallest MTU, which may be reduced further from encrypted tunneling methods such as Internet Protocol Security (IPSec). For the use case where one may want to send a shaped payload larger than the appropriate MTU, a flag bit is provided to indicate whether the incoming packet is the first of a fragmented payload or a subsequent payload fragment. The intent of this flag is to help receiving devices identify the packet expected to carry the frame sync pattern or data quality metric bits.

A Precision Time Protocol (PTP)-based, 64-bit timestamp was added to provide time information for when the first bit of the TM data in the raw packet payload was received by the ground station TM terminal. The timestamp provides nanosecond precision and is based on the 00:00 January 1, 1970 epoch. With the goal of driving ranges toward 1588 PTP timing, but recognizing the current state of that migration, a flag bit identifies whether the timestamp source reference is based on Universal Coordinated Time or International Atomic Time. Since there may be mixed time source environments, the system receiving and processing the TMoIP will be responsible for accounting for leap seconds as needed.

Figure 3-3 shows the format of the TMoIP 218-10 control word.

VER	L	R	M	RES	LEN	SEQ NUMBER

Figure 3-3. TMoIP 218-10 Control Word

[8] Range Commanders Council. "Pulse Code Modulation Standards" in *Telemetry Standards*. Chapter 4. IRIG 106-19. July 2019. May be superseded by update. Retrieved 27 January 2020. Available at https://www.wsmr.army.mil/RCCsite/Documents/106-19_Telemetry_Standards/chapter4.pdf.

[9] Range Commanders Council. "Standards for Data Quality Metrics and Data Quality Encapsulation" in *Telemetry Standards*. Chapter 2 Appendix 2-G. IRIG 106-19. July 2019. May be superseded by update. Retrieved 27 January 2020. Available at https://www.wsmr.army.mil/RCCsite/Documents/106-19_Telemetry_Standards/chapter2.pdf.

Table 3-3 defines the TMoIP 218-10 Control Word fields.

Table 3-3. TMoIP 218-10 Control Word

Field	Bits	Description
VER	4	Version identifier “0000” indicates legacy version 218-10
L	1	Local Defect Alarm, indicates local circuit fault in the TM stream
R	1	Remote Defect Alarm, indicates remote circuit fault in the TM stream
M	2	Local Defect Alarm Modifier
RES	2	Reserved
LEN	6	If non-zero, LEN indicates TMoIP payload length, defined as the TMoIP control word + raw packet payload. If zero, LEN indicates TMoIP payload length greater than 63 bytes. In this case the TMoIP payload length is determined via length fields in lower protocol layers.
SEQ NUMBER	16	Sequence Number

Req The TMoIP raw packet size shall be user configurable.

Opt The TMoIP raw payload size may be auto-configurable, based on user priorities (e.g., stream/delay characteristics).

Req The minimum TMoIP raw packet size = 1 byte.

a. To limit the effects of Ethernet fragmentation, the final Layer 2/3/4/6 packet size should be less than the Ethernet MTU.
b. Padding may be required to meet the minimum Ethernet MTU size.

Figure 3-4 shows the format of the TMoIP 218-P control word.

VER	PDB	SEQ NUMBER

Figure 3-4. TMoIP 218-P Control Word

Table 3-4 defines the TMoIP 218-P Control Word fields.

Table 3-4. TMoIP 218-P Control Word

Field	Bits	Description
VER	4	Version identifier “0001” indicates proprietary variants of 218-10
PDB	12	Proprietary defined bits
SEQ NUMBER	16	Sequence number

This version allows vendors who created modified versions of 218-10 to maintain functionality. Due to variances in implementation, use of this version is not recommended in mixed-vendor environments.

Figure 3-5 shows the format of the TMoIP 218-20 control word.

VER	**PLD**	**mFSS**	**MFSS**	**FRG**	**RES**	**TSR**	**SEQ NUMBER**	**TIMESTAMP**

Figure 3-5. TMoIP 218-20 Control Word

Table 3-5 defines the TMoIP 218-20 Control Word fields.

Table 3-5. TMoIP 218-20 Control Word

Field	Bits	Description
VER	4	Version identifier "0010" indicates 218-20
PLD	2	Payload type "00" indicates no frame alignment "01" indicates PCM frame aligned, first or only packet "10" indicates DQE frame aligned, first or only packet "11" indicates frame aligned, continuation packet
mFSS	2	Minor Frame Sync Status (not applicable for PLD = "00") "00" indicates Search "01" indicates Check "10" indicates Lock "11" indicates Flywheel
MFSS	2	Major Frame Sync Status (not applicable for PLD = "00") "00" indicates Search "01" indicates Check "10" indicates Lock "11" indicates Flywheel
RES	5	Reserved
TSR	1	Timestamp Source Reference "0" indicates Universal Coordinated Time "1" indicates International Atomic Time
SEQ NUMBER	16	Sequence Number
TIMESTAMP	64	64-bit Timestamp – PTP format. See Figure 3-6. 32-bit seconds field 2-bit Reserved 30-bit nanoseconds field Prime epoch 00:00 01 Jan 1970

Req The TMoIP raw packet size shall be user configurable.

Req The TMoIP raw payload size shall be auto-configurable or user-configurable, based on user priorities (e.g. stream/delay characteristics).

Req The minimum TMoIP raw packet size = 1 byte.

Req The timestamp marks the time the ingest system receives the first TM payload data (not 218 or DQE header) bit.

Req Bit rates and changes in bit rates shall be calculated using packet timestamps and algorithms. For compliance, no proprietary packets or bits shall be used.

a. To limit the effects of Ethernet fragmentation, the final Layer 2/3/4/6 packet size should be less than the Ethernet MTU of the network path.
b. Padding may be required to meet the minimum Ethernet MTU size.
c. For large frame aligned payloads that exceed the configured MTU of the ingest system, the payload will need to overflow into one or more continuation packets.
d. Packets larger than network MTU will result in IP fragmentation or dropped packets. Observe the Flags and Fragment Offset fields in the IP header to aid in reassembling large packets fragmented and not reassembled by the network.
e. The raw packet payload may contain data quality metric bits and should not be inverted. Any requirement to invert TM stream bits should be handled prior to DQE.

<table>
<tr><td>31</td><td>30</td><td>29</td><td>28</td><td>27</td><td>26</td><td>25</td><td>24</td><td>23</td><td>22</td><td>21</td><td>20</td><td>19</td><td>18</td><td>17</td><td>16</td><td>15</td><td>14</td><td>13</td><td>12</td><td>11</td><td>10</td><td>09</td><td>08</td><td>07</td><td>06</td><td>05</td><td>04</td><td>03</td><td>02</td><td>01</td><td>00</td></tr>
<tr><td colspan="4">VER</td><td colspan="2">PLD</td><td colspan="2">mFSS</td><td colspan="2">MFSS</td><td>FRG</td><td colspan="4">RES</td><td>TSR</td><td colspan="16">SEQ NUMBER</td></tr>
<tr><td colspan="32">TIMESTAMP [seconds]</td></tr>
<tr><td colspan="2">RES</td><td colspan="30">TIMESTAMP [nanoseconds]</td></tr>
</table>

Figure 3-6. TMoIP 218-20 Control Word (12-Byte Detail)

c. Packet Size. A number of considerations drive the choice of packet size. Table 3-6 illustrates the operational tradeoffs between small packet size and large packet size.

Table 3-6. Packet Size Tradeoffs

Small Packet	Large Packet
High Overhead	Low Overhead
Low Latency	High Latency
Low Delay Variation	
High sample resolution for clock recovery	

From Table 3-6, it would appear that small packets have superior operational characteristics as compared to large packets; however, the benefits of lower latency and delay variation advantages are diminished for high bit rate TM streams greater than 1 Mbps. The advantage is reduced because the packetizing latency decreases as the bit rate of the TM stream increases. In such cases, the desirability for the use of large packets (and the reduced overhead that they incur) increases. It is thus concluded that some user control of the packet size shall be supported to provide the user the ability to optimize system performance.

NOTE Support for packet designs that simplify inter-working with alternate protocols may be included. One example is to provide the capability to generate packets that can be efficiently packed into Multi-Protocol-Over-ATM (Request For Comments [RFC] 2684[10]) cells.

Packet length will be revisited upon definition of the balance of the protocol layers.

[10] IETF. "Multiprotocol Encapsulation over ATM Adaptation Layer 5." RFC 2684. May be superseded or updated. September 1999. Retrieved 22 July 2019. Available at https://datatracker.ietf.org/doc/rfc2684/.

d. Timing. In addition to the payload convergence function, the TMoIP implementation must support timing functions that result in the accurate regeneration of the TM stream timing characteristics at the receive interface.

In these cases, the receive interface must regenerate the native TM stream as it was inserted to the network at the transmit interface. Therefore, two timing-related design mechanisms to be considered are clock recovery and timed payload delivery.

(1) Clock Recovery. Clock recovery is the extraction of output transmission bit timing information from the delivered packet stream. The TMoIP stream carries the timing information natively, but extracting timing from a highly jittered source requires an algorithm that reproduces the source TM clock with the required accuracy and dynamic characteristics. To ensure interoperability between the transmit interface and the receive interface for native TM stream bitrate changes, clock recovery shall be derived from the incoming 218-20 (and onward) packet flow using timestamp information. Table 3-7 identifies a set of clock recovery requirements.

Table 3-7. Clock Recovery

Required/ Optional	Comment			
Req	Adaptive clock recovery support is required for TM clock regeneration			
Req	Bit rates and changes in bit rates shall be calculated using packet timestamps and algorithms. For compliance, no proprietary packets or bits shall be used.			
Req	The clock recovery algorithm must display the following performance characteristics:			
	Spec	**Min**	**Max**	**Notes**
	Jitter			Per IRIG 106 Chapter 4
	Wander			Per IRIG 106 Chapter 4
	Acquisition Time		N/A	TM stream rate ≤ 64 Kbps
	Acquisition Time		2 sec	TM stream rate > 64 Kbps Acquire to ± 500 ppm from stream resynchronization

NOTE	The parameters and requirements for acquisition time are items for further study and will be updated in future revisions of this document.

(2) Timed Delivery. For the TMoIP function, timed delivery is the ability to control the relative phase (skew) of more than one TM stream at the output interface. This function allows the user to perform temporal alignment of the recovered streams and equalize any delays incurred by packetizing time or network transmission time. Some situations where temporal re-alignment of TM streams is required are as follows.

- A single TM stream enters the network at different points and is received at a single site. Due to the differential path delays, the multiple receive streams must be re-aligned.

- A number of TM streams enter the network at different points and are received at a single site. Again, due to the different path delays, these streams must be aligned so that the data corresponds in time.
- A number of TM streams of diverse rates enter the network and are received at a single site. Due to the differential delays in stream packetization, the streams must be aligned to enable the data points to correspond in time.

Opt	Support for timed delivery is optional at this time, but equipment vendors are urged to consider implementation of this feature in their equipment.

3.5.3 Layer 5 (Null)

3.5.4 Layer 4 - Transport

Layer 4 defines mechanisms for providing end-to-end communication control in order to ensure reliable transport of data across the network.

a. User Datagram Protocol (UDP). In the TMoIP implementation, the UDP[11] provides a datagram mode of transport of TM streams over a packet-switched network. This protocol assumes that IP is used as the underlying protocol. The UDP header is appended to the TMoIP Layer 6 payload, and consists of eight bytes. Figure 3-7 shows the TMoIP packet with the UDP header added. The un-shaded block is the overhead added by the UDP header.

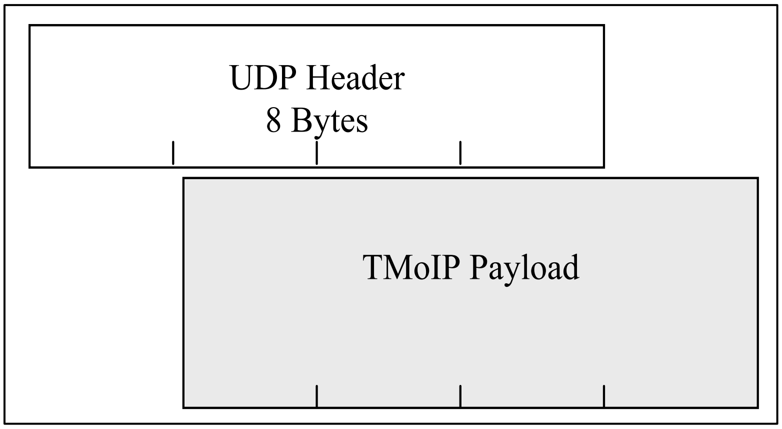

Figure 3-7. TMoIP Layer 4 - Layer 6 implementation

Table 3-8 describes the UDP header fields.

Table 3-8. UDP Header Field Descriptions

Field	Length	Description
Source Port	2	Port number of sending process
Destination Port	2	Port number of receiving process
UDP Length	2	Length of UDP datagram

[11] IETF. "User Datagram Protocol." RFC 768. 28 August 1980. May be superseded or amended by update. Retrieved 7 May 2019. Available at https://datatracker.ietf.org/doc/rfc768/.

UDP Checksum	2	Checksum of UDP header + data

Table 3-9 describes the UDP Header field requirements for TMoIP.

Table 3-9. UDP Header Field Requirements

Field	Notes
Source Port	Provide ability for user to modify
Destination Port	Provide ability for user to modify
UDP Length	Calculated value
UDP Checksum	Calculated value

The UDP protocol provides the following functions.

(1) Check-summing of the packet for error detection.

(2) Support for stream multiplexing. The UDP port is used to support the multiplexing of traffic to a host. In the TMoIP implementation, the UDP port can be used to multiplex the following stream types.

- o Individual TM input/output streams, which can be multiplexed by assigning a different UDP port to each stream.
- o Management streams, which can be differentiated from TM stream traffic by assigning them to a specific UDP port. The UDP port numbers are managed by the Internet Assigned Numbers Authority (IANA). The port numbers are divided into three ranges named the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports, described as follows.
    - ▪ The Well Known Ports are those from 0 through 1023. These ports should not be used without IANA registration.
    - ▪ The Registered Ports are those from 1024 through 49151. These ports should not be used without IANA registration.
    - ▪ The Dynamic and/or Private Ports are those from 49152 through 65535, and are available for use by private individuals.

Req	The TMoIP implementation shall support UDP.

Opt	The TMoIP implementation may provide the capability to assign a separate UDP port to each TM stream.

Opt	The TMoIP implementation may provide the capability to assign a separate UDP port to management streams.

Req	The TMoIP implementation shall support the use of UDP ports 49152 through 65535.

b. Transmission Control Protocol (TCP). An alternate Layer 4 protocol is TCP.[12] In contrast to UDP, TCP provides reliable end-to-end packet delivery using a structured send/receive protocol that includes the acknowledgement of data packets. If a lost packet is detected during transmission, the packet is re-transmitted. While this mechanism works well for the delivery of data traffic without strict timing requirements, it does not lend itself well to the transmission of real-time traffic. This is because the time it takes for packet retransmission exceeds the delivery requirements for most real-time streams. Additionally, TCP is a point-to-point protocol and does not support multicast traffic.

NOTE	Implementation of TCP may be considered in future versions of the TMoIP standard.

3.5.5 Layer 3

Layer 3 provides routing functionality across a sub-network. The TMoIP packet will use the IP protocol as the layer 3 mechanism.[13]

The IP header is appended to the TMoIP Layer 4/Layer 6 payload, and consists of 20 bytes. Figure 3-8 shows the TMoIP packet with the IP header added. The un-shaded block is the overhead added by the IP protocol layer.

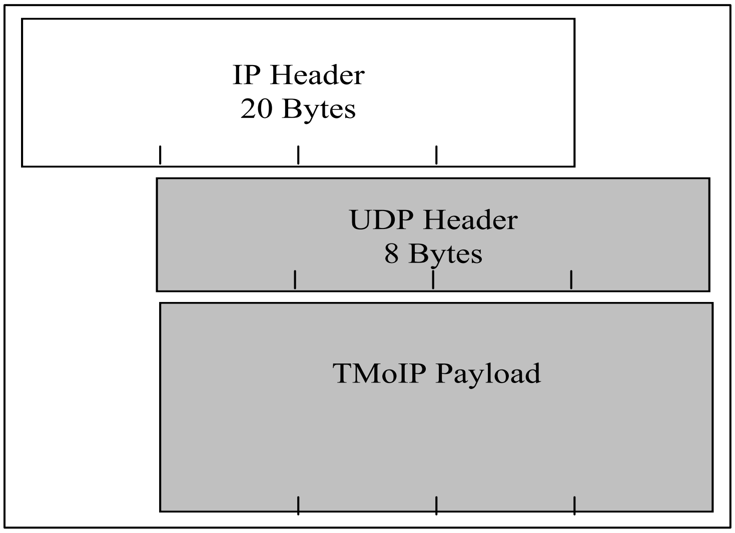

Figure 3-8. TMoIP Layer 3 - Layer 6 Implementation

Table 3-10 describes the IP header fields.

Table 3-10. IP Header Field Descriptions

Field	Length	Description
Version	1	Bits 0 – 3 = Version

[12] IETF. “DoD Standard – Transmission Control Protocol.” RFC 761. Obsoleted by RFC 793 and RFC 7805. January 1980. Retrieved 22 July 2019. Available at https://datatracker.ietf.org/doc/rfc761/.

[13] IETF. “Internet Protocol.” RFC 791. Updated by RFC 2474, RFC 6864, and RFC 1349. September 1981. Retrieved 16 April 2019. Available at https://datatracker.ietf.org/doc/rfc791/.

Header Length		Bits 4 – 7 = IP header length
Type of Service (ToS)	1	Set QoS for particular type of traffic
Total Length	2	Total length of IP packet
ID	2	16-bit ID
Flags Fragment Offset	2	Bits 0 – 3 = flags Bits 4 – 15 = Fragment Offset
Time to Live	1	Number of hops that a packet can travel before being discarded by a router
Protocol Type	1	Protocol, as defined by IANA registry
Header Checksum	2	IP header cyclic redundancy check
Source Address	4	Source IP address
Destination Address	4	Destination IP address

Table 3-11 describes IPv4 Header field requirements for TMoIP.

Table 3-11. IPv4 Header Field Requirements

Field	Notes
Version, Header Length	Code to 0x45 to support IPv4, header length of 20 bytes
Type of Service	Provide ability for user to modify
Total Length	Calculated value
ID	Can be automatically generated or provide user ability to modify
Flags, Fragment Offset	Can be automatically generated or provide user ability to modify
Time to Live	Can be automatically generated or provide user ability to modify
Protocol Type	Code to 0x11 for UDP
Header Checksum	Calculated value
Source Address	Can be automatically generated or provide user ability to modify
Destination Address	Provide ability for user to modify

A key function of the Layer 3 protocol is to provide capability for the transfer of packets between network processors located in the ground network. Each network processor is identified by its IP address. When a packet is prepared for transmission, the IP address of the sending network processor is placed into the Source Address field, and the IP address of the target network processor is placed in the Destination Address field. The intervening network (i.e., the ground network in the case of the TMoIP implementation) will enable the delivery of the packet based upon the destination IP address contained in the packet.

There are three types of IP addresses:

a. Unicast. Unicast addresses are used for traffic destined for a single host;

b. Broadcast. Broadcast addresses are for traffic destined for all hosts on a given network;

c. Multicast. Multicast addresses are used for traffic destined for a set of hosts that belong to a multicast group.

The TMoIP implementation will support unicast and multicast addresses.[14]

The IP address used in multicast operation is called the multicast group address, and has a specific format that includes the multicast group ID. By joining a particular multicast group, a network processor can listen to a multicast address and decode the TM stream being sent to that multicast group. There is no restriction for the number of hosts in a group, so an unrestricted number of network processors can potentially decode a single TM stream.

Req	The TMoIP implementation shall support unicast and multicast IP addresses.

Opt	The TMoIP implementation may provide the capability to assign a separate IP address to each TM stream.

3.5.6 Layer 2

Layer 2 is responsible for packaging raw bits from the physical layer into frames and for transporting the frames from one host to another. The TMoIP implementation will use the 802.3 (Ethernet) Layer 2 protocol (IEEE 802.3). The Ethernet protocol is the dominant Layer 2 protocol in use in IP networks.

The Ethernet overhead consists of header and trailer information that is added to the TMoIP Layer3/Layer 4/Layer 6 payload, and consists of a total of 22 bytes. Figure 3-9 shows the Layer 2 through Layer 6 TMoIP implementation. The un-shaded blocks are the overhead added by the Layer 2 protocol.

[14] IETF. “Host Extensions for IP Multicasting.” RFC 1112. Updated by RFC 2236. August 1989. Retrieved 22 July 2019. Available at https://datatracker.ietf.org/doc/rfc1112/.

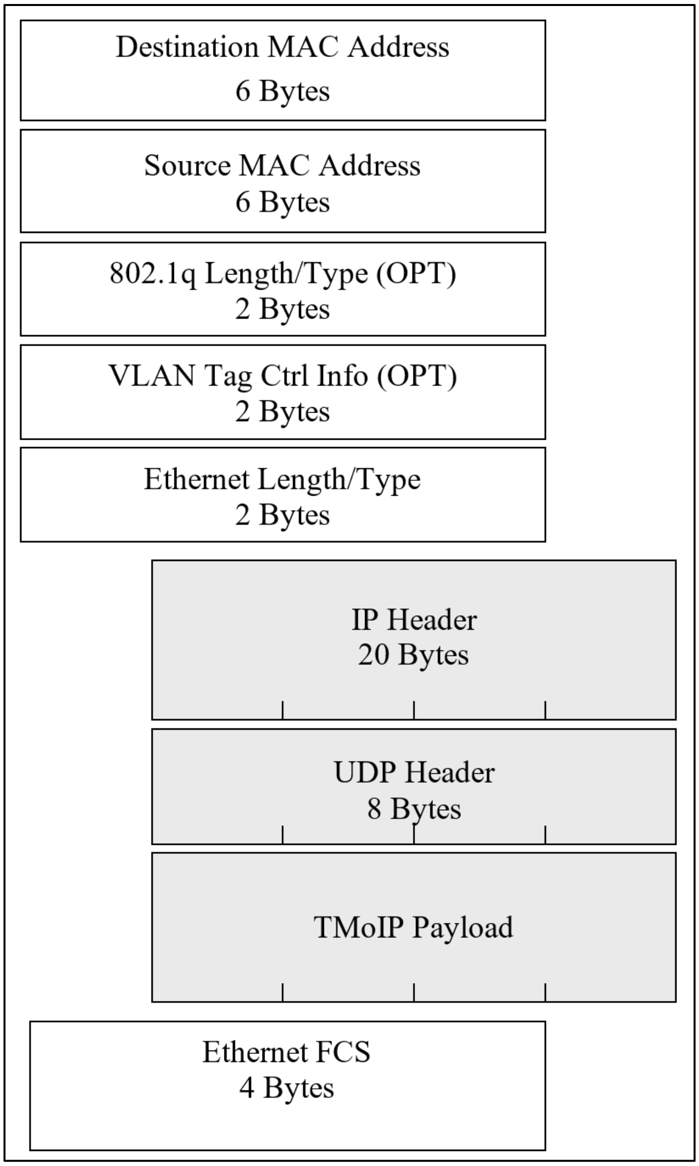

Figure 3-9. TMoIP Layer 2 - Layer 6 Implementation

Table 3-12 describes the Ethernet overhead fields.

Table 3-12. Ethernet Overhead Fields

Field	Length	Description	
Ethernet Dest Addr	6	Destination Address	
Ethernet Src Addr	6	Source Address	
802.1Q Length/Type	2	Indicates that the frame contains virtual local area network (VLAN) tagging	
VLAN Tag Ctrl Info	2	Bit	Description
		0 - 2	User Priority Field
		3	Canonical Format Indicator (CFI)
		4 - 15	VLAN Identifier (VID)

Length/Type	2	Set to 0x0800 (IPv4)
Ethernet FCS	4	Ethernet Frame Check Sequence, typically generated by Ethernet physical layer chip

The TMoIP requirements for the Ethernet overhead fields are described in Table 3-13.

Table 3-13. Ethernet Overhead Field Requirements

Field	Notes
Ethernet Dest Addr	Provide ability for user to modify (Opt)
Ethernet Src Addr	Fixed by host hardware
802.1Q Length/Type	Set to 0x8100 to indicate VLAN tag present if used
VLAN Tag Ctrl Info	Provide ability for user to modify
Length/Type	Set to 0x8000 (IPv4)
Ethernet FCS	Calculated value

The 802.1Q Length/Type and VLAN Tag Ctrl Information fields provide support for IEEE 802.1Q functionality. This 4-byte field, frequently referred to as the VLAN tag, is inserted into the Ethernet frame between the Ethernet Src Addr field and the Length/Type field. The first two bytes consist of the 802.1Q Length/Type field and are set to a value of 0x8100 that indicates the presence of the VLAN tag. The last two bytes of the VLAN tag contain the following information.

a. The first 3 bits are a user priority field that may be used to assign a priority level to the Ethernet frame.

b. The next bit is a CFI used in Ethernet frames to indicate the presence of a routing information field.

c. The last 12 bits are the VID that uniquely identifies the VLAN to which the Ethernet frame belongs.

The IEEE 802.1Q standard allows the transport of separate network streams over a common physical link. In the TMoIP implementation, the VID provides the capability to assign TM streams to a VLAN and provide switching capability based upon the VLAN.

The user priority field provides mechanism for implementing QoS, as defined by the IEEE 802.1p standard. This 3-bit field supports eight different service classes. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE, however, has made some broad recommendations.

Opt	The user shall be capable of assigning the Ethernet destination address.

Opt	The TMoIP implementation may provide the capability to assign a separate VID to each TM stream.

Opt	The TMoIP implementation may provide the capability to assign the User Priority field (802.1p) to each stream.

3.5.7 Layer 1

Layer 1 is responsible for connection to the transmission media and defines physical interconnections and the electrical specification of the signals.

The TMoIP implementation will include physical layer mechanisms associated with Ethernet (IEEE 802.3). A number of implementations exist for Layer 1 transport of native Ethernet traffic.

Req	The following Layer 1 interfaces shall be supported as shown in Table 3-14.

Table 3-14. TMoIP Layer 1 Requirements

Reference	Description	Standard	Support
100BASE-TX	100 Mbps over copper/twisted pair	802.3u	Required
100BASE-FX	100 Mbps over fiber	802.3u	Optional
10BASE-T	10 Mbps over copper/twisted pair	802.3i	Optional
10BASE-F	10 Mbps over fiber	802.3j	Optional
1000BASE-X	Gigabit Ethernet over fiber at 1000 Mbps	802.3z	Optional
1000BASE-T	Gigabit Ethernet over twisted pair at 1000 Mbps	802.3ab	Optional

NOTE	To provide user flexibility, this standard recommends that support for Gigabit Interface Converter/Small Form-factor Pluggable connector interfaces be included in TMoIP equipment that implements fiber optic interfaces.

NOTE	The recommended fiber interface connector types are the SC style (referred to as a subscriber connector, a square connector, or as a standard connector) and the LC style (referred to as a Lucent connector or as a local connector)

3.6 TMoIP Packet Design Summary and Discussion

Figure 3-10 shows the TMoIP packet layout. Each protocol layer adds overhead information to the TMoIP payload, resulting in the final TMoIP packet configuration.

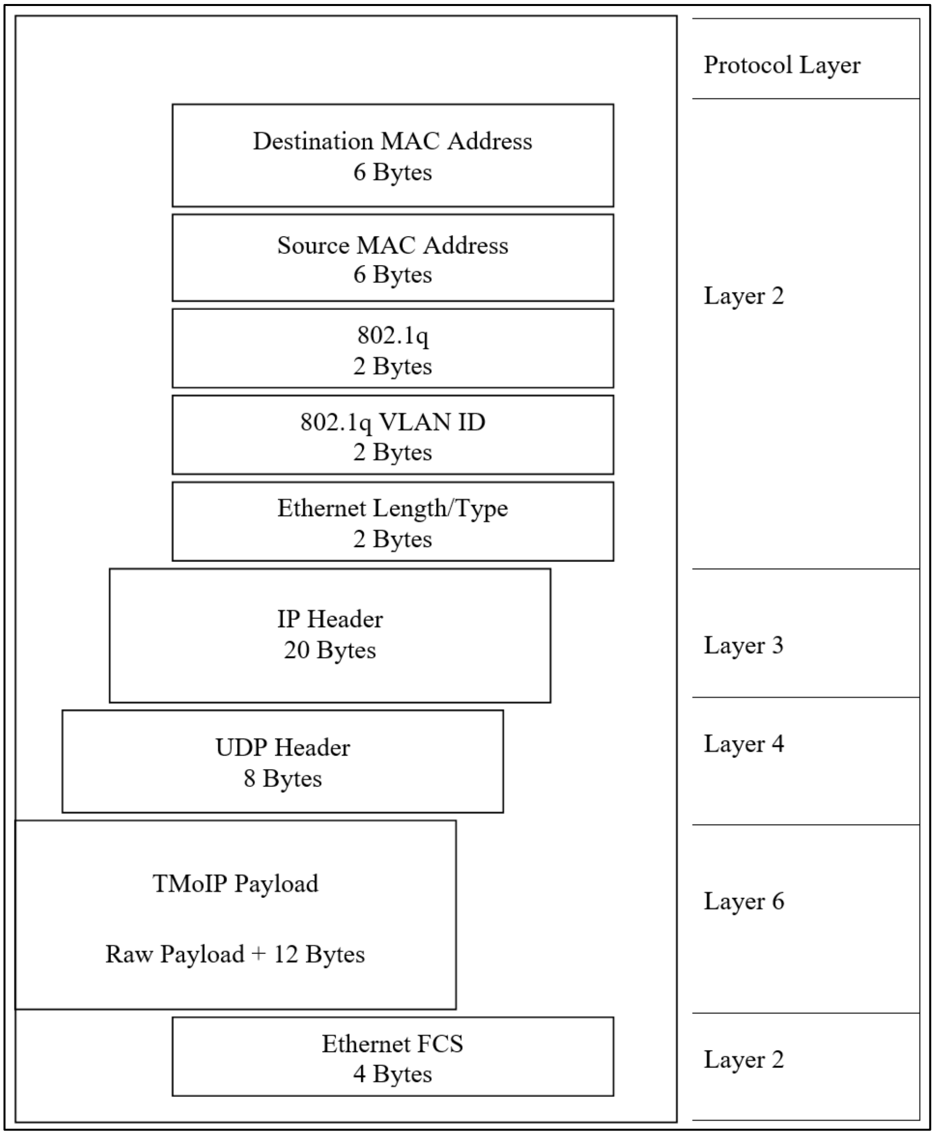

Figure 3-10. TMoIP Packet Layout

Table 3-15 summarizes the field descriptions for the TMoIP packet.

Table 3-15. TMoIP Packet Summary

Field	Description		Length	P/C/F (1)
Ethernet Dest Addr	Identifies station(s) to receive frame		6	P/C
Ethernet Src Addr	Identifies station that originated frame		6	C
802.1Q Length/Type	VLAN tag length/type		2	F = 0x8100
VLAN Tag Ctrl Info	Bit	Description	2	
	0 - 2	User Priority field		P
	3	CFI		F = 0
	4 - 15	VID		P
Length/Type			2	F = 0x0800
IP Header	Byte	Description		

	0	Version + IP header length	1	F = 0x45
20 Bytes Total	1	ToS	1	P
	2 - 3	Total length of IP packet	2	C
	4 - 5	16 bit ID	2	C/F
	6 - 7	Flags + Fragment Offset	2	F
	8	TTL	1	F/P
	9	Protocol (UDP)	1	F = 0x11
	10 - 11	IP Header checksum	2	C
	12 - 15	Source IP address	4	P/C
	18 - 19	Destination IP address	4	P
UDP Header	Byte	Description		
	0 - 1	Source Port	2	P
8 Bytes Total	2 - 3	Destination Port	2	P
	4 - 5	UDP Length	2	C
	6 - 7	UDP Checksum	2	C
TMoIP Payload	TMoIP Control Word		Note [2]	C
	TM Raw Packet Data		Note [3]	C
Ethernet FCS	Ethernet Frame Check Sequence		4	C

1. P = Programmable by user, C = Calculated or placed in packet without user intervention, and F = Fixed.
2. 12 bytes for 218-20. 4 bytes for legacy 218-10 and 218-P.
3. Refer to packet discussion.
4. The following packet constraint considerations have been identified.
   - In the absence of jumbo frame network support, the maximum Ethernet PDU maximum size should be 1500 bytes.
   - The VPNs such as IPSec can reduce the usable MTU below 1500 bytes.
   - Total packet overhead for Layer 2, Layer 3, and Layer 4 is 46 bytes without 802.1Q tagging support, and 50 bytes with 802.1 tagging support.

Table 3-16 shows a number of possible packet sizes. The larger packet sizes optimize the required overhead, and the smaller packet sizes optimize delay and tolerance to errors in the network.

Table 3-16. Sample Payload Calculations

Overhead			TMoIP Payload [1]	Total Payload [2]	Overhead
L2	L3	L4			
22	20	8	76	126	49%
22	20	8	140	190	33%
22	20	8	268	318	19%
22	20	8	524	574	11%
22	20	8	1036	1086	6%

[1] TMoIP payload includes the raw TM payload plus 12 bytes for the TMoIP control word.

[2] The total payload includes the TM payload with the Layer 2, Layer 3, and Layer 4 overhead included. The Layer 2 payload includes support for VLAN overhead.

CHAPTER 4

TMoIP Management

The topics in this chapter consider management level considerations, many of which are implemented in the ground network link and associated end equipment.

4.1 Management Mechanisms

Management capabilities will provide the ability to provision, monitor performance, and manage faults. The management operation can be performed locally or remotely.

Local management supports direct access and provisioning of the network processor. Examples of local management include console interfaces, typically implemented using RS-232 or Ethernet connectivity coupled with command line interface (CLI) or menu-driven user interfaces.

Remote management provides the capability to provision and manage the network processor when it is located in remote locations in the ground network. Examples of remote management configurations in the TCP/IP environment include CLI via the Secure Shell (SSH) application, browser-based applications using HTTP Secure (HTTPS) (Secure Socket Layer), and SNMPv3.

In-band management provides the capability to manage the network processor via the main traffic-bearing interface. Examples of in-band management are management via a separate Layer 2 connection such as an IEEE 802.1q VLAN or a separate Layer 3 IP address.

Implementation of protocols such as eXtensible Markup Language for integration with higher-level management or data collection domains is left to the discretion of the vendor.

Table 4-1 describes the various requirements and optional features for TMoIP management mechanisms.

Table 4-1. Management Mechanisms

Req/Opt[(1)]	**Requirement description**
Req	The TM terminals shall provide a mechanism to support local management functionality.
Req	The TM terminals shall provide a mechanism to support remote management functionality.
Req	Remote management of TM terminals shall provide the SSHv2 protocol[15] or higher.
Req	The SSH protocol provided for remote management shall support the TM terminal CLI.
Opt	The SSH protocol provided for remote management should provide the mechanism to establish a tunnel for SNMP protocol (IETF, RFC 1157) to pass through.
Opt	Remote management of TM terminals should provide the HTTPS protocol.[16]

[15] Internet Engineering Task Force. "The Secure Shell (SSH) Protocol Architecture." RFC 4251. January 2006. Updated by RFC 8308. Retrieved 27 January 2020. Available at https://tools.ietf.org/html/rfc4251.

[16] Internet Engineering Task Force. "HTTP over TLS." RFC 2818. May 2000. Updated by RFC 5785 and RFC 7230. Retrieved 27 January 2020. Available at https://tools.ietf.org/html/rfc2818.

Req	Remote management of TM terminals shall provide the SNMP protocol version 3 with backwards compatibility for SNMP version 2c.

Appendix C provides a minimum set of required and optional alarm, configuration, and statistical parameters.

4.2 QoS

The TMoIP protocol is based upon the IP protocol. The Internet services model (upon which IP is based) of a sender/single receiver is insufficient for real-time data services. In the case of transport of TM data, the real-time requirements are particularly important. Therefore QoS mechanisms need to be defined and implemented to support both multicast and real-time (TM) service transport.

Differentiated services (DiffServ) generically defines a mechanism where traffic is classified into a number of service types and the flow of traffic is controlled based upon the service type.

The TMoIP QoS scheme is based upon the DiffServ model for providing QoS support and uses the following mechanisms:

a. traffic classification and prioritization;

b. preferential queuing of high-priority traffic.

This standard defines the means by which the TM packets can be classified. The queuing and preferential treatment of the TM packets is not in the scope of this document, and will be allocated to the ground network link infrastructure (switches, routers) over which the TMoIP packets propagate.

4.2.1 Layer 2 Mechanisms

The IEEE 802.1p specification enables Layer 2 switches to prioritize traffic and perform dynamic multicast filtering. The prioritization specification works at the media access control (MAC) framing layer (OSI layer 2) and is therefore called a layer 2 mechanism.

The 802.1p header includes a three-bit field for traffic prioritization that allows packets to be grouped into various traffic classes. The IEEE 802.1p standard establishes eight levels of priority. The highest priority is seven, which might go to network-critical traffic such as Routing Information Protocol and Open Shortest Path First table updates. Values five and six might be for delay-sensitive applications such as interactive video and voice. Data classes four through one range from controlled-load applications such as streaming multimedia and business-critical traffic (carrying Session Announcement Protocol [SAP] data, for instance) down to “loss eligible” traffic. The zero value is used as a best-effort default, invoked automatically when no other value has been set. Table 4-2 defines the Layer 2 QoS mechanisms for TMoIP packets.

Table 4-2. Layer 2 QoS Mechanisms

Req/Opt	Requirement description
Opt	To support Layer 2 QoS mechanisms, the TM terminal shall provide the ability to modify the VLAN priority bits.

NOTE	It is recommended that vendors of TMoIP equipment provide shaping of TMoIP streams such that the packet rate at the network ingress has minimum variation.

4.2.2 Layer 3 Mechanisms

Support for QoS via the DiffServ model can also be implemented at Layer 3. This provides QoS support for end equipment such as routers that are Layer 3-aware. Table 4-3 defines the Layer 3 QoS mechanisms for TMoIP packets.

Table 4-3. Layer 3 QoS Mechanisms

Req/Opt[(1)]	Requirement description
Req	To support Layer 3 QoS mechanisms, the TM terminal shall provide the ability to modify DiffServ Code point (DSCP) data for each TM flow.
Opt	Support for extended tagging mechanisms, such as Multi-Protocol Label Switching, is recommended.

4.3 Network Performance

This section describes the characterizations of network performance criteria that impact successful TM stream transport over IP networks. Future versions of this standard will address quantifying these parameters.

4.3.1 Packet Delay Variation

As TMoIP packets are generated by a constant-rate serial bit stream, the packets will natively be generated at a constant rate. Jitter in the inter-packet delay is introduced when the packet rate is impacted by variable switching delays as the packet traverses the network. This jitter is more commonly referred to as packet delay variation, and can result in errors in the regenerated stream if the delay between any two packets is increased too much (resulting in underflow in the receive buffer) or too little (resulting in overflow in the receive buffer).

4.3.2 Delay

Subsection 3.5.2 item c discussed the causes of delay and its effects. In most cases, the largest contribution to delay is incurred in the packet reassembly buffer located at the receiver. One mechanism to mediate the effects of the reassembly buffer delay and to support performing the temporal alignment of a number of telemetry streams is to provide the ability to adjust the depth of the reassembly buffer. Actual implementation details are beyond the scope of this document and will be left to the vendor.

NOTE	In any TMoIP solution, it is recommended that considerations for stream alignment be addressed

4.3.3 Network Errors

Potential sources of network errors that can negatively impact TMoIP operation are:

a. bit errors in network;

b. dropped packets;

c. misaligned packets.

Bit errors that occur in the payload will result in bit errors in the regenerated bit stream. Packet-level errors can be more problematic, as they impact data integrity and can cause dropped packets, which can produce errors in the recovered clock.

Errors that occur on the packet level can be caused by a number of faults, such as bit errors in the addressing fields that result in non-delivery of the packet, or bit errors in the payload that, upon detection, cause the packet to be dropped.

The effects of a lost packet are twofold: The payload itself is lost, resulting in corruption of the TM data; and when adaptive clock recovery is used, the loss of a packet will cause an error in the recovered clock frequency. A “stuff packet” can mitigate the effect of a lost packet on the clock recovery mechanism. A stuff packet is a packet that is inserted into the TMoIP Receiver clock recovery buffer to restore it to the correct level and diminish the effects of a lost packet on the adaptive clock recovery algorithm.

NOTE	This standard recommends that the TMoIP adaptive clock recovery algorithm be architected to tolerate dropped packets.

Table 4-4 defines the mechanisms for limiting the effects of dropped packets on network performance.

Table 4-4. Network Performance - Dropped Packets

Req/Opt(1)	**Requirement description**
Req	In order to maintain the adaptive clock recovery mechanism, the capability to insert stuff packets at the RX TM terminal when a packet loss is detected shall be supported.
Req	The user shall have the ability to enable or disable the packet-stuffing feature on a per-stream basis.
Req	The stuff packet shall be composed of a series of identical bytes. The data pattern of the stuff byte shall be user-defined.

4.4 IPv4 to IPv6 Migration

This standard defines operation in IPv4 network infrastructures. As IPv6 networks become more prevalent, the need to generate native IPv6 traffic will become necessary. Currently, end-to-end networks that support IPv6 traffic are not common enough to warrant the requirement for native IPv6 packet construction for the current revision of this document. Table 4-5 defines the requirements for IPv4 and IPv6 packet construction.

Table 4-5. IPv4/IPv6 Requirements

Req/Opt(1)	**Requirement description**
Req	The TM terminal shall generate packets compliant to IPv4.
Req	The TM terminal shall generate packets compliant to IPv6.

NOTE The RCC TTG recommends that vendors of TMoIP equipment design the architecture of the packetizing engine using programmable logic that has the ability to migrate to IPV6 support via system firmware upgrades.

NOTE The RCC TTG recommends tunneling techniques to support the transport of TMoIP traffic over IPv6 equipment. The tunneling functionality is reserved for external routers in the ground network.

NOTE This version of the TMoIP standard intends for IPv6 addressing features only to be supported. Support for additional features of IPv6 is left to the description of the manufacturer. Advanced features of IPv6 will be further developed in a future version of this standard.

4.5 Multicast Support

An important feature of the IP protocol is the ability to natively support multicast traffic. This section will identify considerations when multicasting TM streams.

Multicast supports communications from one transmitter to multiple receivers over an IP network. Support for a large number of receivers is inherent, as the identity and the number of receivers is not required. Multicast is bandwidth efficient, because the transmitter has to send the packet only once. The packets are replicated by the downstream nodes as required to support delivery to all receivers.

Multicast packets use special types of IP addresses that identify to the network that the packet contains multicast traffic. These IP addresses are referred to as Multicast group addresses. At the network ingress, the network TX stream will be constructed with the multicast group address as the destination address. If a node wants to receive traffic from a particular multicast group, it must inform the network. In this fashion, the receiver “joins” the multicast group. Once the receiver has joined a particular multicast group, the network equipment in the path forwards the packets for that multicast group to the receiver. If no receivers have joined a multicast group, the network equipment will not forward these packets. In this fashion, multicast traffic only consumes network bandwidth when a receiver requests the traffic. Receivers use the IGMP to join a multicast group.

Multicast addresses are identified by the pattern “1110” in the first four bits, which corresponds to a first octet of 224 to 239. The full range of multicast addresses is from 224.0.0.0 to 239.255.255.255.

An additional set of protocols (SAP[17] and Session Description Protocol [SDP][18]) allows multicast senders to communicate the characteristics of their multicast streams to potential receivers. The receivers monitor the SAP packets to identify potential streams that they may want to decode. The SAP listening applications can listen to the well-known SAP multicast

[17] Internet Engineering Task Force. “Session Announcement Protocol.” RFC 2974. October 2000. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc2974/.

[18] Internet Engineering Task Force. “SDP: Session Description Protocol.” RFC 2327. Obsoleted by RFC 4566. April 1998. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc2327/.

address and construct a guide of all advertised multicast sessions. The SAP specification uses SDP as the format of the session descriptions.

Table 4-6 defines multicast requirements for TM terminals.

Table 4-6. Multicast Packets

Req/Opt	Requirement description
Req	The TM terminals that transmit to the ground network shall support the generation of multicast packets with a user-programmable multicast group address.
Req	The TM terminals that receive from the ground network shall support the IGMP version 2 or higher protocols to join and leave multicast groups.

NOTE	The RCC TTG recommends that TMoIP transmitters support generation of SAP/SDP messaging to advertise their content.

APPENDIX A

Recommendations for TM Terminal Layer 1

This appendix provides recommendations and guidelines for the Layer 1 (Physical Layer) implementation of the TM terminal (see Table A-1).

Table A-1. Recommendations and Guidelines for the Layer 1 (Physical Layer) Implementation of the TM Terminal

Category	Recommendation/Guideline
a. Physical	
Req	BNC-type connectors with an impedance of 75 ohms
Opt	BNC-type connectors with an impedance of 50 ohms
Opt	Support of RS530 physical interface
b. Electrical	
Req	Single-ended TTL electrical
Opt	Balanced electrical interface
Req	Support rate adaptive mechanism for signaling rate reconstruction
Opt	Provide for migration to signaling rates to 100 Mbps
c. Encoding	
Req	Encoding shall comply with encoding requirements specified in IRIG 106 Chapter 4 for Non-Return-to-Zero Level serial streams
Opt	Streams can optionally support the remaining IRIG 106 Chapter 4 encoding schemes, including: • Viterbi • Non-Return-to-Zero Mark • Non-Return-to-Zero Space • Randomized • Biphase-L
Note: Req = Required Opt = Optional	

This page intentionally left blank.

APPENDIX B

Considerations for Legacy Asynchronous Transfer Mode Interworking

This appendix describes TMoIP implementation considerations for occasions when the packetized stream is subsequently transported over an ATM network. Using these considerations when constructing the TMoIP stream can offer transport efficiencies, particularly during the process of converting from IP packets to ATM cells.

The IP over ATM encapsulation mechanism (IETF, RFC 2684) initially produces an IP stream from the TM stream source. This mechanism encapsulates the stream using the RFC 2684 encapsulation scheme for transporting IP packets over ATM networks. This process generates ATM cells that carry the IP packets.

Table B-1 shows several possible packet sizes for optimal RFC 2684 encapsulation. The optimal encapsulation provides the most efficient encapsulation of the TMoIP packet into the RFC 2684 format. If the optimal encapsulation is used, then all of the cells in the ATM are completely filled and no bandwidth is wasted because there are no partially filled cells.

Table B-1. Request for Comments (RFC) 2684 Optimal Payloads

Number of ATM Cells	Total Bytes 53/cell	ATM Payload 48/cell	TMoIP Payload	TMoIP Raw Payload	Percent Overhead
20	1060	960	942	888	16
15	785	720	702	648	17
10	530	480	462	408	23
6	318	288	270	153	52
3	159	144	126	72	55

NOTE	Supporting the packet sizes in Table B-1 provides the most efficient payloads for transport over ATM networks.

This page intentionally left blank.

APPENDIX C

Summary of Managed Objects

This appendix summarizes the required and optional parameters of the TMoIP implementation. These managed objects are relevant to the transport function of the equipment that implements TMoIP. Additional managed objects may be implemented, but their definition is not in the scope of this document.

The following requirement topics are covered in this appendix.

Table	Topic	Page
Table C-1.	Alarms	C-1
Table C-2.	Configuration Parameters	C-1
Table C-3.	TM Statistics	C-3
Table C-4.	Ethernet Statistics	C-3

Table C-1. Alarms

Description	Notes
Physical	
TM Input Fault[1]	Per TMoIP flow
Ethernet link failure	Per Ethernet port
Protocol	
Ingress FIFO Overrun	Per TMoIP flow
Egress FIFO Overrun	Per TMoIP flow
Egress FIFO Underrun	Per TMoIP flow

[1] The TM Input Fault is defined as telemetry stream that is out of compliance with IRIG 106.

Table C-2. Configuration Parameters

Description	Notes
Rx Parameters	
Rx Destination IP Address	Accept IP Address
Rx Destination UDP Port	Accept UDP Port
Rx Destination MAC Address	Accept MAC Address
Rx 802.1p Priority	
Rx 802.1p VLAN ID	
Rx DSCP	
Rx IGMP	Enable IGMP Support to respond to IGMP Query packets
Filter Enable/Select	Accept IP Port, UDP Port, MAC Address
Tx Parameters	
Tx Destination IP Address	Target IP Address
Tx Destination MAC Address	Target MAC Address

Tx Destination UDP Port	Target UDP Port
Tx Source IP Address	
Tx Source MAC Address	Read-Only
Tx Source UDP Port	
Tx 802.1p Tag	Enable/Disable (Opt)
Tx 802.1p Priority	
Tx 802.1p VLAN ID	
Tx DSCP	
Tx ARP	Enable/Disable
Tx Data Length	
Packet Size	
Port	
TM Port Configuration Parameters	Vendor defined port configuration parameters
Statistics	
Clear Stats Counters	

Table C-3. TM Statistics

Description	**Notes**
TM Frame, RX	
Reassembled TMoIP Packets	Number of raw TMoIP packets received and reassembled
Sequence Errors	Detected in TMoIP control word
FIFO Overruns	
Dropped Reassembled TMoIP Packets	Number of TMoIP packets dropped
TM Frame, TX	
Assembled TMoIP Packets	Number of raw TMoIP packets assembled for transmission
FIFO Overruns	
FIFO Underruns	

Table C-4. Ethernet Statistics

Description	**Notes**
Rx Frame Counts	
Received Frames	Total all received Ethernet frames
Good Frames	
Forwarded Frames	Forwarded to upper layer
Forwarded Octets	Forwarded to upper layer
Rx Discard Frames	
Total Frame Discards	Total all discards
Rx Buffer Discards	Discards due to buffer overrun
Rx Error Discards	Total discards due to errors
Frame Collision	
Pause Frames	Indicates flow control events

Tx Frame Counts	
Transmitted Frames	Total all transmitted Ethernet frames
Good Frames	
Frames Sent	
Octets Sent	
Pause Frames	
Queue Overflow	
Tx Discard Frames	
Total Frame Discards	Total all transmit frame discards
Tx Buffer Discards	Discards due to buffer overrun
Tx Error Discards	
Late Collision Discards	
Carrier loss Discards	
Retransmit Limit Discards	

This page intentionally left blank.

APPENDIX D

Application Notes

This appendix provides additional application information that, while not in the scope of the TMoIP requirements, is intended to provide information to the user to enable the deployment of a network infrastructure that supports the TMoIP implementation.

D.1 Security

In the scope of the TMoIP protocol, security applies to two functions:

a. secure transmission of TM streams;

b. secure transmission of management information.

Given that TM streams are source-encrypted, the aspect of security is reserved for the provider edge (PE), and is outside of the scope of the TMoIP protocol; however, this standard will make some recommendations to promote network compatibility, and to frame the discussion for future implementations.

For applications outside the scope of Type 1 encryption, use of encryption compliant to Federal Information Processing Standards (FIPS)-140-2[19] Level 2 is recommended. The FIPS-140 document is a set of cryptographic standards issued by the National Institute of Standards and Technology for use by departments and agencies of the US government. Support for FIPS is becoming available in PE equipment.

NOTE	This standard recommends that the TMoIP implementation and connected infrastructure provide support or migration to FIPS-140 encryption.

For applications that require Type 1 encryption this standard recommends that the ground network link equipment allow for IP encapsulation through the use of a tunneling protocol such as Generic Routing Encapsulation. This becomes especially important where the traffic is multicast and not entirely unicast, as Type 1 cryptos prohibit the transport of multicast streams.

NOTE	For installations that require the use of Type 1 encryption, this standard recommends that the ground network link equipment support an IP tunneling protocol to enable tunneling of multicast traffic through the cryptos.

To enable the secure transmission of management information, Version 3 of the SNMP provides support for encryption, authentication, and access control of management packets.

[19] National Institute of Standards and Technology. *Security Requirements for Cryptographic Models*. FIPS Pub 140-2. 25 May 2001. Superseded by FIPS Pub 140-3. Retrieved 27 January 2020. Available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

NOTE This standard recommends that TMoIP implementations that support SNMP management provide immediate support or a migration path to SNMP version 3.

D.2 Reliability and Redundancy

As the IP protocol suite was intended for the best-effort delivery of traffic, reliability was not a prime consideration when the protocol was originally conceived; however, there exist mechanisms in the IP protocol that can be used to provide increased reliability. This section provides an overview of techniques that can be used to enhance the reliability of the ground network link.

The Spanning Tree Protocol (STP) can be used as a mechanism to provide redundant operation. The STP is a Layer 2 mechanism that ensures the existence of a loop-free network topology for any local area network. Spanning Tree eliminates broadcast storms in a mesh network by disabling links that incur loops in the network.

Spanning Tree can be used to provide network redundancy in the following fashion.

a. Design the TMoIP link to intentionally have two paths between endpoints, introducing a loop in the network.

b. Enable the operation of Spanning Tree in the ground network link equipment.

c. The Spanning Tree algorithm will disable one of the paths at all times. If at some point the active path is disabled, the alternate path will become the active path.

This scheme requires the following:

a. all equipment in the ground network link must be STP-enabled;

b. all equipment must have the same version of STP.

This scheme lends itself to the current generation of end equipment that supports enhanced fail-over switching to provide a self-healing network topology.

In addition to providing redundant service, the reliability of the TMoIP network implementation can be improved by providing protection against link oversubscription. The IP standard does not require end stations that are about to transmit to communicate with each other (or establish a connection) prior to the transmission of traffic. One drawback of this scheme is that if too many end stations generate traffic simultaneously, the payload capacity of the network may be exceeded. In the case of the transmission of multiple high-bandwidth real-time TM streams, this is a realistic concern.

D.3 Multicast Routing Considerations

In addition to the requirements to enable the transport of multicast TM traffic, the need exists for routing support of multicast traffic. This function is supported via a set of multicast routing protocols. These protocols construct distribution trees so that data can flow from senders of multicast traffic to all receivers that have joined the group. This function is of particular importance in complex IP networks, where the source traffic must span a number of routers to reach its destination node.

The implementation of multicast routing is reserved for the PE, and is outside the scope of this protocol; however, some application information is presented below to assist the network designer.

D.3.1 Current Multicast Routing Protocols

The following multicast routing protocols are currently used to a significant extent.

a. Protocol-Independent Multicast Sparse Mode;

b. Protocol-Independent Multicast Dense Mode;

c. Distance Vector Multicast Routing Protocol.

D.3.2 Selection Considerations

In the selection of the multicast routing protocol, the following considerations should be addressed.

a. Base Requirement. In simple, linear network configurations multicast routing is not required and only adds to network complexity.

b. Opt-in vs. Opt-out Routing. Multicast routing protocols are differentiated into two basic schemes. In an opt-in implementation, multicast traffic is not transmitted until the routing tree has been constructed. This scheme is bandwidth-efficient, especially in networks where a relative few number of nodes will receive the multicast traffic. In an opt-out implementation, the multicast traffic is initially broadcast to the network, and routers prune multicast traffic forwarding if the downstream nodes are not members of that particular multicast group. This scheme is very efficient when the network is densely populated with nodes that will receive the multicast traffic.

c. Signaling. Multicast routing requires signaling traffic to be exchanged between routers to support the construction of the multicast routing trees. The potential effects of this traffic on the timely delivery of real-time TM streams must be considered by the network planner.

This page intentionally left blank.

APPENDIX E

Citations

Internet Engineering Task Force. “DoD Standard – Transmission Control Protocol.” RFC 761. Obsoleted by RFC 793 and RFC 7805. January 1980. Retrieved 22 July 2019. Available at https://datatracker.ietf.org/doc/rfc761/.

———. “Host Extensions for IP Multicasting.” RFC 1112. Updated by RFC 2236. August 1989. Retrieved 22 July 2019. Available at https://datatracker.ietf.org/doc/rfc1112/.

———. “HTTP over TLS.” RFC 2818. May 2000. Updated by RFC 5785 and RFC 7230. Retrieved 27 January 2020. Available at https://tools.ietf.org/html/rfc2818.

———. “Hypertext Transfer Protocol – HTTP/1.1.” RFC 2616. June 1999. Obsoleted by RFC 7230, RFC 7231, RFC 7232, RFC 7233, RFC 7234, and RFC 7235. Retrieved 27 January 2020. Available at https://tools.ietf.org/html/rfc2616.

——— “Internet Group Management Protocol, Version 3.” RFC 3376. Updated by RFC 4604. October 2002. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc3376/.

———. “Internet Protocol.” RFC 791. Updated by RFC 2474, RFC 6864, and RFC 1349. September 1981. Retrieved 16 April 2019. Available at https://datatracker.ietf.org/doc/rfc791/.

———. “Multiprotocol Encapsulation over ATM Adaptation Layer 5.” RFC 2684. May be superseded or updated. September 1999. Retrieved 22 July 2019. Available at https://datatracker.ietf.org/doc/rfc2684/.

———. “Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture.” RFC 3985. Updated by RFC 5462. March 2005. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc3985/.

———. “Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3).” RFC 3916. September 2004. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc3916/.

———. “SDP: Session Description Protocol.” RFC 2327. Obsoleted by RFC 4566. April 1998. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc2327/.

———. “Session Announcement Protocol.” RFC 2974. October 2000. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc2974/.

———. “Simple Network Management Protocol (SNMP). RFC 1157. May 1990. May be superseded by update. Retrieved 2 January 2020. Available at https://datatracker.ietf.org/doc/rfc1157/.

———. “Structure Agnostic Time Division Multiplexing (TDM) over Packet (SAToP).” RFC 4553. June 2006. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc4553/.

———. “The Secure Shell (SSH) Protocol Architecture.” RFC 4251. January 2006. Updated by RFC 8308. Retrieved 27 January 2020. Available at https://tools.ietf.org/html/rfc4251.

———. “User Datagram Protocol.” RFC 768. 28 August 1980. May be superseded or amended by update. Retrieved 7 May 2019. Available at https://datatracker.ietf.org/doc/rfc768/.

National Institute of Standards and Technology. *Security Requirements for Cryptographic Models*. FIPS Pub 140-2. 25 May 2001. Superseded by FIPS Pub 140-3. Retrieved 27 January 2020. Available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

Range Commanders Council. “Pulse Code Modulation Standards” in *Telemetry Standards*. Chapter 4. IRIG 106-19. July 2019. May be superseded by update. Retrieved 27 January 2020. Available at https://www.wsmr.army.mil/RCCsite/Documents/106-19_Telemetry_Standards/chapter4.pdf.

———. “Standards for Data Quality Metrics and Data Quality Encapsulation” in *Telemetry Standards*. Chapter 2 Appendix 2-G. IRIG 106-19. July 2019. May be superseded by update. Retrieved 27 January 2020. Available at https://www.wsmr.army.mil/RCCsite/Documents/106-19_Telemetry_Standards/chapter2.pdf.

———. *Telemetry Standards*. RCC 106-19. July 2019. May be superseded by update. Retrieved 22 July 2019. Available at https://www.wsmr.army.mil/RCCsite/Pages/Publications.aspx.

APPENDIX F

References

Internet Engineering Task Force. "A Simple Network Management Protocol (SNMP)." RFC 1157. May 1990. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc1157/.

——— "Concise MIB Definitions." RFC 1212. March 1991. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc1212/.

———. "Framework for IP Performance Metrics." RFC 2330. Updated by RFC 7312 and RFC 8468. May 1998. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc2330/.

———. "Internet Protocol, Version 6 (IPv6)." RFC 2460. Obsoleted by RFC 8200. December 1998. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc2460/.

———. "Layer Two Tunneling Protocol – Version 3 (L2TPv3)." RFC 3931. Updated by RFC 5641. March 2005. Retrieved 24 July 2019. Available at https://datatracker.ietf.org/doc/rfc3931/.

———. "Multiprotocol Label Switching Architecture." RFC 3031. Updated by RFC 6790 and RFC 6178. January 2001. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc3031/.

———. "Network Time Protocol (Version 3) Specification, Implementation and Analysis." RFC 1305. Obsoleted by RFC 5905. March 1992. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc1305/.

——— "RTP: A Transport Protocol for Real-Time Applications." RFC 1889. Obsoleted by RFC 3550. January 1996. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc1889/.

———. "Time Division Multiplexing over IP (TDMoIP)." RFC 5087. December 2007. May be superseded or updated. Retrieved 23 July 2019. Available at https://datatracker.ietf.org/doc/rfc5087/.

END OF RCC DOCUMENT